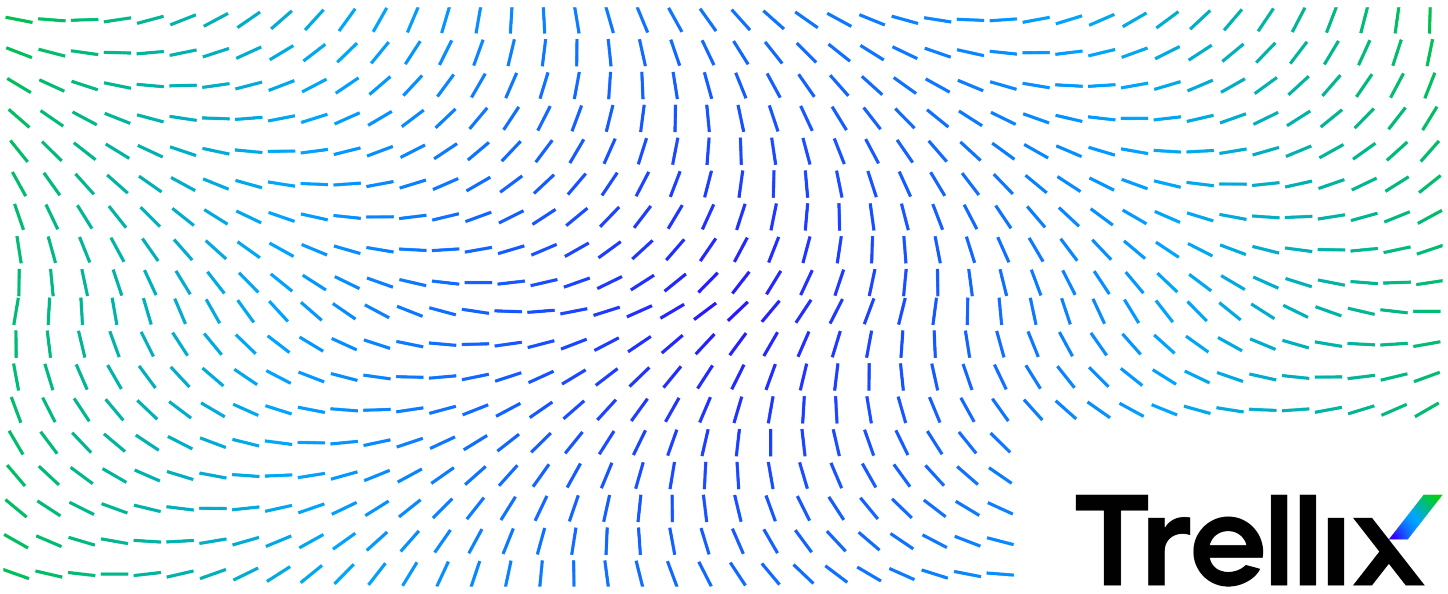
Trellix Endpoint Security (ENS) 10.7.x Product Guide - Windows



Contents

Product overview. 20

Overview of Trellix Endpoint Security (ENS). 20

How Trellix ENS works. 20

Threat Prevention. 22

Overview of Threat Prevention. 22

Key features of Threat Prevention. 22

How Threat Prevention works. 23

Firewall. 25

Overview of Firewall. 25

Key features of Firewall. 25

How Firewall works. 26

Web Control. 27

Overview of Web Control. 27

Key features of Web Control. 27

How Web Control works. 28

Adaptive Threat Protection. 29

Overview of Adaptive Threat Protection. 29

Key features of Adaptive Threat Protection. 30

How Adaptive Threat Protection works. 31

Feature overview. 36

Threat Prevention. 36

How content files work. 36

How false positive mitigation works. 37

How application protection rules work. 37

How signatures protect applications and systems. . . . 38
How Network IPS works. . . . 40
How Trellix GTI works. . . . 41
How on-access scanning works. . . . 41
How AMSI integration with Threat Prevention improves security. . . . 43
How the script scanner works. . . . 43
How on-demand scanning works. . . . 45
When the global scan cache is flushed. . . . 46
How system utilization works. . . . 47
How Threat Prevention limits CPU usage. . . . 48
How Remote Storage scanning works. . . . 48
Threat Prevention additions to Trellix ePO - On-prem. . . . 49
Permission sets and Threat Prevention Trellix ePO - On-prem. . . . 50
Client tasks and Threat Prevention. . . . 53
What to do first. . . . 54
Firewall. . . . 55
How firewall rules work. . . . 55
How firewall rule groups work. . . . 56
Predefined firewall rule groups in Trellix ePO - On-prem. . . . 56
Predefined firewall rule groups on a client system. . . . 57
How Trellix core networking rules work. . . . 59
Firewall rules in the Trellix core networking group. . . . 59
Using timed groups. . . . 61
Making groups location-aware. . . . 62
Firewall rule groups and connection isolation. . . . 65
Firewall stateful packet filtering and inspection. . . . 67
How stateful packet filtering works. . . . 67
How stateful packet inspection works. . . . 68
Firewall state table. . . . 69
Stateful protocol tracking. . . . 69

Using trusted networks to allow traffic automatically. 71
Using trusted executables and applications to reduce false positives. 71
Using the Firewall Catalog to reference existing items. 72
Firewall protocols. 72
How Adaptive mode affects Firewall. 74
FAQ — Trellix GTI and Firewall. 75
Firewall additions to Trellix ePO - On-prem. 76
Permission sets and Firewall (Trellix ePO - On-prem). 78
Client tasks and Firewall. 80
Web Control. 81
Supported and unsupported browsers. 81
Identifying threats while browsing. 81
Identifying threats while searching. 83
Site reports provide details. 83
How Web Control blocks or warns about a site or download. 85
How Web Control and Skyhigh Client Proxy work together. 85
How web gateway enforcement works. 86
How safety ratings are compiled. 87
How file downloads are scanned. 87
How Trellix GTI works. 88
How Web Control works with Web Reporter. 88
Information that the software sends to Trellix ePO - On-prem. 89
Web Control additions to Trellix ePO - On-prem. 90
Permission sets and Web Control (Trellix ePO - On-prem). 91
Client tasks and Web Control. 93
Frequently asked questions. 94
Adaptive Threat Protection. 95
How file and certificate reputations control access. 95
How a reputation is determined. 96
File reputation versus process reputation. 99

When is the cache flushed? . . . 99
How content files work . . . 100
How ATP remediates threats . . . 101
How enhanced remediation protects systems . . . 102
How false positive mitigation works . . . 105
How Real Protect scanning monitors activity . . . 106
How enhanced script scanning improves security . . . 107
Test Real Protect scanning . . . 109
Real Protect test scan result codes . . . 110
How Credential Theft Protection works . . . 111
How Adaptive Threat Protection protects against fileless attack methods . . . 111
How Dynamic Application Containment works . . . 112
Adaptive Threat Protection additions to Trellix ePO - On-prem . . . 113
Permission sets and Adaptive Threat Protection (Trellix ePO - On-prem) . . . 115
Server settings and Adaptive Threat Protection . . . 117
Client tasks and Adaptive Threat Protection . . . 117
Using Adaptive Threat Protection in your environment . . . 118
Building file prevalence using Observe mode . . . 118
Monitoring and making adjustments . . . 118
Submitting files for further analysis . . . 119

Configuring with Trellix ePO - On-prem . . . 121

Configuring common features . . . 121
Policies and Common . . . 121
Protect services and files . . . 122
Set up logging for client activity . . . 123
Control access to the client interface . . . 123
Effects of setting an administrator password . . . 124
Configure temporary access to the client interface . . . 124
Example workflow for using a temporary password . . . 125
Configure client interface lockout behavior . . . 126

Unlock the client interface from Trellix ePO - On-prem. . . . 127
Prevent AAC from blocking trusted programs. . . . 127
Excluding processes from AAC. . . . 128
Configure proxy server settings. . . . 128
Configure default behavior for updates. . . . 129
How the Default Client Update task works. . . . 129
Protecting Trellix processes from third-party DLLs. . . . 130
How the Validation and Trust Protection service works. . . . 130
How AAC works. . . . 131
Validation failures. . . . 132
Considerations when trusting a third-party certificate. . . . 133
Upload a third-party certificate. . . . 133
Allow certificate authentication. . . . 134
Delete certificates from the certificate store. . . . 134
Configuring Threat Prevention. . . . 135
Policies and Threat Prevention. . . . 135
Preventing Threat Prevention from blocking trusted programs, networks, and services. . . . 136
Wildcards in exclusions. . . . 140
Preventing threats from accessing systems. . . . 142
How threats gain access. . . . 143
Types of Access Protection rules. . . . 144
Trellix-defined Access Protection rules. . . . 146
How targets in subrules are evaluated. . . . 154
How buffer overflow exploits occur. . . . 155
Excluding items from Exploit Prevention. . . . 156
Protect files, registry, processes, and services with Access Protection rules. . . . 158
Prevent Access Protection from blocking trusted programs. . . . 159
Configure Exploit Prevention settings to block threats. . . . 160
Exclude items from Exploit Prevention protection. . . . 167
Add Exclusion or Edit Exclusion. . . . 168

Get the signer distinguished name from Trellix ePO - On-prem to use to exclude executables. . 174
Assigning multiple instances of Exploit Prevention policy. 174
Scanning for threats on client systems. 175
Types of scans. 175
Configure settings for all scans. 178
Exclude items from AMSI scanning. 178
Define which potentially unwanted programs to detect. 179
Enable detection and response for potentially unwanted programs. 180
Configure scans that run automatically when files are accessed. 180
Determining which scanning policies you need. 181
Choosing when to scan files with the on-access scanner. 181
Best practices: Reducing the impact of on-access scans on users. 182
Configure Threat Prevention with no connection to Trellix GTI. 183
Verify ScriptScan exclusions. 184
Configure predefined scans that can be run manually or scheduled. 184
Best practices: Reducing the impact of on-demand scans on users. 184
Schedule quick scans and full scans from Trellix ePO - On-prem. 187
Configure and schedule custom scans from Trellix ePO - On-prem. 188
Best practice: Daily memory scans. 188
Best practice: Regularly scheduled scans per system type. 189
Pause the On-Demand Scan from Trellix ePO - On-prem. 190
Cancel the On-Demand Scan from Trellix ePO - On-prem. 190
Configuring Firewall. 191
Policies and Firewall. 191
Enable and configure Firewall. 193
Block DNS traffic. 193
Define networks to use in rules and groups. 194
Exclude network addresses from a Trellix GTI lookup. 194
Configure trusted executables. 195
Get the signer distinguished name from Trellix ePO - On-prem to use to specify trusted executables 195

Manage firewall rules and groups. . . . 195
Wildcards in firewall rules. . . . 196
Create connection isolation groups. . . . 199
Create timed groups. . . . 200
Use the Firewall Catalog. . . . 200
Tuning Firewall. . . . 202
Using Adaptive mode to create client rules automatically. . . . 203
FAQ — Adaptive mode. . . . 203
Analyzing client data. . . . 204
Manage Firewall client rules. . . . 205
Configuring Web Control. . . . 205
Policies and Web Control. . . . 205
How policies work. . . . 208
Assign multiple instances of a policy. . . . 208
Evaluating policy settings with Observe mode. . . . 209
Enable and disable Web Control. . . . 209
Configuring browsers to force-enable the Web Control plug-in. . . . 210
Track browser events to use for reports. . . . 210
Specify enforcement behavior for specific actions. . . . 211
Warn about or block unknown URLs and file downloads. . . . 211
Scan files before downloading. . . . 211
Download files from not yet verified URLs. . . . 212
Block all internal sites. . . . 212
Configure Secure Search. . . . 212
Send Web Control logs from Trellix ePO - On-prem to Web Reporter. . . . 213
Manage blocked and allowed sites. . . . 213
Prohibit use of specific browsers. . . . 215
Specify rating actions and block site access based on web category. . . . 216
Customize user notifications for blocked content. . . . 217
Configuring Adaptive Threat Protection. . . . 217

Policies and Adaptive Threat Protection. 217
Containing applications dynamically. 220
Enable the trigger threshold for Dynamic Application Containment. 220
Configure Trellix-defined containment rules. 221
Trellix-defined Dynamic Application Containment rules. 221
Best practice: Tune Dynamic Application Containment. 237
View contained applications from Trellix ePO - On-prem. 237
Prevent Dynamic Application Containment from containing trusted programs. 238
Get the signer distinguished name from Trellix ePO - On-prem to use to exclude executables. . 238
Allowing contained applications to run normally. 239
Configure Adaptive Threat Protection. 239
Exclude processes from Adaptive Threat Protection scanning. 239
Wildcards in exclusions. 240
Best practices: Improve performance during program compilation. 243
Exclude items from enhanced script scanning. 244
Configure Adaptive Threat Protection with no connection to Trellix GTI. 246

Managing with Trellix ePO - On-prem. 247

Managing common features. 247
Keeping your protection up to date. 247
Check the content date and version. 247
Update content files with Trellix ePO - On-prem. 248
Using repository lists for update sites. 249
How mirror tasks work. 250
Submitting threat samples for analysis. 250
Common additions to Trellix ePO - On-prem. 250
Permission sets and Common (Trellix ePO - On-prem). 252
Client tasks and Common. 252
Managing Threat Prevention. 253
Check the content date and version. 253
Update content files with Trellix ePO - On-prem. 254

Content file update strategies. . . . 255
Submitting threat samples for analysis. . . . 256
Handling new malware with Extra.DAT files. . . . 256
Download and deploy an Extra.DAT file to client systems from Trellix ePO - On-prem. . . . 256
Remove AMCore content on the client system from Trellix ePO - On-prem. . . . 257
Responding to detections. . . . 257
Responding to access point violations. . . . 257
Responding to Exploit Prevention detections. . . . 258
Filter the Exploit Prevention Events list. . . . 259
Aggregate Exploit Prevention events. . . . 259
Create exclusions from Exploit Prevention events. . . . 260
Responding to unwanted program detections. . . . 261
Responding to on-access scan detections. . . . 261
Responding to on-demand scan detections. . . . 262
Quarantined items. . . . 262
Specify quarantine location and retention time. . . . 262
Restore quarantined items from Trellix ePO - On-prem. . . . 263
Enabling activity logging for on-demand scan. . . . 263
Configure on-demand scanning activity logging for managed systems. . . . 263
View on-demand scan activity logging status on managed systems. . . . 264
Configure on-demand scanning activity logging for standalone systems. . . . 264
Disable on-demand scan activity logging. . . . 264
Set the required product log size. . . . 265
Analyzing your protection. . . . 265
Managing Adaptive Threat Protection. . . . 266
Check the content date and version. . . . 266
Update content files with Trellix ePO - On-prem. . . . 267
Content file update strategies. . . . 267
Submitting threat samples for analysis. . . . 268
Handling new false positives with Extra.DAT files. . . . 268

Download and deploy an Extra.DAT file to client systems from Trellix ePO - On-prem. 268
Restore quarantined objects from Trellix ePO - On-prem. 269
Monitoring activity in your environment. 270
Monitoring your protection. 270
Dashboards, monitors, and Common. 270
Queries, reports, and Common. 277
Server tasks and Common. 282
Roll up system or event data for Trellix ENS (Trellix ePO - On-prem). 284
Events, responses, and Common. 284
Monitoring Threat Prevention activity. 285
Dashboards, monitors, and Threat Prevention. 285
Queries, reports, and Threat Prevention. 289
Server tasks and Threat Prevention. 296
Roll up system or event data for Trellix ENS (Trellix ePO - On-prem). 298
Events, responses, and Threat Prevention. 298
Monitoring Firewall activity. 299
Dashboards, monitors, and Firewall. 299
Queries, reports, and Firewall. 300
Server tasks and Firewall. 302
Roll up system or event data for Trellix ENS (Trellix ePO - On-prem). 304
Events, responses, and Firewall. 305
Monitoring Web Control activity. 305
Dashboards, monitors, and Web Control. 305
Queries, reports, and Web Control. 308
Server tasks and Web Control. 310
Roll up system or event data for Trellix ENS (Trellix ePO - On-prem). 312
Events, responses, and Web Control. 312
Monitoring Adaptive Threat Protection activity. 313
Dashboards, monitors, and Adaptive Threat Protection. 313
Queries, reports, and Adaptive Threat Protection. 315

Server tasks and Adaptive Threat Protection. 318
Roll up system or event data for Trellix ENS (Trellix ePO - On-prem). 320
Events, responses, and Adaptive Threat Protection. 320
Navigating the Story Graph. 321
Disable a rule that triggered a detection for a known safe file. 325
Checking recent events for threats. 326
Check details about recent threat events. 327
Respond to events. 327
Using on a client system. 328
Using the Trellix Endpoint Security (ENS) Client. 328
How the Trellix Endpoint Security (ENS) Client works. 328
Open the Trellix Endpoint Security (ENS) Client. 328
Get information about your protection. 328
Checking for threats. 329
Check the content date and version on a client system. 329
Update content and software manually. 330
Using Threat Prevention on a client system. 330
Check the content date and version on a client system. 330
Update content and software manually. 331
Responding to prompts and threat detections. 331
Respond to a scan prompt. 331
Respond to a threat-detection prompt. 332
View and respond to threats detected on a client system. 333
Manage quarantined items on a client system. 334
How Threat Prevention provides maximum protection when rescanning quarantined items. . . 335
Scanning for threats. 336
Scan a specific file or folder on a client system. 336
Scan susceptible areas on a client system. 337
Scan a client system that might be infected. 338
Disable Trellix ENS scanners from the Trellix system tray. 339

Using Firewall on a client system. . . . 340
Enable and disable Firewall from the Trellix system tray icon. . . . 340
Enable or view Firewall timed groups from the Trellix system tray icon. . . . 340
Using Web Control on a client system. . . . 340
Enable the Web Control plug-in from the browser on a client system. . . . 340
Get information about a site that you're viewing. . . . 342
Get information about a site from search results. . . . 343
Using Adaptive Threat Protection on a client system. . . . 343
Check the content date and version on a client system. . . . 343
Update content and software manually. . . . 343
Respond to a file-reputation prompt. . . . 344
Disable Trellix ENS scanners from the Trellix system tray. . . . 345
Restore quarantined objects on a client system. . . . 345
Check connection status. . . . 346
Managing on a client system. . . . 347
Managing common features on a client system. . . . 347
Log on as administrator. . . . 347
Disable and enable features. . . . 347
Protect services and files on a client system. . . . 348
Set up logging for client activity on a client system. . . . 348
Control access to the client interface on a client system. . . . 349
Restricting and allowing access to features. . . . 349
Unlock the client interface on a client system. . . . 350
Configure proxy server settings on a client system. . . . 350
Keeping your protection up to date. . . . 351
Configure automatic updates for the client. . . . 351
Configure where the client gets its updates. . . . 351
Configure default behavior for updates from the client. . . . 352
Configure, schedule, and run update tasks from the client. . . . 353
Configure, schedule, and run mirror tasks. . . . 353

Allow certificate authentication on a client system. 353
Managing Threat Prevention on a client system. 354
Handling new malware with Extra.DAT files on a client system. 354
Download and load an Extra.DAT file on a client system. 354
Change the AMCore content version on a client system. 355
Specify quarantine location and retention time on a client system. 355
Preventing threats from accessing systems. 356
Protect files, registry, processes, and services with Access Protection rules on a client system. 357
Prevent Access Protection from blocking trusted programs on a client system. 358
Configure Exploit Prevention settings to block threats on a client system. 359
Exclude items from Exploit Prevention protection on a client system. 360
Get the signer distinguished name to exclude executables on a client system. 360
Scanning for threats on client computers. 361
Types of scans. 361
Configure settings for all scans on a client system. 364
Define which potentially unwanted programs to detect on a client system. 364
Enable potentially unwanted program detection on a client system. 365
Configure scans that run automatically when files are accessed on a client system. 366
Configure Threat Prevention with no connection to Trellix GTI on a client system. 366
Configure, schedule, and run scans on a client system. 367
Configure predefined scans that can be run manually or scheduled on a client system. 368
Best practices: Reducing the impact of on-demand scans on users on a client system. 369
Managing Firewall on a client system. 372
Enable and configure Firewall on a client system. 372
Block DNS traffic on a client system. 372
Define networks to use in rules and groups on a client system. 373
Exclude network addresses from a Trellix GTI lookup on a client system. 374
Configure trusted executables on a client system. 374
Get the signer distinguished name to specify trusted executables on a client system. 375
Create and manage Firewall rules and groups on a client system. 376

Wildcards in firewall rules. 377
Create connection isolation groups on a client system. 380
Create timed groups on a client system. 381
Managing Web Control on a client system. 382
Enable Web Control and configure its options on a client system. 382
Specify rating actions and block site access based on web category on a client system. 384
Using safety ratings to control access. 385
Using web categories to control access. 385
Managing Adaptive Threat Protection on a client system. 385
Handling new false positives with Extra.DAT files. 385
Download and load an Extra.DAT file on a client system. 386
Containing applications dynamically on a client system. 386
Enable the trigger threshold for Dynamic Application Containment on a client system. 387
Configure Trellix-defined containment rules on a client system. 387
Manage contained applications on a client system. 388
Prevent Dynamic Application Containment from containing trusted programs on a client system. . . 388
Get the signer distinguished name to exclude executables on a client system. 389
Configure Adaptive Threat Protection on a client system. 390
Exclude processes from Adaptive Threat Protection scanning on a client system. 390
Configure Adaptive Threat Protection with no connection to Trellix GTI on a client system. 391
Monitoring activity on a client system. 393
Monitoring your protection on a client system. 393
Check the Event Log for recent activity. 393
Log file names and locations. 393
Monitoring Threat Prevention activity on a client system. 395
Check the Event Log for recent activity. 395
Threat Prevention log file names and locations. 395
Monitoring Firewall activity on a client system. 397
Check the Event Log for recent activity. 397
Firewall log file names and locations. 397

Monitoring Web Control activity on a client system. . . . 398
Check the Event Log for recent activity. . . . 398
Web Control log file names and locations. . . . 398
Monitoring Adaptive Threat Protection activity on a client system. . . . 399
Check the Event Log for recent activity. . . . 399
Disable the Story Graph on a client system. . . . 400
Adaptive Threat Protection log file names and locations. . . . 400
Using the command line interface. . . . 402
On-demand scan command line interface. . . . 403
Custom on-demand scan command line interface. . . . 406
Update command line interface. . . . 414
Using Expert Rules. . . . 415
What are Expert Rules. . . . 415
How Expert Rules work. . . . 417
Expert Rules to protect files. . . . 417
Create Expert Rules to protect Files using ePO. . . . 417
Create Expert Rules to protect Files on a client system. . . . 418
Expert Rule syntax to protect Files. . . . 419
Sample Expert Rules to protect files. . . . 421
Match Loaded_DLLs with AND/OR check. . . . 421
Prevent file creation in a network path. . . . 421
Prevent file creation. . . . 422
Detect InstallUtil execution. . . . 424
Manage users from creating symbolic links and junctions. . . . 424
Expert Rules to protect processes. . . . 426
Create Expert Rules to protect processes using ePO. . . . 426
Create Expert Rules for processes on client system. . . . 427
Expert Rule syntax to protect processes. . . . 427
Sample Expert Rules to protect Processes. . . . 431
Prevent notepad execution. . . . 431

Block specific PowerShell parameters. . . . 432
Trigger a process scan. . . . 432
Expert rules to protect Registry. . . . 434
Create Expert Rules to protect registry using ePO. . . . 434
Create Expert Rules for registry on client system. . . . 435
Expert Rule syntax to protect registry. . . . 436
Sample Expert Rules to protect registry. . . . 440
Prevent changing registry value. . . . 440
Prevent DLL injection through AppInit_DLLs. . . . 440
Detect exporting SAM from registry. . . . 442
Expert rules to protect Buffer overflow. . . . 443
Create Expert Rules to prevent Buffer Overflow using ePO. . . . 443
Create Expert Rules for Buffer Overflow on client system. . . . 443
Sample Expert Rule to prevent Buffer Overflow. . . . 444
Expert rules to protect Illegal API use. . . . 445
Create Expert Rules to prevent Illegal API use using ePO. . . . 445
Create Expert Rules for Illegal API Use on client system. . . . 446
Sample Expert Rule to prevent Illegal API Use. . . . 447
Expert rules to protect Services. . . . 447
Create Expert Rules to protect Services using Trellix ePO - On-prem. . . . 447
Create Expert Rules to protect Services on client system. . . . 448
Sample Expert Rule to protect Services. . . . 449
Validate and enforce an Expert Rule on a client system. . . . 450
Learn Expert Rules for files, processes, and registry. . . . 451
AAC rule structure. . . . 451
Expert Rule commands. . . . 451
Rule command. . . . 451
Initiator command. . . . 452
Process command. . . . 452
Target command. . . . 453

Next_Process_Behavior command. 453
Match command. 454
Include and Exclude commands. 454
AggregateMatch command. 457
Reaction SCAN command. 457
How match criteria in AAC-based subrules are evaluated. 461
Valid parent-child relationships between AAC commands. 462
Match object type values. 463
Match type values. 464
OBJECT_NAME guidelines. 483
ACCESS_MASK flags. 486
Commands to query system state. 491
iDump command. 491
iEnv command. 492
iList command. 492
iReg command. 493
iSystem command. 495
iTerminate command. 496
iUser command. 497
iUtil command. 497
Learn Expert Rules for Buffer overflow, Illegal API use and Services. 498
Legacy McAfee Host IPS rule structure. 498
Legacy Syntax. 498
Wildcards. 498
Environment variables. 499
Using the Include and Exclude keywords. 499
Sections that are common to all class types. 500
Class types. 503
Buffer Overflow class type. 503
Illegal API Use class type. 505

Services class type. 506
Troubleshooting Expert rules. 508

Product overview

Overview of Trellix Endpoint Security (ENS)

Trellix Endpoint Security (ENS) protects servers, computer systems, laptops, and tablets against known and unknown threats. These threats include malware, suspicious communications, unsafe websites, and downloaded files.

Trellix ENS enables multiple defense technologies to communicate in real time to analyze and protect against threats.

Trellix ENS consists of these security modules:

- **Threat Prevention** — Prevents threats from accessing systems, scans files automatically when they are accessed, and runs targeted scans for malware on client systems.
- **Firewall** — Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications.
- **Web Control** — Monitors web searching and browsing activity on client systems and blocks websites and downloads based on safety rating and content.
- **Adaptive Threat Protection** — Analyzes content from your enterprise and decides how to respond based on file reputation, rules, and reputation thresholds.

The Common module provides settings for common features, such as interface security and logging. This module is installed automatically if any other module is installed.

All modules integrate into a single Trellix ENS interface on the client system. Each module works together and independently to provide several layers of security.

How Trellix ENS works

Trellix ENS intercepts threats, monitors overall system health, and reports detection and status information. Client software is installed on each system to perform these tasks.

Typically, you install one or more Trellix ENS modules on client systems, manage detections, and configure settings that determine how product features work.

Trellix ePO - On-prem

You use Trellix ePO - On-prem to deploy and manage Trellix ENS modules on client systems.

Each module includes an extension and a software package that are installed on the Trellix ePO - On-prem server. Trellix ePO - On-prem then deploys the software to client systems. Trellix ePO - On-prem.

Using Trellix Agent, the client software communicates with Trellix ePO - On-prem for policy configuration and enforcement, product updates, and reporting.

Client modules

The client software protects systems with regular updates, continuous monitoring, and detailed reporting.

It sends data about detections on your computers to the Trellix ePO - On-prem server. This data is used to generate reports about detections and security issues on your computers.

TIE server and Trellix DXL

The Trellix ENS framework integrates with Trellix Threat Intelligence Exchange (TIE) and Trellix® Data Exchange Layer when using Adaptive Threat Protection. These optional products enable you to control file reputation locally and share the information immediately throughout your environment.

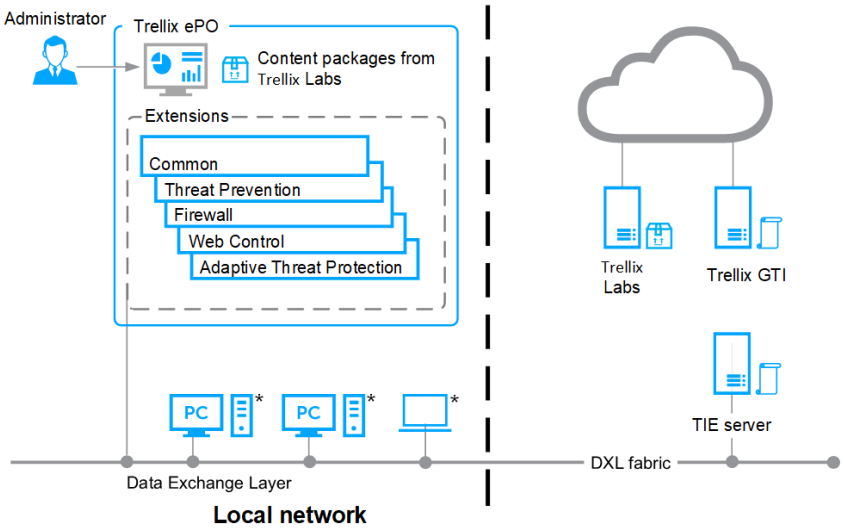
Trellix GTI

Threat Prevention, Firewall, Web Control, and Adaptive Threat Protection query Trellix Global Threat Intelligence for reputation information to determine how to handle files on the client system.

Trellix Labs

The client software communicates with Trellix Labs for content file and engine updates. Trellix Labs regularly releases updated content packages.

How it works



* Client modules: Common, Threat Prevention, Firewall, Web Control, and Adaptive Threat Protection

How your protection stays up to date

Regular updates of Trellix ENS protect your computers from the latest threats.

To perform updates, the client software connects to a local or remote Trellix ePO - On-prem server or directly to a site on the Internet. Trellix ENS checks for:

- Updates to the content files that detect threats. Content files contain definitions for threats such as viruses and spyware, and these definitions are updated as new threats are discovered.
- Upgrades to software components, such as updates and hotfixes.

Threat Prevention

Overview of Threat Prevention

Trellix Endpoint Security (ENS) Threat Prevention blocks threats from accessing systems, scans files automatically when they are accessed, and runs targeted scans for malware on client systems.

Threat Prevention detects threats based on security content files. Security content updates are delivered automatically to target specific vulnerabilities and block emerging threats from executing.

Threat Prevention protects your environment from the following:

- Viruses, worms, and trojan horses
- Access point violations — unwanted changes to files, shares, registry keys, registry values, and preventing or restricting processes and services from executing threat behavior.
- Buffer overflow exploits
- Illegal API use — malicious API calls being made by unknown or compromised application
- Network intrusions, such as network denial-of-service attacks and bandwidth-oriented attacks
- Potentially unwanted code and programs
- Vulnerability focused threats
- Zero-day exploits
- Threats in non-browser-based scripts, such as PowerShell, JavaScript, and VBScript

You use Trellix ePO - On-prem to deploy and manage Threat Prevention on client systems.

Key features of Threat Prevention

The key features of Threat Prevention protect against threats entering your environment, detect malware in your environment, and correct issues by cleaning or repairing infected files.

Protect

Protect your systems from intrusions before they gain access to your environment using these Threat Prevention features.

- **Access Protection** — Protect against unwanted changes to client systems by restricting access to specified files, shares, registry keys, registry values, and preventing or restricting processes and services from executing threat behavior.
- **Exploit Prevention** — Threat Prevention uses signatures in content updates to protect against these exploits:
    - **Buffer Overflow Protection** — Stop exploited buffer overflows from executing arbitrary code.
    - **Illegal API Use** — Protect against malicious API calls being made by unknown or compromised applications running on the system.
    - **Network Intrusion Prevention (Network IPS)** — Protect against network denial-of-service attacks and bandwidth-oriented attacks that deny or degrade network traffic.

    - **Expert Rules** — Provide additional parameters and allow more flexibility than the Access Protection custom rules. But, to create Expert Rules, you must understand the Trellix proprietary syntaxes.
- **Command line interface** — Run Full Scan, Quick Scan, custom on-demand scans, and update security content from the command line or as part of a batch file.

Detect

Detect threats when they occur in your environment using these Threat Prevention features.

- **On-Access Scan** — Scan for threats as files are read from, or written to, disk. Integrates with Antimalware Scan Interface (AMSI) to provide enhanced scanning for threats in non-browser-based scripts.
- **On-Demand Scan** — Run or schedule predefined scans, including scans of spyware-related registry entries that weren't previously cleaned. Run scans only when the system is idle. Restrict CPU usage to optimize scan performance.
- **Potentially Unwanted Programs** — Detect potentially unwanted programs, such as spyware and adware, and prevent them from running in your environment.
- **Quarantine** — Quarantine infected items, attempt to clean or repair them, or automatically delete them.
- **Dashboards and monitors** — Display statistics about Threat Prevention, including scan duration, content update status, and applications with the most exploits. (Managed systems)
- **Queries and reports** — Retrieve detailed information about Threat Prevention, including threat count, scan completion, detection response, false positive mitigation events, and Trellix GTI sensitivity level. (Managed systems)
- **Early Launch Anti-Malware** — Support the ELAM feature included with Windows 8 and later releases. ELAM collects the list of device drivers loaded during the boot cycle and scans them once the scanning services are running.

Correct

Correct security issues, handle detections, improve performance, and enhance protection using these Threat Prevention features.

- **Actions** — Take the specified action when detections occur.
- **Alerts** — Notify when detections occur and limit traffic with filters.
- **Extra.DAT files** — Protect against new threats, such as a major virus outbreak. Trellix ePO - On-prem
- **Scheduled scans** — Run scans during nonpeak times to improve system and scan performance.
- **Content repositories** — Reduce network traffic over the enterprise Internet or intranet by moving the content file repository closer to client systems. (Managed systems)
- **Log files** (Trellix Endpoint Security (ENS) Client) — Provide a history of detected items, which you can use to determine if you need to change settings to enhance protection or improve system performance.
- **Dashboards and monitors** — Review activity and use that information to tune Threat Prevention settings. (Managed systems)

How Threat Prevention works

Threat Prevention has two components: an extension installed on the Trellix ePO - On-prem server and the protection software itself, including the scan engine and content files, installed on the client system. Threat Prevention includes the protection software itself and the scan engine and content files installed on the client system.

Also installed on the client system is Trellix Endpoint Security (ENS) Common, which includes the Trellix Endpoint Security (ENS) Client.

Using Trellix Agent, the client software communicates with Trellix ePO - On-prem for configuration and reporting, Trellix Global Threat Intelligence for reputation information, and Trellix Labs for content file and engine updates.

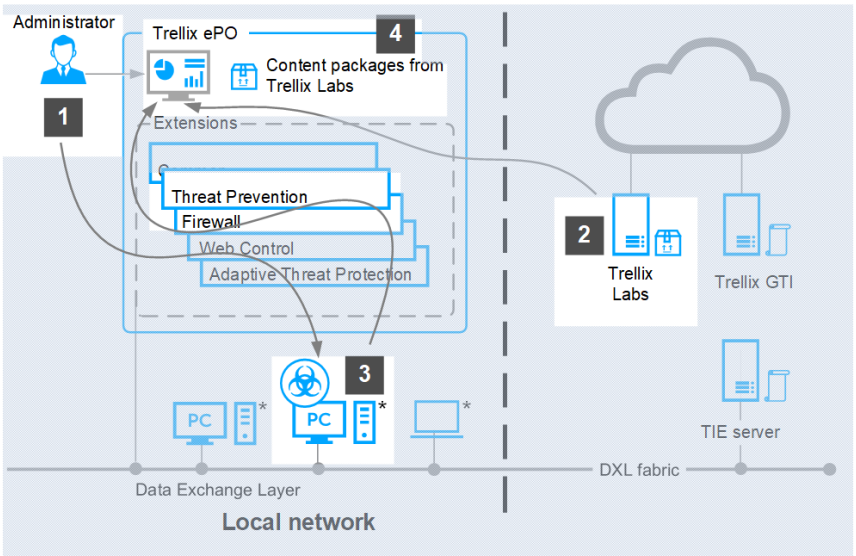
Using Trellix Agent, the client software communicates with Trellix Global Threat Intelligence for reputation information and Trellix Labs for content file and engine updates.

Workflow example — Access Protection

Threat Prevention follows this basic process to protect files, registry keys, registry values, processes, and services.

1. If managed, the administrator configures protection rules in the **Access Protection** policy and enforces it to the client system.
2. The administrator configures protection rules in the **Access Protection** policy in Trellix ePO - On-prem and enforces it to the client system.
3. The administrator downloads the latest content files from Trellix Labs.
4. A user downloads a legitimate program (not malware), MyProgram.exe, from the Internet and runs the program. MyProgram.exe starts and also starts a child process called AnnoyMe.exe. AnnoyMe.exe tries to change the operating system to make sure that AnnoyMe.exe always loads on startup. Threat Prevention processes the request and matches the action against an existing Trellix-defined or user-defined protection rule. Threat Prevention prevents AnnoyMe.exe from changing the operating system.
5. Threat Prevention logs the details. Threat Prevention logs the details, then generates and sends an event to Trellix ePO - On-prem.

How it works



* Client modules: Common, **Threat Prevention**, Firewall, Web Control, and Adaptive Threat Protection

Client system

In addition to Threat Prevention, the client system includes:

- **Content files** (including AMCore content, also called malware signatures, Access Protection, and Exploit Prevention content) — Works with the scan engine to identify and handle threats.
- **Scan engine** — Scans the files, folders, and disks on the client system and compares the results to the known virus information in the content files.
- **Trellix Agent** — Provides secure communication between managed products and the Trellix ePO - On-prem server.
- **Trellix Endpoint Security (ENS) Common** — Provides services, such as updating, logging, reporting events and properties, task scheduling, communication, and storing settings.

Trellix ePO - On-prem

The Trellix ePO - On-prem server uses these components to manage and update client systems remotely:

- **Trellix ePO - On-prem** — Manages and enforces Threat Prevention policies from a central location and provides queries and dashboards to track activity and detections.
- **Content repository** — Retrieves the content updates from the Trellix download site. Using a content repository in your organization, you can copy content files automatically and minimize bandwidth.

Trellix server

Trellix, home to Trellix Labs and Trellix support, provides the following services.

- **Trellix Labs** (Threat Library) — Researches and stores detailed information about malware and potentially unwanted programs, including how to handle them.
- **Trellix GTI** (heuristic network check for suspicious files) — Looks for suspicious programs and DLLs running on client systems that Threat Prevention protects. The Trellix GTI feature sends the fingerprint of each suspicious file to Trellix Labs for analysis and response.
- **Content and engine updates** — Provides protection against specific vulnerabilities and blocks emerging threats (including buffer-overflow attacks) from executing.

Firewall

Overview of Firewall

Trellix Endpoint Security (ENS) Firewall protects systems, network resources, and applications from external and internal attacks.

Firewall scans all incoming and outgoing traffic and compares it to its list of firewall rules, which is a set of criteria with associated actions. If a packet matches all criteria in a rule, the firewall acts according to the rule, blocking or allowing the packet through the firewall.

You use Trellix ePO - On-prem to deploy and manage Firewall on client systems.

Key features of Firewall

The key features of Firewall protect against threats, detect security issues, and correct false positives.

Protect

Protect your network and applications using these Firewall features:

- **Rules** — Define the criteria Firewall uses to determine whether to block or allow incoming and outgoing traffic.
- **Rule groups** — Organize firewall rules for easy management, enabling you to apply rules manually or on a schedule, and to only process traffic based on connection type.
- **Stateful packet filtering and inspection** — Track network connection state and characteristics in a state table, allowing only packets that match a known open connection.
- **Reputation-based control** — Block untrusted executables, or all traffic from an untrusted network, based on reputation.

Detect

Detect security issues using these Firewall features:

- **Dashboards and monitors** — Display intrusion and detection events from Trellix GTI and Firewall.
- **Queries and reports** — Retrieve detailed information about Firewall, including client rules, errors, intrusion and block events, and save that information in reports.
- **Alerts** — Display alerts for blocked traffic, based on executable or network reputation.
- **Log traffic** — Log all blocked or allowed traffic.

Correct

Reduce or eliminate false positives using these Firewall features:

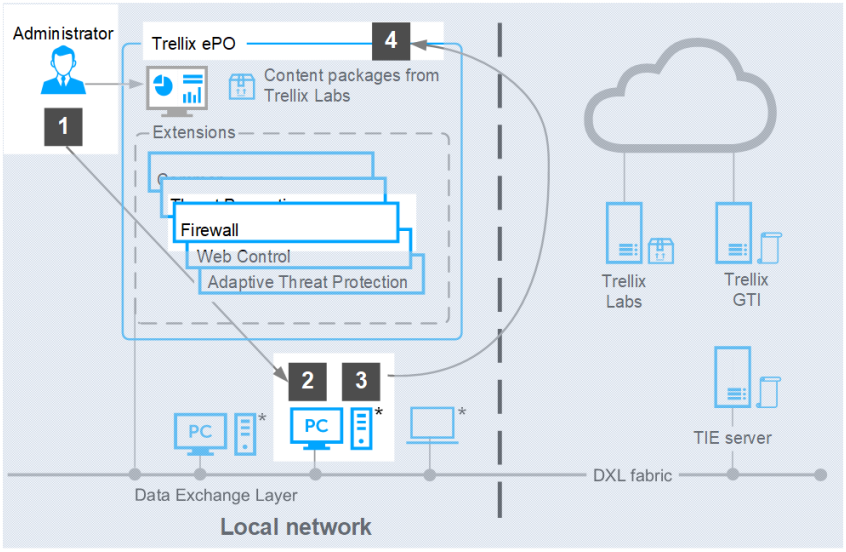
- **Adaptive mode** — Create rules automatically on the client system to allow legitimate activity. Once created, analyze client rules to decide which to convert to server-mandated policies.
- **Defined networks** — Define trusted networks to allow traffic from networks that your organization considers safe.
- **Trusted executables** — Maintain a list of safe executables to reduce false positives.
- **Firewall Catalog** — Define rules and groups to add to multiple policies, or networks and applications to add to firewall rules.
- **Client options** — Allow users to disable Firewall temporarily for troubleshooting.
- **Dashboards and monitors** — Monitor activity and intrusion detections, then use that information to tune Firewall settings.

How Firewall works

Firewall scans all incoming and outgoing traffic at the packet level and compares packets to the configured firewall rules to determine whether to allow or block the traffic.

1. The administrator configures firewall rules in Trellix ePO - On-prem and enforces the policy to the client system.
2. If managed, the administrator configures firewall rules in Trellix ePO - On-prem and enforces the policy to the client system.
3. The user performs a task that initiates network activity and generates traffic.
4. Firewall scans all incoming and outgoing traffic and compares packets to configured rules. If the traffic matches a rule, Firewall blocks or allows it, based on the rule criteria.
5. Firewall logs the details. Firewall logs the details, then generates and sends an event to Trellix ePO - On-prem.

How it works



* Client modules: Common, Threat Prevention, **Firewall**, Web Control, and Adaptive Threat Protection

Web Control

Overview of Web Control

Trellix Endpoint Security (ENS) Web Control monitors web searching and browsing activity on client computers. It protects against threats on webpages and in file downloads.

A Trellix team analyzes each website and assigns a color-coded safety rating based on test results. The color indicates the level of safety for the site.

Web Control uses the test results to identify web-based threats. Software installed on the client system adds features that appear in the browser window and search results to notify users.

You use Trellix ePO - On-prem to deploy and manage Web Control on client systems. Settings control access to sites based on their safety rating, the type of content they contain, and their URL or domain name.

Settings control access to sites based on their safety rating and the type of content they contain.

Key features of Web Control

The key features of Web Control protect your systems from web-based threats, detect threats, and correct issues with file downloads.

Protect

Protect your systems from malicious websites and downloads using these Web Control features:

- **Block and Allow List** — Prevent users from visiting specific URLs or domains or always allow access to sites that are important to your business.
- **Rating Actions and Web Category Blocking** — Use safety ratings and web categories defined by Trellix to control user access to sites, pages, and downloads.
- **Secure Search** — Automatically block risky sites from appearing in search results based on their safety rating.
- **Self protection** — Prevent users from disabling the Web Control plug-in or uninstalling or changing Web Control files, registry keys, registry values, services, and processes.

Detect

Detect malicious websites using these Web Control features:

- **Web Control button in the browser window** — The Web Control plug-in displays a button indicating the safety rating for the site. Click the button for more information about the site.
- **Web Control icon on search results pages** — An icon appears next to each listed site. The color of the icon indicates the safety rating for the site. Hover over the icon for more information about the site.
- **Site reports** — Details show how the safety rating was calculated based on types of threats detected, test results, and other data.
- **Dashboards and monitors** — Display statistics about Web Control activity, including visits and downloads from sites by rating, content type, and blocked or allowed list.
- **Queries and reports** — Retrieve detailed information about Web Control browser events, and save it in reports.

Correct

Monitor and tune Web Control behavior using these features:

- **Interlock with other Trellix products** — Disable Web Control automatically if it detects a web gateway appliance or if Skyhigh Client Proxy is installed *and* in redirection mode.
- **File scanning for file downloads** — Web Control sends files to Threat Prevention for scanning. If it detects a threat, Threat Prevention responds with the configured action such as clean, and alerts the user.
- **Dashboards and monitors** — Monitor activity to understand browsing activity, then use that information to tune Web Control settings.
- **Exclusions** — Prevent Web Control from rating or blocking specific IP addresses.

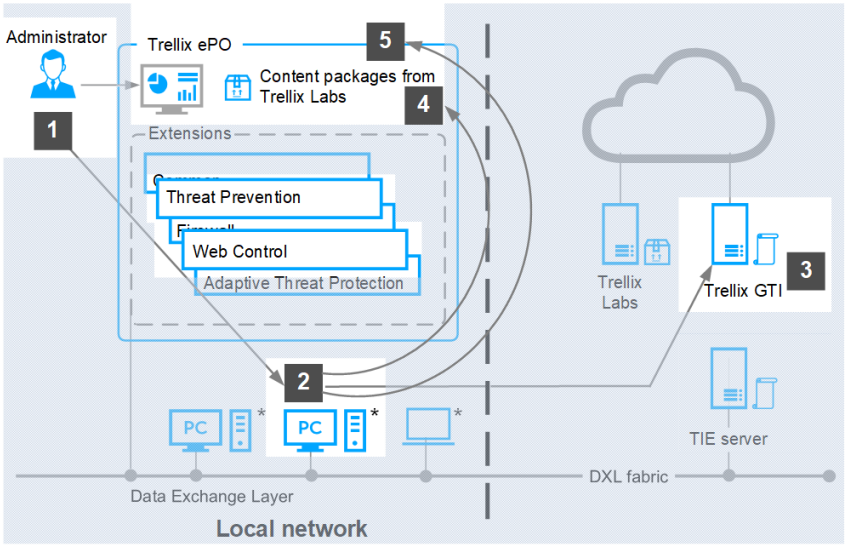
How Web Control works

Web Control queries Trellix GTI for reputation information to determine how to handle navigation to URLs.

1. The administrator configures Web Control settings in Trellix ePO - On-prem and enforces the policy to the client system.
2. If managed, the administrator configures Web Control settings in Trellix ePO - On-prem and enforces the policy to the client system.
3. The user visits or accesses a resource from a website.
4. Web Control requests the URL reputation from Trellix GTI .
    - If the URL reputation is green, Web Control allows navigation to the URL and displays the page. Otherwise, Web Control navigates to either the block or warn page, based on settings.
    - If the URL reputation is unrated but matches a category in Trellix GTI , Web Control allows or blocks navigation to the URL, based on **Content Actions** settings.

5. If the request is a file download and the file reputation is not malicious, Web Control allows the download, even if the URL reputation is malicious. If the file reputation is unknown, Web Control sends the file to Threat Prevention for scanning by the on-demand scanner. Threat Prevention checks the file against the AMCore content file. If it matches a signature or hash in content, the file download is blocked. Otherwise, the file is downloaded.
6. Web Control logs the details. Web Control logs the details, then generates and sends an event to Trellix ePO - On-prem.

How it works



* Client modules: Common, Threat Prevention, Firewall, **Web Control**, and Adaptive Threat Protection

Web Control and Skyhigh Client Proxy

When Web Control is disabled because Client Proxy is present and redirecting:

- Web Control ignores rating and enforcement actions.
- Web Control browser controls are disabled.
- Trellix Endpoint Security (ENS) Client **Status** page shows Web Control status as **Disabled**.
- Trellix Endpoint Security (ENS) Client **Settings** page indicates that Web Control is disabled because Client Proxy is detected.

Adaptive Threat Protection

Overview of Adaptive Threat Protection

Trellix Endpoint Security (ENS) Adaptive Threat Protection examines your enterprise content and decides what to do based on file reputation, rules, and reputation thresholds.

Adaptive Threat Protection provides these benefits:

- Fast detection and protection against security threats and malware.

- The ability to know which systems or devices are compromised, and how the threat spread through your environment.
- The ability to immediately clean specific files based on their threat reputations and your risk criteria.
- Integration with Real Protect scanning to perform automated behavior analysis in the cloud and on client systems.
- Credential Theft Protection (CTP) safeguards the Local Security Authority Subsystem Service (LSASS.exe) from potential hacker threats. Processes which unexpectedly attempt to access the Microsoft LSASS.exe process for credentials will have that action blocked and an event will be sent to Trellix ePO - On-prem.
- Enhanced script scanning, including integration with Antimalware Scan Interface (AMSI).
- The ability to identify fileless attack methods in which no persistent malware file exists.
- The ability to monitor unknown processes and automatically remediate changes to the system.
- Real-time integration with Sandbox server, Adaptive Threat Protection, and Trellix Threat Intelligence Exchange enables submission of unknown files during file creation and execution. This returns detailed file assessment and data on reputation and malware classification. The integration allows you to respond to threats and share the information throughout your environment.

For more threat intelligence sources and functionality, deploy the Trellix Threat Intelligence Exchange (TIE) server. For information, contact your reseller or sales representative.

Optional components

Adaptive Threat Protection can integrate with these optional components:

- **TIE server** — A server that stores information about file and certificate reputations, and additional metadata, then shares that information with other systems.
- **Trellix DXL** — Clients and brokers that enable bidirectional communication between the Adaptive Threat Protection module on the managed system and the TIE server. Trellix DXL is optional, but it is required for communication with the TIE server.

These components include Trellix ePO - On-prem extensions that add several features and reports.

Key features of Adaptive Threat Protection

The key features of ATP protect your enterprise from files with unknown reputations, detect malicious patterns, and correct false positives.

Protect

Protect your enterprise by blocking or containing files with unknown reputations using these ATP features:

- **Reputation-based file handling** — ATP alerts when an unknown file enters the environment. Instead of sending the file information to Trellix for analysis, ATP can block the file immediately.
- **Integration with the TIE server** — If available, the TIE server provides information about how many systems ran the file. Sandbox server helps determine whether the file is a threat.
- **Dynamic Application Containment** — Allows unknown files to run in a container, limiting the actions they can take. When a company first uses a file whose reputation is not known, ATP can run it in a container. Containment rules define which actions the contained application can't perform. Dynamic Application Containment also contains processes when they load PE files (Portable Executables) and DLLs (Dynamic Link Libraries) that downgrade the process reputation.

Detect

Detect malicious patterns and malware in memory using these ATP features:

- **Real Protect scanning** — Performs automated behavior analysis. Real Protect inspects suspicious files and activities on a client system and detects malicious patterns using machine-learning techniques. Real Protect client-based and cloud-based scans include DLL scanning to keep trusted processes from loading untrusted PE and DLL files.
- **Credential Theft Protection** — Protects against credential theft. The credential theft protection technology is designed to cease attacks specifically targeting the Local Security Authority Subsystem Service (LSASS).
- **Enhanced script scanning** — Integration with AMSI (Antimalware Scan Interface) provides enhanced scanning for threats in non-browser-based scripts, such as PowerShell, JavaScript, and VBScript.
- **ATP rules** — Determines what processes can and can't do within a specific context and can change reputation based on the context and behavior.

Correct

Clean files and eliminate false positives using these ATP features:

- **File cleaning** — ATP can clean files when the file reputation reaches a specified threshold.
- **Enhanced remediation** — If a process is unknown, enhanced remediation monitors its behavior and logs all files that the process creates and, optionally, all files that the process changes or deletes. If a monitored process exhibits malicious behavior, enhanced remediation stops the process, its children, and ancestors, and rolls back the changes that it made, restoring the system as close as possible to its original state before the process ran.
- **Custom file exclusions** — If a custom file is trusted, but has a default reputation of malicious, it is blocked. You can exclude it from scanning or change the file's reputation to trusted and allow it to run in the organization without requesting an updated DAT file from Trellix.
- **False positive mitigation**:
    - If ATP gets a file reputation above a certain threshold from the TIE server or Trellix GTI , it can automatically override a false positive detection by Adaptive Threat Protection or Threat Prevention.
    - If Adaptive Threat Protection determines that a detection is a false positive, Trellix Labs might release a negative Extra.DAT file to suppress the detection until the next content update.
- **Adaptive Threat Protection rules** — Trellix delivers updates to rules in AMCore content every month.
- **Trellix ePO - On-prem Dashboards and reports** — Show activity and detections, which you can use to tune Adaptive Threat Protection settings. (Managed systems)

How Adaptive Threat Protection works

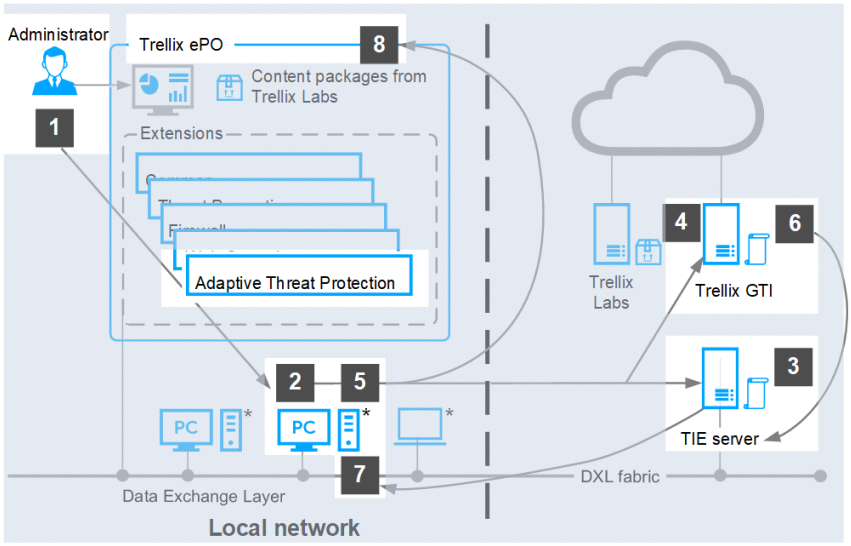
Adaptive Threat Protection uses the local reputation cache, the TIE server, and Trellix GTI for reputation information to determine how to handle files and processes on the client system. ATP uses rules to target live-off-the-land and fileless attacks, and enhanced remediation to roll back changes if attacks occur.

1. (Managed systems) The administrator configures ATP settings in Trellix ePO - On-prem and enforces it to the client system.
2. A user executes a file on the client system. Adaptive Threat Protection checks the local reputation cache for the file.
3. If the file is not in the local reputation cache, ATP queries the TIE server, if available, for the reputation.
4. If the file is not in the TIE server database, the TIE server queries Trellix GTI for the reputation. If the TIE server is not available, ATP queries Trellix GTI for the reputation.

5. Depending on the file's reputation and ATP settings:
    - The file is allowed to run.
    - The file is cleaned.
    - The file is blocked.
    - The file is allowed to run in a container.
    - The user is prompted for the action to take.

    For a process with a **Known Trusted** reputation, Adaptive Threat Protection rules determine the appropriate actions for the process. ATP monitors the process, its children, and ancestors for suspicious behavior, which can indicate a fileless attack, and blocks the process if needed. If the process reputation is **Unknown** (50) or lower, enhanced remediation backs up changes, and rolls back if the process exhibits malicious behavior.
6. Trellix GTI returns the latest file reputation information to the TIE server.
7. The TIE server updates the database and sends the updated reputation information to all ATP-enabled systems to immediately protect your environment.
8. ATP logs the details then, if managed, generates and sends an event to Trellix ePO - On-prem.

How it works



* Client modules: Common, Threat Prevention, Firewall, Web Control, and **Adaptive Threat Protection**

The way Adaptive Threat Protection functions depends on whether it communicates with the TIE server and whether it is connected to the Internet and connects directly to Trellix GTI .

If TIE server and Trellix DXL are present (Managed systems)

If the TIE server is present, Adaptive Threat Protection uses the Trellix DXL framework to share file and threat information instantly across the whole enterprise. You can see the specific system where a threat was first detected and where it went from there, and stop it immediately.

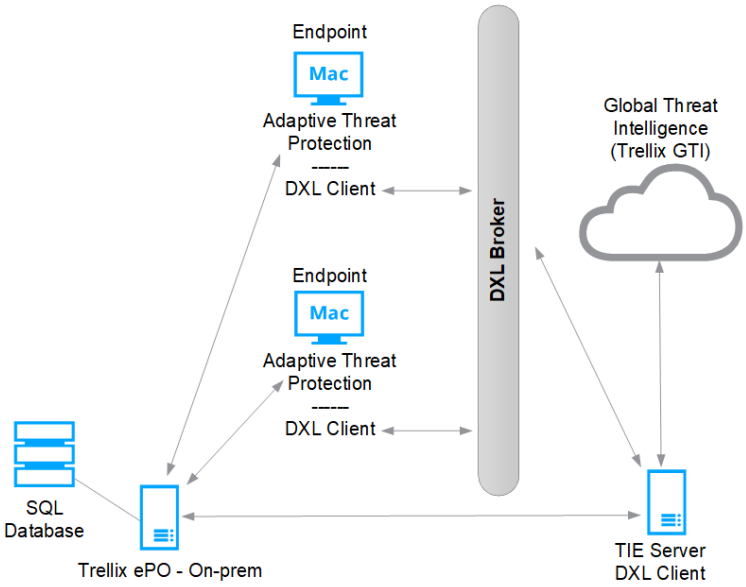
Adaptive Threat Protection with the TIE server enables you to control file reputation at a local level, in your environment. You decide which files can run and which are blocked, and the Trellix DXL shares the information immediately throughout your environment.

Note

To prevent business operations from being negatively impacted, Trellix might ignore some reputations in the TIE server, such as setting a Microsoft certificate to **Known Malicious**.

Adaptive Threat Protection and the TIE server communicate file reputation information and file metadata. The Trellix DXL framework immediately passes that information to managed endpoints. It also shares information with other Trellix products that access the Trellix DXL , such as Trellix Enterprise Security Manager and Trellix Intrusion Prevention System.

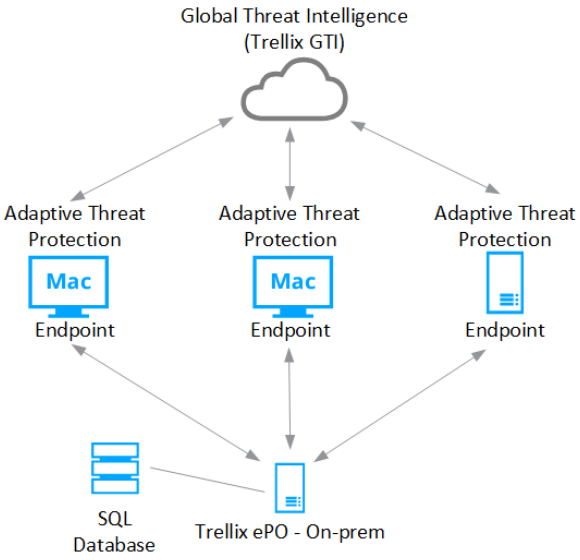
Adaptive Threat Protection with TIE server and Trellix DXL



If the TIE server and Trellix DXL are not present (Managed systems)

Adaptive Threat Protection communicates with Trellix GTI for file reputation information.

Adaptive Threat Protection with Trellix ePO - On-prem and Trellix GTI

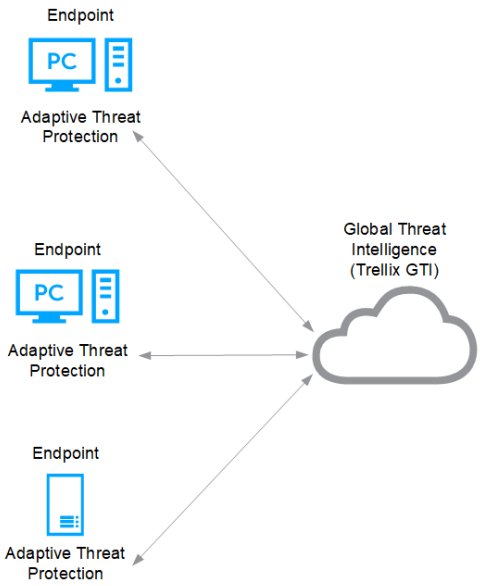


If the TIE server isn't present and the system isn't connected to the Internet, Adaptive Threat Protection determines the file reputation using ATP rules on the local system.

If TIE server and Trellix DXL are not present (Self-managed systems)

Adaptive Threat Protection communicates with Trellix GTI for file reputation information.

Adaptive Threat Protection with Trellix GTI



If the TIE server isn't present and the system isn't connected to the Internet, Adaptive Threat Protection determines the file reputation using ATP rules on the local system.

Feature overview

Threat Prevention

How content files work

When searching files for threats, the scan engine compares the contents of the scanned files to known threat information stored in the AMCore content files. Exploit Prevention uses its own content files to protect against exploits.

Trellix Labs finds and adds known threat information (signatures) to the content files. With the signatures, content files include information about cleaning and counteracting damage that the detected malware can cause. New threats appear, and Trellix Labs releases updated content files, regularly.

Caution

If the signature of a threat isn't in the installed content files, the scan engine can't detect that threat, leaving your system vulnerable to attack.

Trellix ENS stores the currently loaded content file and the previous two versions in the Program Files\Common Files\McAfee\Engine\content folder. If needed, you can revert to a previous version.

If new malware is discovered and extra detection is required outside of the regular content update schedule, Trellix Labs releases an Extra.DAT file. Trellix ePO - On-prem

AMCore content package

Trellix Labs releases AMCore content packages daily by 7:00 p.m. (GMT/UTC). If a new threat warrants it, daily AMCore content files might be released earlier and, sometimes, releases might be delayed.

To receive alerts regarding delays or important notifications, subscribe to the Support Notification Service (SNS). See KB67828.

The AMCore content package contains updates to the Threat Prevention scan engine and signatures based on results of ongoing threat research.

Tip

Best practice: For answers to frequently asked questions about AMCore content files (V3 DAT), see KB82396.

Exploit Prevention content package

The Exploit Prevention content package includes:

- **Memory protection signatures** — Generic Buffer Overflow Protection (GBOP), caller validation, Generic Privilege Escalation Prevention (GPEP), and Targeted API Monitoring.

- **Network Intrusion Prevention signatures** protect:
  - Systems located downstream in a network segment.
  - Servers and the systems that connect to them.
  - Against network denial-of-service attacks and bandwidth-oriented attacks that deny or degrade network traffic.
- **Access Protection signatures** — Files, Registry key, Registry value, Processes, and Services.
- **Application Protection List** — Processes that Exploit Prevention protects.

Exploit Prevention content is similar to the McAfee Host IPS content files. See KB51504. To view KB51504, you must first log on to the ServicePortal and then search the Knowledge Center for KB51504.

Trellix releases new Exploit Prevention content files once a month. To make sure that Threat Prevention uses the latest content files, retrieve these files from Trellix and update your systems regularly.

How false positive mitigation works

Trellix ENS and AMCore use false positive mitigation to prevent files from being incorrectly considered a threat (or convicted). This feature is available when either Threat Prevention or Adaptive Threat Protection are installed.

Some heuristic-based reputations providers might assess reputation scores that introduce false positives, such as when the reputation of a file is above **Unknown** (50), but below a trusted reputation level.

When Threat Prevention detects a threat, AMCore checks the reputation of the convicted file to determine whether to suppress the conviction. If the file has the reputation of **Might Be Trusted** (70) or higher, false positive mitigation suppresses the conviction. Trellix ENS also uses telemetry data in AMCore Content updates, which can include information from other sources, such as Trellix GTI and Trust DATs, to further mitigate false positives.

When false positive mitigation suppresses a conviction, Threat Prevention generates a False Positive Mitigation event (34928), displays it in the **Event Log** in Trellix Endpoint Security (ENS) Client, and sends it to the Trellix ePO - On-prem **Threat Event Log**.

False positive mitigation is always enabled by default. Disabling ATP or enabling ATP Observe mode doesn't disable false positive mitigation.

How application protection rules work

Application protection rules specify the processes that Exploit Prevention monitors for buffer overflow and illegal API use violations. Only processes in the **Application Protection Rules** list with the inclusion status of **Include** are monitored.

When a monitored process starts, Exploit Prevention injects its DLLs into the process to monitor it for buffer overflow and illegal API use violations.

The Exploit Prevention content provided by Trellix includes a list of applications that are protected. Threat Prevention displays these applications in the **Application Protection Rules** section of the **Exploit Prevention** settings page. To keep protection current, updates to Exploit Prevention content replace the Trellix-defined application protection rules in the **Exploit Prevention** settings with the latest application protection rules.

You can enable, disable, and change the inclusion status and executables of Trellix-defined application protection rules, but you can't delete them. You can also create and duplicate your own application protection rules. Any changes you make to these rules persist through content updates.

If the inclusion status of the application protection rule is:

- **Include** — Exploit Prevention injects its DLLs and monitors the process for violations. Protected applications include Microsoft applications such as PowerPoint, Outlook, Excel, web browsers, and known vulnerable processes such as svchost.exe and services.
- **Exclude** — Exploit Prevention doesn't inject its DLLs and doesn't monitor the process for violations.

  Note

  Setting the inclusion status to **Exclude** has the same effect as adding an exclusion in the **Exclusions** section and specifying only the process information.

  Typically, processes such as slsvc.exe and mcshield.exe, are excluded due to known compatibility or redundancy issues.

If the list includes conflicting application protection rules, **Exclude** status rules take precedence over **Include**.

Note

Trellix Endpoint Security (ENS) Client displays the complete list of protected applications, not just the applications currently running on the client system.

Application protection rules created in the Trellix Endpoint Security (ENS) Client are not sent to Trellix ePO - On-prem and might be overwritten when the administrator deploys an updated policy.

How signatures protect applications and systems

Signatures are collections of rules that compare behavior against known attacks and perform an action when a match is detected. Trellix delivers signatures in Exploit Prevention content updates.

When the Exploit Prevention content file is updated, the list of signatures is updated.

Signature types

Threat Prevention includes these signature types:

- **Files** signatures report or block operations such as renaming or executing, on specific files, paths, or drives.
- **Services** signatures report or block operations such as starting, stopping, or changing the startup mode, on services.
- **Registry** signatures report or block operations such as creating or deleting, on registry keys and registry values.
- **Processes** signatures report or block operations such as access or running, on processes.
- **Buffer Overflow** signatures report or block malicious programs inserted into the memory space exploited by an attack.
- **Illegal API Use** signatures report or block API calls that might result in malicious activity.

- **Network IPS** signatures report or block malicious data that flows between the system and the rest of the network.

Note

Buffer Overflow and Illegal API Use signatures protect specific processes, which are defined in the **Application Protection Rules** list. When an attack is detected, Exploit Prevention can stop the behavior initiated by the attack.

Behavioral rules

Behavioral rules block zero-day attacks and enforce proper operating system and application behavior. Heuristic behavioral rules define a profile of legitimate activity. Activity not matching these rules is considered suspicious and triggers a response. For example, a behavioral rule might state that only a web server process can access HTML files. If any other process tries to access HTML files, Exploit Prevention responds with the configured action. This type of protection, called application shielding and enveloping, prevents applications and their data from being compromised and prevents applications from being used to attack other applications.

Behavioral rules also block buffer overflow exploits, preventing code execution that results from a buffer overflow attack, one of the most common methods of attack.

Actions

An action is what Exploit Prevention does when a signature is triggered.

- **Block** — Prevents the operation.
- **Report** — Allows the operation and reports the event.

If neither is selected, the signature is disabled: Exploit Prevention allows the operation and doesn't report the event.

The Exploit Prevention content file automatically sets the action for signatures based on severity level. Typically, signatures with a severity level of **High** are set to both **Block** and **Report**. You can change the action for a specific signature in the **Signatures** section of the **Exploit Prevention** settings. Any changes you make to the signature actions persist through content updates.

Note

You can't delete or otherwise change default signatures.

Severity levels

Each signature has a default severity level, which describes the potential danger of an attack.

- **High** — Signatures that protect against clearly identifiable security threats or malicious actions. Most of these signatures are specific to well-identified exploits and are mostly non-behavioral in nature.

  Caution

  To prevent exposing systems to exploit attacks, set signatures with a severity of **High** to **Block** on every host.

- **Medium** — Signatures that are behavioral in nature and prevent applications from operating outside of their environment (relevant for clients protecting web servers and Microsoft SQL Server).

  Tip

  Best practice: On critical servers, set signatures with a severity of **Medium** to **Block** after fine-tuning.

- **Low** — Signatures that are behavioral in nature and shield applications. Shielding means locking down application and system resources so that they can't be changed. Setting signatures with a severity of **Low** to **Block** increases the security of the system, but requires additional tuning.
- **Informational** — Signatures that indicate a change to the system configuration that might create a benign security risk or an attempt to access sensitive system information. Events at this level occur during normal system activity and generally aren't evidence of an attack.
- **Disabled** — Signatures that are disabled in the Exploit Prevention content file. A **Disabled** status indicates there is no severity assigned to it.

In Trellix ENS versions 10.2 and earlier, the **Protection Level** setting controls signature actions. If you assign an **Exploit Prevention** policy from Trellix ENS version 10.7 or later to client systems running an earlier version, the **Protection Level** doesn't change and it isn't configurable from the policy. If **Protection Level** was set to **Standard**, only high-severity signatures are detected and blocked. If **Protection Level** was **Maximum**, high-severity and medium-severity signatures are detected and blocked.

Custom signatures

You can create custom signatures, also called rules, to enhance the protection provided by the default signatures. For example, when you create a folder with important files, you can create a custom signature to protect it.

You can create:

- **Custom Access Protection rules** to protect specific files, services, registry keys and values, and processes. Create these rules by clicking **Add** in the **Rules** section of the **Access Protection** settings.
- **Expert Exploit Prevention Rules** to prevent buffer overflow and illegal API use exploits, as well as protect files, services, registry, and processes. Create these rules by clicking **Add Expert Rule** in the **Signatures** section of the **Exploit Prevention** settings.

Note

You can't create Network IPS Expert Rules.

How Network IPS works

The Network Intrusion Prevention (also known as Network IPS) technology monitors network activity to protect client systems from threats.

The Network IPS protection filter driver inspects all data that flows between the client system and the network. It compares the network data with the known network-based attacks in the Network IPS signatures. If the data matches a known attack, Network IPS responds with the configured action, for example, blocking the data from the system.

Network IPS also enables you to automatically block network intruder hosts for a specified period, even if the action for the Network IPS signature isn't set to **Block**. Use this option to protect client systems against network denial-of-service attacks that deny or degrade network traffic.

How Trellix GTI works

Trellix GTI uses heuristics or file reputation to check for suspicious files through on-access scanning and on-demand scanning.

The scanner submits fingerprints of samples, or hashes, to a central database server hosted by Trellix Labs to determine if they are malware. By submitting hashes, detection might be made available sooner than when Trellix Labs publishes the next content file update.

You can configure the sensitivity level that Trellix GTI uses when it determines if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. But, allowing more detections can result in more false positives. The Trellix GTI sensitivity level is set to **Medium** by default. Configure the sensitivity level for each scanner in the **On-Access Scan** and **On-Demand Scan** settings.

You can configure Trellix ENS to use a proxy server for retrieving Trellix GTI reputation information in the Common settings.

For frequently asked questions about Trellix GTI , see KB53735.

How on-access scanning works

The on-access scanner examines files as the user accesses them, providing continuous, real-time detection of threats.

The on-access scanner integrates with the system at the lowest levels (File-System Filter Driver) and scans files where they first enter the system. When detections occur, the on-access scanner delivers notifications to the Service Interface.

You can also configure the on-access scanner to integrate with AMSI, a generic interface standard, provided by Microsoft and supported on Windows 10, Windows Server 2016, and Windows Server 2019 systems. AMSI allows applications and services to integrate with Threat Prevention, providing better protection against malware. Integrating with AMSI provides enhanced scanning for threats in non-browser-based scripts, such as PowerShell, JavaScript, and VBScript.

The on-access scan detection list is cleared when the Trellix ENS service restarts or the system reboots.

If you configure Trellix GTI , the scanner uses heuristics to check for suspicious files.

Windows 8 and Windows 10 — If the scanner detects a threat in the path of an installed Windows Store app, the scanner marks it as tampered. Windows adds the tampered flag to the tile for the app. When you try to run it, Windows notifies you of the problem and directs you to the Windows Store to reinstall.

The scanner uses this criteria to determine whether to scan an item:

- The file extension matches the configuration.
- The file information isn't in the global scan cache.
- The file hasn't been excluded or previously scanned.

Read scan

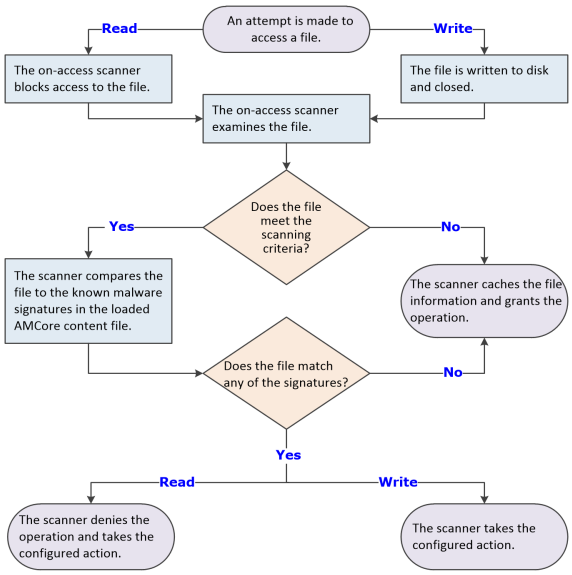
When Read scan is selected and an attempt is made to read, open, or execute a file:

1. The scanner blocks the request.
2. The scanner determines whether the item must be scanned.
    - If the file doesn't need to be scanned, the scanner unblocks the file, caches the file information, and grants the operation.
    - If the file needs to be scanned, the scan engine scans the file, comparing it to signatures in the currently loaded AMCore content file.
        - If the file is clean, the scanner unblocks the file and caches the result.
        - If the file contains a threat, the scanner denies access to the file and responds with the configured action. For example, if the action is to clean the file, the scanner:
            - Uses information in the currently loaded AMCore content file to clean the file.
            - Records the results in the activity log.
            - Notifies the user that it detected a threat in the file, and prompts for the action to take (clean or delete the file).

Write scan

The scanner examines the file only after it is written to disk and closed. When Write scan is selected and a file is written to disk:

1. The scanner determines whether the item must be scanned.
    a. If the file doesn't need to be scanned, the scanner caches the file information, and grants the operation.
    b. If the file needs to be scanned, the scan engine scans the file, comparing it to signatures in the currently loaded AMCore content file.
        - If the file is clean, the scanner caches the result.
        - If the file contains a threat, the scanner responds with the configured action. The scanner doesn't deny access to the file.



How AMSI integration with Threat Prevention improves security

You can enable integration with Antimalware Scan Interface (AMSI) to provide protection against non-browser-based scripts, such as PowerShell, JavaScript, and VBScript. With this feature enabled, AMSI blocks the script before execution.

AMSI is a generic interface standard provided by Microsoft and supported on Windows 10, Windows Server 2016, and Windows 2019 systems. It allows applications and services to integrate with Threat Prevention, providing better protection against malware.

Tip

Best practice: For the best protection against script-based threats, enable this option with ScriptScan, which scans browser-based scripts, and Adaptive Threat Protection enhanced scanning.

Actions and Exclusions

AMSI scanning uses the **Actions** and **Exclusions** specified for **Standard** process types in the **Process Settings** section of the **On-Access Scan** settings.

AMSI uses the threat detection responses specified in the **Actions** settings. For example, if **Threat detection first response** is set to **Clean files**, AMSI also takes this action.

AMSI excludes most files that are excluded from on-access scans. Some scripts, such as PowerShell, are fileless and are not excluded from AMSI.

How the script scanner works

The Threat Prevention script scanner intercepts and scans scripts before they are executed.

ScriptScan is a Browser Helper Object that examines JavaScript and VBScript code for malicious scripts before they are executed. If the script is clean, it passes to JavaScript or VBScript for handling. If ScriptScan detects a malicious script, it blocks the script from executing.

Note

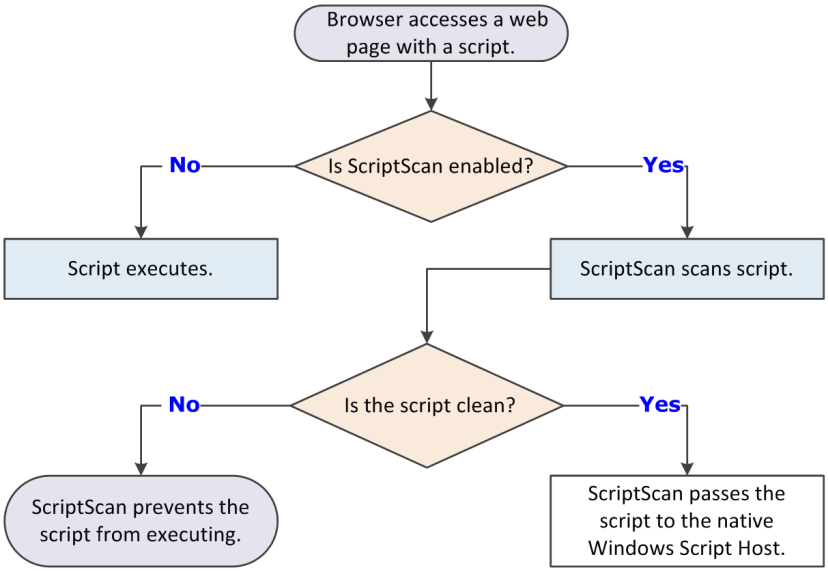
ScriptScan examines scripts for Internet Explorer only. It doesn't look at scripts system-wide and doesn't examine scripts run by wscript.exe or cscript.exe.

When Threat Prevention is installed, the first time that Internet Explorer starts, a prompt to enable one or more Trellix add-ons appears. For ScriptScan to scan scripts:

- The **Enable ScriptScan** setting must be selected. ScriptScan is disabled by default.
- The add-on must be enabled in the browser.

Caution

If ScriptScan is disabled when Internet Explorer starts and then is enabled, it doesn't detect malicious scripts in that instance of Internet Explorer. You must restart Internet Explorer after enabling ScriptScan for it to detect malicious scripts.



- If the script is clean, the script scanner passes the script to the native Windows Script Host.
- If the script contains a potential threat, the script scanner prevents the script from executing.

Best practices: ScriptScan exclusions

Script-intensive websites and web-based applications might experience poor performance when ScriptScan is enabled. Instead of disabling ScriptScan, we recommend specifying URL exclusions for trusted sites, such as sites in an intranet or web applications that are known safe.

You can specify substrings or partial URLs for ScriptScan exclusions. If an exclusion string matches any part of the URL, the URL is excluded. For example, specifying an exclusion of "msn.com" excludes both http://money.msn.com and http://www.msn.com.

When creating URL exclusions:

- Wildcard characters aren't supported.
- More complete URLs result in improved performance.
- Don't include port numbers.
- Use only fully qualified domain names (FQDN) and NetBIOS names.

Note

New URL exclusions are not applied to currently running Internet Explorer browsers. You must restart Internet Explorer for the new exclusions to take effect.

How on-demand scanning works

The on-demand scanner searches files, folders, memory, and registry, looking for malware that might have infected the computer.

You decide when and how often the on-demand scans occur. You can scan systems manually, at a scheduled time, or at startup. Use on-demand scans to supplement the continuous protection of the on-access scanner, such as to scan latent and inactive processes.

The on-demand scan detection list is cleared when the next on-demand scan starts.

1. The on-demand scanner uses the following criteria to determine if the item must be scanned:
    - The file extension matches the configuration.
    - The file hasn't been cached, excluded, or previously scanned (if the scanner uses the scan cache).

    Note

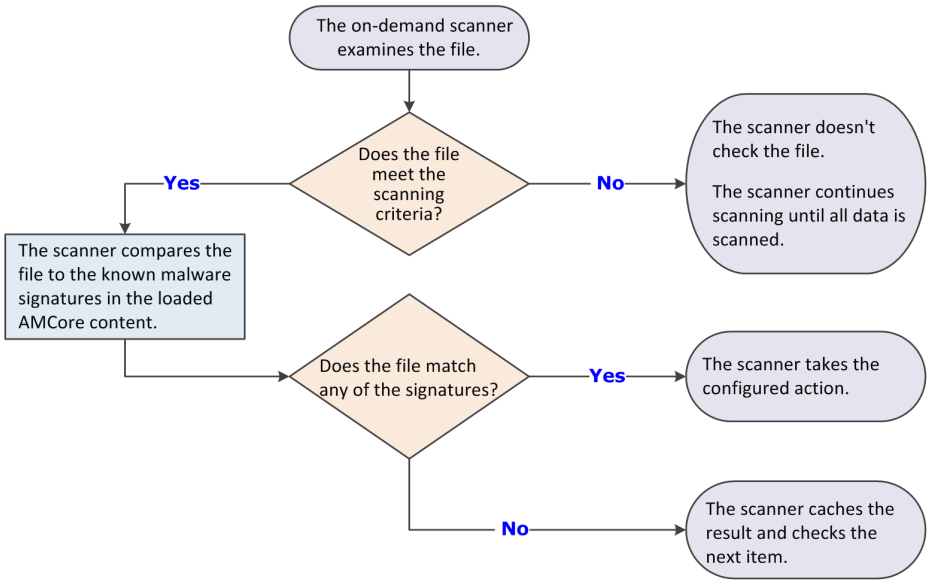
    If you configure Trellix GTI , the scanner uses heuristics to check for suspicious files.

2. If the file meets the scanning criteria, the scanner compares the information in the item to the known malware signatures in the currently loaded AMCore content files.
    - If the file is clean, the result is cached, and the scanner checks the next item.

- If the file contains a threat, the scanner responds with the configured action. For example, if the action is to clean the file, the scanner:
  - Uses information in the currently loaded AMCore content file to clean the file.
  - Records the results in the activity log.
  - Notifies the user that it detected a threat in the file, and includes the item name and the action taken.

  Windows 8 and Windows 10 — If the scanner detects a threat in the path of an installed Windows Store app, the scanner marks it as tampered. Windows adds the tampered flag to the tile for the app. When you try to run it, Windows notifies you of the problem and directs you to the Windows Store to reinstall.

3. If the item doesn't meet the scanning requirements, the scanner doesn't check it. Instead, the scanner continues until all data is scanned.



When the global scan cache is flushed

The global scan cache stores the clean scan results. The on-access scanner and on-demand scanner can check the cache to avoid scanning known clean files and improve performance.

- The Threat Prevention global scan cache is flushed when:
  - The **On-Access Scan** or **On-Demand Scan** configuration changes.
  - An Extra.DAT file is loaded.
  - The daily AMCore Content file includes an updated Trust DAT. Trust DATs are released every 1–2 weeks, as needed for new certificates.
  - The system reboots in safe mode.
- An individual object is flushed from the cache when:
  - The object has changed on the disk.
  - The object expires.

- By default, items in the cache are flushed after 5 days, if the entire cache hasn't been flushed in that time. The expiration time for an item might differ from the default if the cache is full. Recently accessed cache items are retained; older items expire and are removed.

If the process is signed by a trusted certificate, the signing certificate is cached and remains in the cache after the system reboots. The scanner is less likely to scan files accessed by processes that are signed by a cached trusted certificate, resulting in scan avoidance and improved performance.

How system utilization works

System utilization (throttling) determines the amount of CPU time allotted during an on-demand scan.

The on-demand scanner uses the Windows Set Priority setting for the scan process and thread priority.

Note

Each task runs independently, unaware of the limits for other tasks.

System utilization settings

System utilization setting	This option...	Best practices
Low	• Provides improved performance for other running applications. • Sets the number of threads for the scan to 1.	Select this option for systems with end-user activity.
Below normal	• Sets the number of threads for the scan to be equal to the number of CPUs. • Is the default setting for the preconfigured **Full Scan** and **Quick Scan** on-demand scans.	
Normal	• Enables the scan to complete faster. • Sets the number of threads for the scan to twice the number of CPUs.	Select this option for systems that have large volumes and little end-user activity.

System utilization setting	This option...	Best practices
	• Is the default setting for custom on-demand scans.	

CPU usage during scans

You can use the Windows Task Manager to view CPU utilization consumed by the Trellix Scanner service process (mcshield.exe).

The scan process for **Full Scan** and **Quick Scan** on-demand scans runs at low priority. But, if no other processes are running during a scan, the mcshield.exe process might consume a higher amount of CPU resources. If any other processes make system requests, mcshield.exe releases the CPU resources.

How Threat Prevention limits CPU usage

To optimize the performance of a client system, you can restrict the CPU usage of on-demand scans.

The CPU utilization of a client system increases during an on-demand scan. With other processes and services running parallel to the on-demand scan, the CPU utilization can rise up to 100%. The high CPU utilization affects the performance of the system.

You can prevent this situation by enabling **Limit maximum CPU usage** and defining a threshold percentage for CPU usage. During an on-demand scan, the CPU utilization value doesn't exceed the threshold value.

The threshold value is inversely proportional to the time needed to complete the scan. The higher the threshold value, the quicker the scan finishes.

The **Limit maximum CPU usage** option restricts CPU usage for full scans, quick scans, and custom scans.

This option only applies to scanning files. It doesn't limit CPU usage when scanning other items, such as memory, registry, and boot sectors.

Note

This option is available only when the **Scan anytime** option is selected.

How Remote Storage scanning works

Remote Storage scanning restores files that have been migrated to storage to the local system before scanning.

Remote Storage monitors the amount of available space on the local system. When needed, Remote Storage automatically migrates the content (data) from eligible files from the client system to a storage device, such as a tape library. When a user opens a file whose data has been migrated, Remote Storage automatically recalls the data from the storage device.

Select the **Files that have been migrated to storage** option to configure the on-demand scanner to scan files that Remote Storage manages. When the scanner encounters a file with migrated content, it restores the file to the local system before scanning.

Note

This option doesn't apply to files stored in Microsoft OneDrive. The on-demand scanner doesn't download OneDrive files or scan files that haven't been downloaded.

For more information, see What is Remote Storage.

Threat Prevention additions to Trellix ePO - On-prem

This managed product extends your ability to secure your network with these features and enhancements.

Important

You must have appropriate permissions to access most features.

Trellix ePO - On-prem feature	Addition	Management platform
Client tasks	Client tasks that you can use to automate management and maintenance on client systems.	All
Dashboards	• Dashboards and monitors that you can use to keep watch on your environment.	• All
	• Custom dashboards	• Trellix ePO - On-prem
Events and responses	• Events for which you can configure automatic responses. • Event groups and event types that you can use to customize automatic responses.	All

Trellix ePO - On-prem feature	Addition	Management platform
Managed system properties	Properties that you can review in the **System Tree** or use to customize queries.	All
Permissions sets	**Endpoint Security Threat Prevention** and **Endpoint Security Threat Prevention Client** permission categories, available in all existing permission sets.	Trellix ePO - On-prem
Policies	• **Exploit Prevention**, **On-Access Scan**, **On-Demand Scan**, and **Options** policy categories in the **Endpoint Security Threat Prevention** product group.	• All
	• Custom policies	• Trellix ePO - On-prem
Queries and reports	Query names include the module name for easier filtering. • Default queries that you can use to run reports.	• All
	• Custom property groups based on managed system properties that you can use to build your own queries and reports.	• Trellix ePO - On-prem

For information about these features, see the Trellix ePO - On-prem documentation.

Permission sets and Threat Prevention Trellix ePO - On-prem

Permission sets define rights for managed product functionality in Trellix ePO - On-prem.

Threat Prevention adds the **Endpoint Security Threat Prevention** and **Endpoint Security Threat Prevention Client** permission group to each permission set.

Permission groups define the access rights to the features. Trellix ePO - On-prem grants all permissions for all products and features to global administrators. Administrators then assign user roles to existing permission sets or create permission sets.

Your managed product adds these permission controls to Trellix ePO - On-prem.

Permissions sets	Default permissions
Executive Reviewer **Endpoint Security Threat Prevention** and **Endpoint Security Threat Prevention Client**	No permissions
Global Reviewer **Endpoint Security Threat Prevention**	Views policy and task settings.
Global Reviewer **Endpoint Security Threat Prevention Client**	No permissions
Group Admin **Endpoint Security Threat Prevention** and **Endpoint Security Threat Prevention Client**	No permissions
Group Reviewer **Endpoint Security Threat Prevention** and **Endpoint Security Threat Prevention Client**	No permissions

This managed product grants **No Permissions** by default.

Permissions must be granted for users to access or use permission-controlled features.

Permissions required per feature

Features	Required permissions
Automatic Responses	• **Automatic Responses** • **Event Notifications** • Any feature-specific permissions depending on the feature used (such as **System Tree** or queries).

Features	Required permissions
Client tasks	**Endpoint Security Threat Prevention: Tasks** in the **Endpoint Security Threat Prevention** permission group
Dashboards and monitors	• **Dashboards** • **Queries**
Policies	**Endpoint Security Threat Prevention: Policy** in the **Endpoint Security Threat Prevention** permission group
Reporting	• **Systems** • **System Tree** access • **Threat Event Log** • **View Exploit Prevention Events** in the **Endpoint Security Threat Prevention Client** permission group
Queries	• **Queries & Reports** • **View Queries** in the **Endpoint Security Threat Prevention Client** permission group
Server tasks	**Server Tasks**
System Tree	• **Systems** • **System Tree** access
Threat Event Log	• **Systems** • **System Tree** access • **Threat Event Log**

For information about managing permission sets, see the Trellix ePO - On-prem documentation.

Client tasks and Threat Prevention

Automate management or maintenance on managed systems using client tasks.

Your managed product adds these client tasks to the **Client Task Catalog**. You can use client tasks as is, edit them, or create new ones.

Threat Prevention default client tasks

Client task	Description
Custom On-Demand Scan	Examines all parts of the managed computer for potential threats, at times that don't interfere with your work.
Policy-Based On-Demand Scan	Runs the default **Quick Scan** and **Full Scan** on-demand scans from Trellix ePO - On-prem. Configure the behavior of quick and full scans in the **On-Demand Scan** policy settings.
Restore from Quarantine	Restores individual items from the quarantine.
Roll Back AMCore Content	Removes specified version numbers of the AMCore content files from client systems.

Threat Prevention leverages the following default Trellix Agent client tasks.

Trellix Agent default client tasks

Client task	Description	Management platform
Product Deployment	Deploys Trellix products to client systems.	Trellix ePO - On-prem
Product Update	Updates content files, engines, and all Trellix products automatically.	All
Mirror Repositories	Replicates the updated content and engine files from the first accessible repository to a mirror site on your network.	Trellix ePO - On-prem

Client task	Description	Management platform
	For information about using distributed repositories to keep your security software up to date, see the Trellix ePO - On-prem *Best Practices Guide*.	

For information about client tasks and the **Client Task Catalog**, see the Trellix ePO - On-prem documentation.

What to do first

Once installed, Threat Prevention uses the content files packaged with the product to provide general security for your environment. We recommend that you download the latest content files and customize the configuration to meet your requirements before deploying to client systems.

Immediately after installation:

1. **Set user interface security** — Configure the access options and password to control access to specific components or the whole Trellix Endpoint Security (ENS) Client interface.
2. **Configure logging on the client** — Specify the location of log files for Trellix ENS features, types of information, and severity level of events to log. Select which client events to forward to Trellix ePO - On-prem and whether to log events to the Windows Application log.
3. **Confirm engine and content files** — Verify that client systems have the latest engine and content files installed using Trellix Endpoint Security (ENS) Client or Trellix ePO - On-prem. Verify that client systems have the latest engine and content files installed using Trellix Endpoint Security (ENS) Client.
4. **Prevent intrusions** — Make sure Access Protection and Exploit Prevention are enabled, specify reactions to signatures and exclusions, and configure rules to prevent unwanted changes to commonly used files and settings.
5. **Configure settings that apply to all scans**:
    - Quarantine location and the number of days to keep quarantined items before automatically deleting them
    - Detection names to exclude from scans
    - Potentially unwanted programs such as spyware and adware to detect
6. **Configure scans that run automatically when files are accessed** — Configure the on-access scanner to detect and respond to potential threats as files are accessed in your environment. Enable detection of potentially unwanted programs.
7. **Configure and schedule regular targeted scans** — Configure on-demand scans to perform:
    - Daily memory scans
    - Weekly or daily scans of active user locations, such as user profile folder, Temp folder, registry entries, registered files, and Windows folder
8. **Configure engine and content file updates** — Configure a Trellix Agent **Product Update** client task to make sure that you have the most current content files, engine, and product upgrades.

Firewall

How firewall rules work

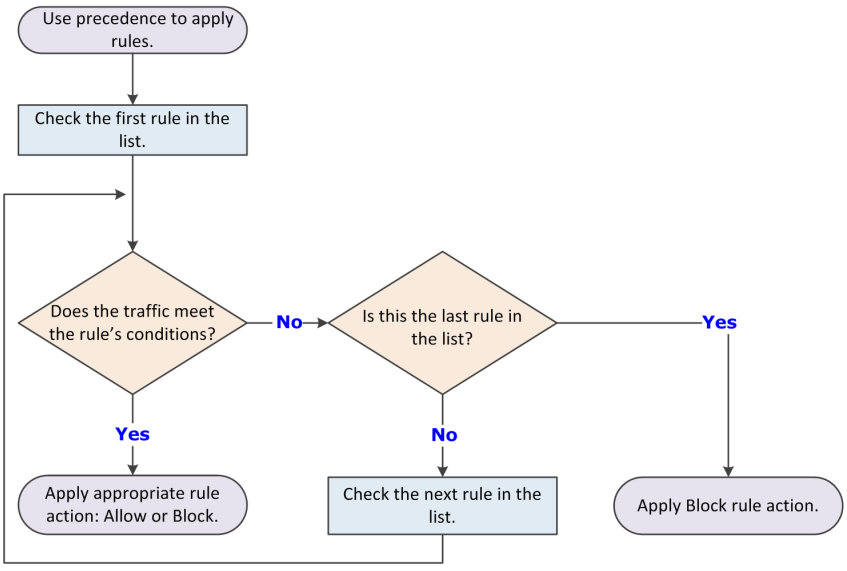
Firewall rules determine how to handle network traffic. Each rule provides a set of conditions that traffic must meet, and an action to allow or block traffic.

When Firewall finds traffic that matches a rule's conditions, it performs the associated action.

You can define rules broadly (for example, all IP traffic) or narrowly (for example, identifying a specific application or service) and specify options. You can group rules according to a work function, service, or application for easier management. Like rules, you can define rule groups by network, transport, application, schedule, and location options.

Firewall uses precedence to apply rules:

1. Firewall applies the rule at the top of the firewall rules list. If the traffic meets this rule's conditions, Firewall allows or blocks the traffic. It doesn't try to apply any other rules in the list.
2. If the traffic doesn't meet the first rule's conditions, Firewall continues to the next rule in the list until it finds a rule that the traffic matches.
3. If no rule matches, the firewall automatically blocks the traffic.



If Adaptive mode is activated, an Allow rule is created for the traffic. Sometimes the intercepted traffic matches more than one rule in the list. In this case, precedence means that Firewall applies only the first matching rule in the list.

Best practices

Place the more specific rules at the top of the list, and the more general rules at the bottom. This order makes sure that Firewall filters traffic appropriately.

For example, to allow all HTTP requests except from a specific address (for example, IP address 10.10.10.1), create two rules:

- **Block rule** — Block HTTP traffic from IP address 10.10.10.1. This rule is specific.
- **Allow rule** — Allow all traffic using the HTTP service. This rule is general.

Place the Block rule higher in the firewall rules list than the Allow rule. When the firewall intercepts the HTTP request from address 10.10.10.1, the first matching rule it finds is the one that blocks this traffic through the firewall.

If the general Allow rule is higher than the specific Block rule, Firewall matches requests against the Allow rule before finding the Block rule. It allows the traffic, even though you wanted to block the HTTP request from a specific address.

How firewall rule groups work

Firewall rule groups organize firewall rules for easy management. The software includes predefined rule groups with rules that allow needed services, such as Trellix ePO - On-prem and DNS, to run.

Firewall rule groups don't affect the way Firewall handles the rules; the software processes rules from top to bottom.

Firewall processes the settings for the group before processing the settings for the rules it contains. If a conflict exists between these settings, the group settings take precedence.

You can create customized rule groups:

- **Timed groups** — Activate the group's settings manually or on a specified schedule.
- **Connection isolation groups** — Process only traffic that matches a defined connection type and group criteria.

Predefined firewall rule groups in Trellix ePO - On-prem

The predefined firewall groups include needed rules, such as core networking rules to allow Trellix applications.

Firewall group	Description
Trellix core networking	Contains the core networking rules provided by Trellix and includes rules to allow Trellix applications and DNS. **Note:** You can't change or delete rules in this rule group. If you need to, you can create a duplicate of the group, make changes to the rules, then select the **Disable Trellix core networking rules** option in the Firewall **Options** policy to disable the group. But, this might disrupt network communications on the client system.

Firewall group	Description
ePolicy Orchestrator server	Contains rules to allow Trellix ePO - On-prem services to run.
Basic networking (Required)	Contains rules to allow basic networking services, such as DNS, to run.
VPN	Contains rules to allow VPN services to run.
ICMP	Contains rules to allow all ICMP traffic.
Windows AD authentication	Contains rules to allow Windows Active Directory authentication.
NetBIOS	Contains rules to allow inbound and outbound NetBIOS services and sessions, and block untrusted NetBIOS services.
Web/FTP	Contains rules to allow outbound HTTPS and FTP services.
Mail clients	Contains rules to allow outbound mail services, such as POP.
Network tools	Contains rules to allow Remote Desktop (RDP) connections.

Predefined firewall rule groups on a client system

The predefined firewall groups include needed rules, such as core networking rules to allow Trellix applications.

Note

If a firewall group has no rules defined, it appears in gray to indicate that the group is empty.

Firewall group	Description
Trellix core networking	Contains the core networking rules provided by Trellix and includes rules to allow Trellix applications and DNS. **Note:** You can't change or delete rules in this rule group. If you need to, you can create a duplicate of the group, make changes to the rules, then select the **Disable Trellix core networking rules** option in the Firewall **Options** policy to disable the group. But, this might disrupt network communications on the client system.
Admin-defined	Contains rules defined by the administrator at the management server. This group appears on the Trellix Endpoint Security (ENS) Client only if the client system is managed by Trellix ePO - On-prem. In this case, the group displays **Enabled** even if it contains no rules. **Note:** These rules can't be changed or deleted on the Trellix Endpoint Security (ENS) Client.
User-defined	Contains rules defined on the Trellix Endpoint Security (ENS) Client. This group displays **Enabled** even if it contains no rules. Because these rules are created on the client system, these rules might be overwritten when the policy is enforced, depending on policy settings.
Adaptive	Contains client exception rules that are created automatically when the system is in Adaptive mode. This group displays **Enabled** even if Adaptive mode is not enabled and the group contains no rules. Once

Firewall group	Description
	Adaptive mode is enabled, the group is populated with automatically generated rules. Because these rules are created on the client system, these rules might be overwritten when the policy is enforced, depending on policy settings.
Default	Contains default rules provided by Trellix. **Note:** These rules can't be changed or deleted.

How Trellix core networking rules work

Trellix core networking rules are provided by Trellix in the predefined Trellix core networking group and allow network traffic related to Trellix applications, DNS, and critical system processes.

You can't change or delete rules in this rule group. If you need to, you can create a duplicate of the group, make changes to the rules, then select the **Disable Trellix core networking rules** option in the Firewall **Options** policy to disable the group. But, this might disrupt network communications on the client system.

You might want to disable the Trellix core networking rules to have more control of network traffic using firewall rules. For example, allow DNS-related traffic to only specific DNS server IP addresses.

Best practice: If you disable Trellix core networking rules, make sure you thoroughly test the policy before implementing it in a production environment.

If you disable these rules, you might need to make configuration changes in the Firewall **Options** or **Firewall Rules** policy. The changes depend on what type of network traffic is blocked and how you want to allow the network traffic. For example, you can create specific firewall rules to allow traffic, or allow traffic by trusted executables or trusted networks.

Firewall rules in the Trellix core networking group

The Trellix core networking group includes firewall rules to allow network traffic related to Trellix applications, DNS, and critical system processes.

Note

If you select the **Disable Trellix core networking rules** option in the Firewall **Options** policy, Firewall only disables some of the rules. This prevents Firewall from blocking specific types of critical application and non-application network traffic that could cause outages.

Firewall rule	Description	Can you disable it?
Allow outbound system applications	Allows outbound network traffic for the Windows SYSTEM executable process.	Yes
Allow ARP traffic	Allows inbound and outbound network traffic for ARP (Address Resolution Protocol) packets (Ethernet Protocol 0x806).	No
Allow EAPOL traffic	Allows inbound and outbound network traffic for EAPOL (Extensible Authentication Protocol over LAN) packets (Ethernet Protocol 0x888E).	Yes
Allow outbound stock applications	Allows outbound network traffic for Windows critical processes. For example, services.exe, svchost.exe, lsass.exe, userinit.exe, winlogon.exe, alg.exe, spoolsv.exe, and dns.exe.	Yes
Allow Trellix signed applications	Allows inbound and outbound network traffic related to Trellix products based on signer certificate value.	No
Allow Trellix signed applications 2		
Allow Trellix signed applications 3		
Allow Trellix signed applications 4		
Allow outbound ICMPv4 traffic	Allows outbound network traffic related to the ICMPv4 transport protocol.	Yes

Firewall rule	Description	Can you disable it?
Allow outbound ICMPv6 traffic	Allows outbound network traffic related to the ICMPv6 transport protocol.	Yes
Allow outbound DNS traffic	Allows outbound network traffic related to remote host UDP Port 53 (default port for DNS resolution).	Yes
Allow inbound traffic from special IP addresses	Allows inbound network traffic for the special IP address 0.0.0.0 (IPv4 and IPv6).	Yes
Allow outbound loopback and broadcast traffic	Allows outbound network traffic related to IPv4/IPv6 loopback and broadcast traffic.	Yes
Allow reserved IP traffic	Allows inbound and outbound network traffic for the RESERVED Transport Protocol 255 (0xFF).	Yes
Allow outbound BOOTP traffic	Allows outbound network traffic for BOOTP and DHCP traffic (UDP port 67 and 68).	No
Allow outbound DHCPv6 traffic	Allows outbound network traffic for DHCPv6 traffic (UDP port 546 and 547).	Yes

Using timed groups

Timed groups are Firewall rule groups that are active for a set time.

For example, a timed group can be enabled to allow a client system to connect to a public network and establish a VPN connection.

Depending on settings, groups can be activated either:

- On a specified schedule.

- Manually by selecting options from the Trellix system tray icon.

Making groups location-aware

You can make a group and its rules location-aware and create connection isolation.

Note

Settings for **Transport** and **Executables** aren't available for connection isolation groups.

The **Location** and **Network Options** of the group enable you to make the groups network adapter-aware. Use network adapter groups to apply adapter-specific rules for computers with multiple network interfaces. After enabling location status and naming the location, parameters for allowed connections can include the following for each network adapter:

- **Location**:
    - **Connection-specific DNS suffix**
    - **Default gateway** IP address
    - **DHCP server** IP address
    - **DNS server** queried to resolve URLs
    - **Primary WINS server** IP address
    - **Secondary WINS server** IP address
    - **Domain reachability (HTTPS)**
    - **Registry key**

    Note

    If you specify more than one location-criteria parameter, all are applied to the location-aware group.

- **Networks** (local):
    - **Single IP address**
    - **Range**
    - **Subnet**

If two location-aware groups apply to a connection, Firewall uses normal precedence, processing the first applicable group in its rule list. If no rule in the first group matches, rule processing continues.

When Firewall matches a location-aware group's parameters to an active connection, it applies the rules in the group. It treats the rules as a small rule set and uses normal precedence. If some rules don't match the intercepted traffic, Firewall ignores them.

If this option is selected...	Then...
Enable location awareness	A location name is needed.

If this option is selected...	Then...
Require that Trellix ePO - On-prem is reachable	The Trellix ePO - On-prem is reachable and the FQDN of the server has been resolved. To determine whether the Trellix ePO - On-prem server is available, Firewall performs DNS and WINS queries for the Trellix ePO - On-prem server name, which is registered with Trellix Agent. If both WINS and DNS fail to resolve the name, the Trellix ePO - On-prem server is not available.
Local Network	The IP address of the adapter must match one of the list entries.
Connection-specific DNS suffix	The DNS suffix of the adapter must match one of the list entries.
Default gateway	The default adapter gateway IP address must match at least one of the list entries.
DHCP server	The adapter DHCP server IP address must match at least one of the list entries.
DNS server	The adapter DNS server IP address must match any of the list entries.
Primary WINS server	The adapter primary WINS server IP address must match at least one of the list entries.
Secondary WINS server	The adapter secondary WINS server IP address must match at least one of the list entries.
Domain reachability (HTTPS)	The specified domain must be reachable using HTTPS. To determine whether the domain is reachable, Firewall checks for the valid SSL certificate of the domain. The location-aware group criteria matches and the rules are applied only if the domain has a valid certificate.

If this option is selected...	Then...
Registry Key	The value given in the registry key criteria must match the windows registry key.

You can select a criteria from the above list, or you can choose not to provide any criteria, which would mean that the **Location Aware Group** is always enabled.

Location Criteria of similar type is **OR** with each other, and criteria of different type is **AND** with each other. See below:

Location Aware Groups
Connection-specific DNS suffix OR **Connection-specific DNS suffix**
AND
Default gateway OR **Default gateway**
AND
DHCP server OR **DHCP server**
AND
DNS server OR **DNS server**
AND
Primary WINS server OR **Primary WINS server**

Location Aware Groups
AND
Secondary WINS server OR **Secondary WINS server**
AND
Domain reachability (HTTPS) OR **Domain reachability (HTTPS)**
AND
Registry Key OR **Registry Key**

Firewall rule groups and connection isolation

Prevent undesirable traffic from accessing a designated network by using connection isolation for groups.

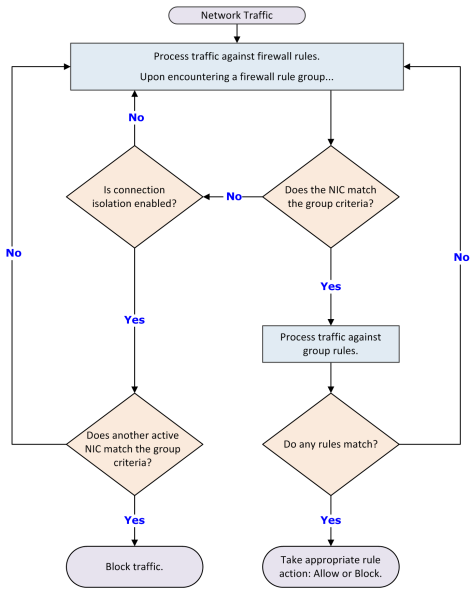
When connection isolation is enabled for a group, and an active Network Interface Card (NIC) matches the group criteria, Firewall only processes traffic that matches:

- Allow rules above the group in the firewall rules list
- Group criteria

All other traffic is blocked.

Note

Any group with connection isolation enabled can't have associated transport options or executables.



As examples of using connection isolation, consider two settings: a corporate environment and a hotel. The active firewall rules list contains rules and groups in this order:

1. Rules for basic connection
2. VPN connection rules
3. Group with corporate LAN connection rules
4. Group with VPN connection rules

Example: connection isolation on the corporate network

Connection rules are processed until the group with corporate LAN connection rules is encountered. This group contains these settings:

- **Connection type** = **Wired**
- **Connection-specific DNS suffix** = mycompany.com
- **Default gateway**
- **Connection isolation** = Enabled

The computer has both LAN and wireless network adapters. The computer connects to the corporate network with a wired connection. But, the wireless interface is still active, so it connects to a hotspot outside the office. The computer connects to both networks because the rules for basic access are at the top of the firewall rules list. The wired LAN connection is active and meets the criteria of the corporate LAN group. The firewall processes the traffic through the LAN but because connection isolation is enabled, all other traffic not through the LAN is blocked.

Example: connection isolation at a hotel

Connection rules are processed until the group with VPN connection rules is encountered. This group contains these settings:

- **Connection type** = **Virtual**

- **Connection-specific DNS suffix** = vpn.mycompany.com
- **IP address** = An address in a range specific to the VPN concentrator
- **Connection isolation** = Enabled

General connection rules allow the setup of a timed account at the hotel to gain Internet access. The VPN connection rules allow connection and use of the VPN tunnel. After the tunnel is established, the VPN client creates a virtual adapter that matches the criteria of the VPN group. The only traffic the firewall allows is inside the VPN tunnel and the basic traffic on the actual adapter. Attempts by other hotel guests to access the computer over the network, either wired or wireless, are blocked.

Firewall stateful packet filtering and inspection

Firewall provides both stateful packet filtering and stateful packet inspection.

Stateful packet filtering is the stateful tracking of TCP/UDP/ICMP protocol information at Transport Layer 4 and lower of the OSI network stack. Each packet is examined. If the inspected packet matches an existing firewall Allow rule, the packet is allowed and an entry is made in a state table. The state table dynamically tracks connections previously matched against a static rule set, and reflects the current connection state of the TCP/UDP/ICMP protocols. If an inspected packet matches an existing entry in the state table, the packet is allowed without further scrutiny. When a connection is closed or times out, its entry is removed from the state table.

Stateful packet inspection is the process of stateful packet filtering and tracking commands at Application Layer 7 of the OSI network stack. This combination offers a strong definition of the computer's connection state. Access to the application-level commands provides error-free inspection and securing of the FTP protocol.

How stateful packet filtering works

Stateful filtering involves processing a packet against two rule sets: a configurable firewall rule set and a dynamic firewall rule set or state table.

The configurable rules have two possible actions:

- **Allow** — The packet is permitted and an entry is made in the state table.
- **Block** — The packet is blocked and no entry is made in the state table.

The state table entries result from network activity and reflect the state of the network stack. Each rule in the state table has only one action, **Allow**, so that any packet matched to a rule in the state table is automatically permitted.

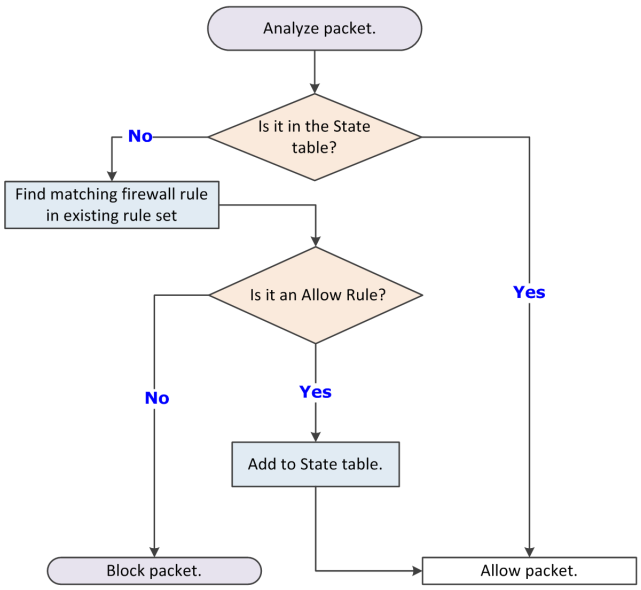
The filtering process includes the following:

1. The firewall compares an incoming packet against entries in the state table. If the packet matches any entry in the table, the packet is immediately allowed. If not, the configurable firewall rules list is examined.

   Note

   A state table entry is considered a match if the Protocol, Local Address, Local Port, Remote Address, and Remote Port match those elements of the packet.

2. If the packet matches an Allow rule, it is allowed and an entry is created in the state table.
3. If the packet matches a Block rule, it is blocked.
4. If the packet doesn't match any configurable rule, it is blocked.



How stateful packet inspection works

Stateful packet inspection combines stateful filtering with access to application-level commands, which secure protocols such as FTP.

FTP involves two connections: *control* for commands and *data* for the information. When a client connects to an FTP server:

- The control channel is established on FTP destination port 21.
- An entry is made in the state table.

If **Use FTP protocol inspection** is enabled, the firewall performs stateful packet inspection on packets arriving through the FTP control channel on port 21.

With the control channel open, the client communicates with the FTP server. The firewall parses the PORT command in the packet and creates a second entry in the state table to allow the data connection.

When the FTP server is in active mode, it opens the data connection; in passive mode, the client initiates the connection. When the FTP server receives the first data transfer command (LIST), it opens the data connection toward the client and transfers the data. The data channel is closed after the transmission is completed.

The combination of the control connection and data connections is called a session. FTP dynamic rules are sometimes called session rules. The session remains established until its control channel entry is deleted from the state table. During the periodic cleanup of the table, if a session's control channel has been deleted, all data connections are then deleted.

Firewall state table

A firewall state table dynamically stores information about active connections allowed by firewall rules.

Each entry in the table defines a connection based on:

- **Protocol** — The predefined way one service talks with another; includes TCP, UDP, and ICMP protocols.
- **IP addresses for local and remote computers** — Each computer is assigned a unique IP address. IPv4, the current standard for IP addresses, permits addresses 32 bits long, whereas IPv6, a newer standard, permits addresses 128 bits long. Many operating systems, including Windows Vista and later, support IPv6. Firewall supports both standards.
- **Port numbers for local and remote computers** — A computer sends and receives services using numbered ports. For example, HTTP service typically is available on port 80, and FTP services on port 21. Port numbers range from 0–65535.
- **Process ID (PID)** — A unique identifier for the process associated with a connection's traffic.
- **Timestamp** — The time of the last incoming or outgoing packet associated with the connection.
- **Timeout** — The time limit (in seconds) after which the entry is removed from the table if no packet matching the connection is received. The timeout for TCP connections is enforced only when the connection isn't established.
- **Direction** — The direction (incoming or outgoing) of the traffic that triggered the entry. After a connection is established, bidirectional traffic is allowed even with unidirectional rules, provided the entry matches the connection's parameters in the state table.

Considerations for the state table

- If firewall rule sets change, all active connections are checked against the new rule set. If no matching rule is found, the connection entry is discarded from the state table.
- If an adapter obtains a new IP address, the firewall recognizes the new configuration and drops all state table entries with invalid local IP addresses.
- When the process ends, all entries in the state table associated with a process are deleted.

Stateful protocol tracking

Firewall monitors and handles connections based on the protocol.

Protocol	How protocol is handled
UDP	A UDP connection is added to the state table when a matching static rule is found and the action from the rule is Allow. Generic UDP connections remain in the state table as long as the connection isn't idle longer than the specified timeout period. These connections carry application-level protocols unknown to the firewall.
ICMPv4/v6	Only ICMP Echo Request and Echo Reply message types are tracked.

Protocol	How protocol is handled
	In contrast to the reliable connection-oriented TCP protocol, UDP and ICMPv4/v6 are less reliable, connectionless protocols. To secure these protocols, the firewall considers generic UDP and ICMP connections to be virtual connections. Virtual connections are held only as long as the connection isn't idle longer than the timeout period specified for the connection. Set the timeout for virtual connections in the Firewall **Options** settings.
TCP	TCP protocol works on the S3-way handshake. • The client computer initiates a new connection, sending a packet to its target with a SYN bit set. • The target responds by sending a packet to the client with a SYN-ACK bit set. • The client responds by sending a packet with an ACK bit set and the stateful connection is established. All outgoing packets are allowed, but only incoming packets that are part of the established connection are allowed. An exception is when the firewall first queries the TCP protocol and adds all pre-existing connections that match the static rules. Pre-existing connections without a matching static rule are blocked. The TCP connection timeout is enforced only when the connection isn't established. A second or forced TCP timeout applies to established TCP connections only. A registry setting controls this timeout, which has a default value of one hour. Every four minutes the firewall queries the TCP stack and discards connections that TCP doesn't report.
DNS	Query/response matching makes sure that DNS responses are only allowed: • To the local port that originated the query • From a remote IP address that has been queried during the UDP Virtual Connection Timeout interval Incoming DNS responses are allowed if:

Protocol	How protocol is handled
	• The connection in the state table hasn't expired. • The response comes from the same remote IP address and port where the request was sent.
DHCP	Query/response matching makes sure that return packets are allowed only for legitimate queries. Thus incoming DHCP responses are allowed if: • The connection in the state table hasn't expired. • The response transaction ID matches the one from the request.

Using trusted networks to allow traffic automatically

Trusted networks are IP addresses, IP address ranges, and subnets that your organization considers safe.

Defining a network as trusted causes Firewall to create an internal bi-directional **Allow** rule with remote network criteria set to the trusted network. Any traffic to and from the trusted networks is allowed.

Using trusted executables and applications to reduce false positives

Trusted executables are executables that have no known vulnerabilities and are considered safe. Firewall allows network traffic initiated from trusted executables.

Configuring a trusted executable creates a bi-directional **Allow** rule for that executable at the top of the Firewall rules list.

Note

Firewall treats all files and folder names in rules as case insensitive. For example, if the path for a trusted executable is C:\Temp\FTP.exe, Firewall also allows C:\temp\ftp.exe and c:\TEMP\FTP.EXE.

Maintaining a list of safe executables for a system reduces or eliminates most false positives. For example, when you run a backup application, many false positive events might be triggered. To avoid triggering false positives, make the backup application a trusted executable.

Note

A trusted executable is susceptible to common vulnerabilities, such as buffer overflow and illegal use. So, Firewall still monitors trusted executables and triggers events to prevent exploits.

The **Firewall Catalog** contains executables and applications. Executables in the catalog can be associated with a container application. You can add executables and applications from the catalog to your list of trusted executables. Once defined, you can reference the executables in rules and groups.

Using the Firewall Catalog to reference existing items

The **Firewall Catalog** simplifies the process of creating firewall rules and groups by enabling you to reference existing rules, groups, network options, applications, executables, and locations.

When referencing a catalog item, you create a dependent link between it and a firewall rule or group. Any change to the item in the catalog also changes the item wherever it is used. You can remove the dependency by breaking the link.

The **Firewall Catalog**, found in Trellix ePO - On-prem under **Policy**, includes previously added firewall rule and firewall group items. You can add items individually to the catalog by linking items from firewall and rule groups. You can also import items from XML-format exports of **Rules** policies.

Firewall protocols

Firewall protection works at several layers of the network architecture, where different criteria are used to restrict network traffic. This architecture is built on the TCP/IP suite.

Link layer

The link layer protocol describes the media access control (MAC) method, and some minor error-detection facilities.

Ethernet LAN (802.3), wireless Wi-Fi (802.11x), and virtual LAN (VPN) are in this layer. Both firewall rules and groups distinguish between wired, wireless, and virtual links.

Network layer

The network layer protocols define whole-network addressing schemes, routing, and network control schemes.

It also supports arbitrary non-IP protocols, but can't detect any network or transport layer parameters for them. At best, this layer allows the administrator to block or allow these network layer protocols. The numbers associated with the non-IP protocols are based on the Ethernet numbers defined by the Internet Assigned Numbers Authority (IANA).

Firewall offers full support for IPv4 and IPv6 on Microsoft Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows 8, and Windows 10.

Transport layers

IP can be used as the network protocol for many transport protocols. In practice, four are commonly used:

TCP	TCP is a connection-oriented, reliable transport protocol. It guarantees that the data contained in network packets are delivered reliably, and in order. It also controls the rate at which data is received and transmitted. This control requires a certain

	amount of overhead, and makes the timing of TCP operations unpredictable when network conditions are suboptimal. TCP is the transport layer for most application protocols. HTTP, FTP, SMTP, RDP, SSH, POP, and IMAP all use TCP. TCP multiplexes between application-layer protocols using the concept of "ports." Each TCP packet contains a source and destination port number, from 0–65535. Usually, the server end of a TCP connection listens for connections on a fixed port. Ports 0–1023 are reserved as "well-known ports." The IANA assigns numbers in this range to protocols. Most operating systems require a process to have special permissions to listen on one of these ports. Firewall rules are constructed to block certain ports and allow others, limiting the activities that can occur on the network.
UDP	User Datagram Protocol is a connectionless best-effort transport protocol. It makes no guarantees about reliability or packet order, and lacks flow control features. In practice, it has some desirable properties for certain classes of traffic. UDP is often used as a transport protocol for performance-critical applications. It is also used in real-time multi-media applications. A dropped packet causes only a momentary glitch in the datastream and is more acceptable than a stream that stops to wait for retransmission. IP telephony and videoconferencing software often uses UDP, as do some multi-player video games. The UDP multiplexing scheme is identical to that of TCP: each datagram has a source and destination port, ranging from 0–65535.
ICMP	Internet Control Message Protocol, version 4 (ICMPv4) and version 6 (ICMPv6), is used as an out-of-band communication channel between IP hosts. It is useful in troubleshooting, and needed for the proper function of an IP network, because it is the error reporting mechanism.

	IPv4 and IPv6 have separate, unrelated ICMP protocol variants. ICMPv4 is often called simply ICMP. ICMPv6 is important in an IPv6 network. It is used for several critical tasks, such as neighbor discovery (which ARP handles in an IPv4 network). Users are discouraged from blocking ICMPv6 traffic if IPv6 is supported on their network. Instead of port numbers, both versions of ICMP define message types. *Echo Request* and *Echo Reply* are used for ping. *Destination Unreachable* messages indicate routing failures. ICMP also implements a Traceroute facility, though UDP and TCP can also be used for this purpose.
Other transport protocols	IP supports over a hundred other transport protocols, but most are rarely used. The complete list of IANA-recognized protocols is at least minimally supported. Rules can be created to block or allow traffic over all IP transport protocols. But, the firewall doesn't support any multiplexing mechanism that these protocols might use. Several are used to overlay other types of networks on top of an IP network (network tunneling). Some of these protocols (notably GRE, AH, and ESP) are used for IP encryption and VPNs. See Protocol numbers for the IP protocol numbers.

Common unsupported protocols

There are several network protocols that Firewall doesn't support. Traffic belonging to these protocols, usually with an unparsable EtherType, is always blocked or always allowed, depending on the selection in the **Options** settings.

How Adaptive mode affects Firewall

In Adaptive mode, Firewall automatically allows all traffic that doesn't match an existing Block rule, and creates dynamic Allow rules for that non-matching traffic.

When Firewall is running normally, it continually monitors the network traffic that a computer sends and receives. Firewall allows or blocks traffic based on the rules. If the traffic can't be matched against an existing rule, it is automatically blocked.

You can create an explicit Allow rule for any traffic. For security reasons, incoming pings (ICMP traffic) are blocked in Adaptive mode unless an explicit Allow rule is created for it. Incoming traffic to a port that isn't open on the host is also blocked unless an

explicit Allow rule is created for the traffic. For example, if the telnet service isn't running, incoming TCP traffic to port 23 (telnet) is blocked automatically.

Firewall displays the rules created on client systems through Adaptive mode, and enables you to save and migrate these administrative rules.

Stateful filtering

When Adaptive mode is applied with the stateful firewall, the filtering process creates a rule to handle the incoming packet:

1. The firewall compares an incoming packet against entries in the state table and finds no match, then examines the static rule list and finds no match.
2. No entry is made in the state table, but if the packet is a TCP packet, it is put in a pending list. If not, the packet is dropped.
3. If new rules are permitted, a unidirectional static Allow rule is created. If the packet is a TCP packet, an entry is made in the state table.
4. If a new rule isn't permitted, the packet is dropped.

FAQ — Trellix GTI and Firewall

Here are answers to frequently asked questions.

Firewall **Options** settings in the **Trellix GTI Network Reputation** section enable you to block incoming and outgoing traffic from a network connection based on Trellix GTI reputation.

What is Trellix GTI ?

Trellix GTI is a global Internet reputation intelligence system that determines what is good and bad behavior on the Internet. Trellix GTI uses real-time analysis of worldwide behavioral and sending patterns for email, web activity, malware, and system-to-system behavior. Using data obtained from the analysis, Trellix GTI dynamically calculates reputation scores that represent the level of risk to your network when you visit a webpage. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images.

For frequently asked questions about Trellix GTI , see KB53735.

How does Trellix GTI work with Firewall?

Firewall uses the value of the **Incoming network-reputation threshold** and **Outgoing network-reputation threshold** options to create internal rules on the client system. If incoming or outgoing traffic matches these rules, Firewall queries Trellix GTI for the reputation of the source or destination IP address. Firewall uses this information to determine whether to block incoming or outgoing traffic.

- **Treat match as intrusion** — Treats traffic that matches the Trellix GTI block threshold setting as an intrusion and displays an alert.
- **Log matching traffic** — Treats traffic that matches the Trellix GTI block threshold setting as a detection and displays an event in the **Event Log** on the Trellix Endpoint Security (ENS) Client. Firewall also sends an event to Trellix ePO - On-prem.

If incoming or outgoing traffic matches these rules, Firewall queries Trellix GTI for the File reputation. Firewall uses this information to determine whether to block incoming or outgoing traffic from executables.

- **Block all untrusted executables** — Blocks network activity from all executables that are not signed, have invalid signatures, or have unknown reputations (Disabled by default).
- **Enable Observe mode** — Tracks the untrusted executables and send events to Trellix ePO - On-prem, but doesn't block the executables (Disabled by default).

Note

This option is available only in Trellix ePO - On-prem.

What do you mean by "reputation"?

For each IP address on the Internet, Trellix GTI calculates a reputation value. Trellix GTI bases the value on sending or hosting behavior and various environmental data collected from customers and partners about the state of Internet threat landscape. The reputation is expressed in four classes, based on our analysis:

- **Do not block** (minimal risk) — This is a legitimate source or destination of content/traffic.
- **High Risk** — This source/destination sends or hosts potentially malicious content/traffic that Trellix considers risky.
- **Medium Risk** — This source/destination shows behavior that Trellix considers suspicious. Any content/traffic from the site requires special scrutiny.
- **Unverified** — This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is needed.

Does Trellix GTI introduce latency? How much?

When Trellix GTI is contacted to do a reputation lookup, some latency is inevitable. Trellix does everything possible to minimize this latency. Trellix GTI :

- Checks reputations only when the options are selected.
- Uses an intelligent caching architecture. In normal network usage patterns, the cache resolves most wanted connections without a live reputation query.

If Firewall can't reach the Trellix GTI servers, does traffic stop?

If Trellix GTI is not reachable, you can configure Firewall to either block all traffic by default or allow traffic unless firewall rules specifically block it.

Firewall additions to Trellix ePO - On-prem

This managed product extends your ability to secure your network with these features and enhancements.

Important

You must have appropriate permissions to access most features.

Trellix ePO - On-prem feature	Addition	Management platform
Actions	Actions that you can perform from the **System Tree** or use to customize automatic responses.	All
Client tasks	Client tasks that you can use to automate management and maintenance on client systems.	All
Dashboards	• Dashboards and monitors that you can use to keep watch on your environment.	• All
	• Custom dashboards	• Trellix ePO - On-prem
Events and responses	• Events for which you can configure automatic responses. • Event groups and event types that you can use to customize automatic responses.	All
Permissions sets	**Endpoint Security Firewall**, **Endpoint Security Firewall Catalog**, and **Endpoint Security Firewall Client** permission categories, available in all existing permission sets.	Trellix ePO - On-prem
Policies	**Options** and **Rules** policy categories in the **Endpoint Security Firewall** product group.	• All
	• Custom policies	• Trellix ePO - On-prem
Queries and reports	Query names include the module name for easier filtering.	• All

Trellix ePO - On-prem feature	Addition	Management platform
	• Default queries that you can use to run reports.	
	• Custom property groups based on managed system properties that you can use to build your own queries and reports.	• Trellix ePO - On-prem
Server tasks	**Endpoint Security Firewall Property Translator** server task that translates Firewall client rules in the client properties stored in the Trellix ePO - On-prem database, and adds them to the **Firewall Client Rules** page.	Trellix ePO - On-prem
Firewall Client Rules	**Firewall Client Rules** under **Reporting** displays firewall client rules created on a client system to allow activity that a firewall rules blocks.	All
Firewall Catalog	**Firewall Catalog** under **Policy** displays items in the **Firewall Catalog** and lets you edit, create, delete, and export them.	All

For information about these features, see the Trellix ePO - On-prem documentation.

Permission sets and Firewall (Trellix ePO - On-prem)

Permission sets define rights for managed product functionality in Trellix ePO - On-prem.

Firewall adds the **Endpoint Security Firewall**, **Endpoint Security Firewall Catalog**, and **Endpoint Security Firewall Client** permission groups to each permission set.

Permission groups define the access rights to the features. Trellix ePO - On-prem grants all permissions for all products and features to global administrators. Administrators then assign user roles to existing permission sets or create permission sets.

Your managed product adds these permission controls to Trellix ePO - On-prem.

Permissions sets	Default permissions
Executive Reviewer **Endpoint Security Firewall**, **Endpoint Security Firewall Catalog**, and **Endpoint Security Firewall Client**	No permissions
Global Reviewer **Endpoint Security Firewall**	Views policy and task settings.
Global Reviewer **Endpoint Security Firewall Catalog** and **Endpoint Security Firewall Client**	No permissions
Group Admin **Endpoint Security Firewall**, **Endpoint Security Firewall Catalog**, and **Endpoint Security Firewall Client**	No permissions
Group Reviewer **Endpoint Security Firewall**, **Endpoint Security Firewall Catalog**, and **Endpoint Security Firewall Client**	No permissions

This managed product grants **No Permissions** by default.

Permissions must be granted for users to access or use permission-controlled features.

Permissions required per feature

Feature	Required permissions
Automatic Responses	**Automatic Responses**, **Event Notifications**, **Client Events**
Client events and client rules	**Systems**, **System Tree** access, **Threat Event Log** **General** in the **Endpoint Security Firewall Client** permission group

Feature	Required permissions
Dashboards and monitors	**Dashboards**, **Queries**
Policies	**Endpoint Security Firewall: Firewall** in the **Endpoint Security Firewall** permission group
Queries	**Queries & Reports**
Server tasks	**Server Tasks**
System Tree	**Systems**, **System Tree** access
Threat Event Log	**Systems**, **System Tree** access, **Threat Event Log**

For information about managing permission sets, see the Trellix ePO - On-prem documentation.

Client tasks and Firewall

Automate management or maintenance on managed systems using client tasks.

Depending on your permissions, you can use default client tasks as is, edit them, or create client tasks using Trellix ePO - On-prem.

Firewall leverages the following default Trellix Agent client tasks.

Trellix Agent default client tasks

Client task	Description	Management platform
Product Deployment	Deploys Trellix products to client systems.	Trellix ePO - On-prem
Product Update	Updates content files, engines, and all Trellix products automatically.	All

For information about client tasks and the **Client Task Catalog**, see the Trellix ePO - On-prem documentation.

Web Control

Supported and unsupported browsers

Web Control supports Microsoft Edge, Microsoft Chromium Edge, Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer.

Note

The Web Control plug-in has access to all data in the browser, including potentially sensitive information such as passwords and credit card information. But, Web Control doesn't store this data.

Web Control supports these browsers and versions:

- Edge — Current version

  Note

  Web Control supports Edge browser on Windows 10 Creators Update (15063) and later only.

- Chromium Edge — Current version
- Chrome — Current version. Chrome doesn't support the **Show Balloon** option
- Firefox — Current version, including multi-process architecture (E10S)
- Firefox ESR (Extended Support Release) — Current version and previous version
- Internet Explorer 11

Because Microsoft, Google, and Mozilla release new versions frequently, Web Control might not work with a new update. A Web Control update is released as soon as possible to support the changes to Edge, Chromium Edge, Chrome, or Firefox.

For the latest information about browsers that Web Control supports, see KB82761.

Note

(Self-managed systems) All browsers — supported and unsupported — are allowed by default.

Identifying threats while browsing

When users browse to a website, a color-coded button  appears in the browser. The color of the button corresponds to the safety rating for the site.

Note

The safety rating applies to HTTP and HTTPS protocol URLs only.

Edge, Chromium Edge, Chrome, and Firefox	Description
	This site is tested daily and certified safe by Trellix SECURE
	This site is safe.
	This site might have some issues.
	This site has some serious issues.
	No rating is available for this site. This button appears for FILE (file://) protocol URLs.
	A communication error occurred with the Trellix GTI server that contains rating information.
	Web Control didn't query Trellix GTI for this site, which indicates that the site is internal or in a private IP address range.
	This site is a phishing site. Phishing is an attempt to acquire sensitive information such as user names, passwords, and credit card details. Phishing sites masquerade as trustworthy entities in electronic communication.
	A setting allows this site.
	A setting disabled Web Control.

The location of the button depends on the browser:

- **Edge** — Right corner of the address bar
- **Chromium Edge** — Right corner of the address bar
- **Chrome** — Right corner of the address bar
- **Firefox** — Right corner of the address bar
- **Internet Explorer** — Web Control toolbar

Identifying threats while searching

When users type keywords into a search engine such as Google, Yahoo, Bing, or Ask, safety icons appear next to sites in the search results page. The color of the button corresponds to the site's safety rating.

	Tests revealed no significant problems.
	Tests revealed some issues that users might need to know about. For example, the site tried to change the testers' browser defaults, displayed pop-ups, or sent testers a significant amount of non-spam email.
	Tests revealed some serious issues that users must consider carefully before accessing this site. For example, the site sent testers spam email or bundled adware with a download.
	A Web Control setting blocked this site.
	This site is unrated.

Site reports provide details

Users can view the site report for a website to get detailed information about specific threats.

Site reports are delivered from the Trellix GTI ratings server and provide the following information.

This item...	Indicates...
Overview	The overall rating for the website, determined from these tests: • Evaluation of a website's email and download practices using proprietary data collection and analysis techniques.

This item...	Indicates...
	• Examination of the website itself to see if it engages in annoying practices such as excessive pop-ups or requests to change your home page. • Analysis of the website's online affiliations to see if it associates with other suspicious sites. • Combination of the Trellix review of suspicious sites with feedback from our Threat Intelligence services.
Online Affiliations	How aggressively the site tries to get you to go to other sites that Trellix flagged with a red rating. Suspicious sites often associate with other suspicious sites. The primary purpose of feeder sites is to get you to visit the suspicious site. A site can receive a red rating if, for example, it links too aggressively to other red sites. In this case, Web Control considers the site red by association.
Web Spam Tests	The overall rating for a website's email practices, based on the test results. Trellix rates sites based on how much email we receive after entering an address on the site, and how much the email looks like spam. If either measure is higher than what is considered acceptable, Trellix rates the site yellow. If both measures are high or one looks egregious, Trellix rates the site red.
Download Tests	The overall rating about the impact a site's downloadable software had on our test computer, based on the test results. Trellix gives red flags to sites with virus-infected downloads or to sites that add unrelated software considered by many to people be adware or spyware. The rating also considers the network servers that a downloaded program contacts during operation, and any changes to browser settings or computer registry files.

How Web Control blocks or warns about a site or download

When a user visits or accesses a resource from a site that has been blocked or warned about, Web Control displays a page or pop-up message indicating the reason.

If rating actions for a site are set to:

- **Warn** — Web Control displays a warning to notify users of potential dangers associated with the site.
- **Block** — Web Control displays a message that the site is blocked and prevents users from accessing the site.

If rating actions for downloads from a site are set to:

- **Warn** — Web Control displays a warning to notify users of potential dangers associated with the download file and allows user to block or continue with the download.
- **Block** — Web Control displays a message that the site is blocked and prevents the download.

Note

If the file reputation is not malicious, Web Control allows file downloads from a blocked site using the complete URL.

How Web Control and Skyhigh Client Proxy work together

Web Control can disable itself when operating inside your enterprise network to allow Skyhigh Client Proxy to perform web reputation checking.

Note

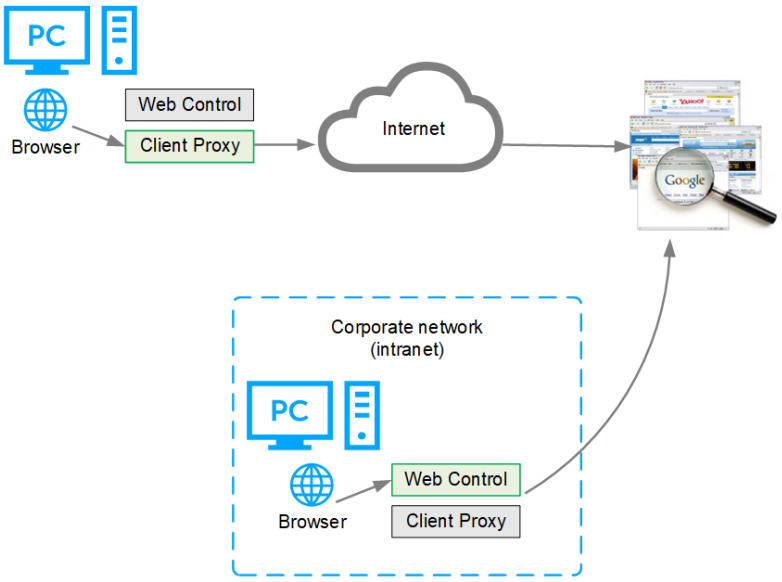
For Web Control to be disabled, the client system must meet the Client Proxy criteria set in the **MCP Policy** settings.

Web Control remains enabled unless both of the following are true:

- The **Disable if Skyhigh Client Proxy is detected** option is selected. If this option is not selected, Web Control remains enabled even if Client Proxy is redirecting.
- Client Proxy is redirecting. If Client Proxy is installed but not redirecting for some reason, such as network or license issues, Web Control is enabled.

When Web Control is configured to be disabled when Client Proxy is redirecting:

- When the client system is outside the internal network, Web Control is disabled and Client Proxy redirects network traffic.
- When the client system moves from outside to inside the internal network, Client Proxy stops redirecting and Web Control is reenabled.



When Web Control is disabled because Client Proxy is present and redirecting:

- Web Control ignores rating and enforcement actions.
- Web Control browser controls are disabled.
- Trellix Endpoint Security (ENS) Client **Status** page shows Web Control status as **Disabled**.
- Trellix Endpoint Security (ENS) Client **Settings** page indicates that Web Control is disabled because Client Proxy is detected.

How web gateway enforcement works

Web gateways protect users from threats with proactive analysis to filter malicious content from web traffic.

Gateways scan the webpage active content to understand behavior, predict intent, and protect against targeted attacks. If your organization uses a web gateway, you can specify that Web Control not enforce site ratings when a web gateway is detected.

Use one of these methods to configure Web Control to detect a web gateway.

- **Use your organization's default gateway** Web Control compares the client's default gateway IP address with the organization's gateway IP address specified in the policy. If the IP addresses match, the default gateway enforces network traffic, rather than Web Control.
- **Detect web gateway enforcement** Web Control tries to contact the respective site. If Web Control can't retrieve content from this site, a web gateway enforces network traffic, rather than Web Control. Your web gateway must block the site.
- **Specify internal landmark to use** If Web Control resolves the specified DNS name or IP addresses, it doesn't perform rating or enforcement actions.

Tip

Best practice: Enter both a DNS name and IP addresses.

- If you enter the DNS name, Web Control performs a DNS query (doesn't check the local cache) on the host name. If at least one IP address is detected, Web Control doesn't perform rating or enforcement actions.
- If you enter IP addresses, Web Control resolves the name for each address. If at least one valid host name is detected, Web Control stops processing and doesn't perform rating or enforcement actions.
- If you enter both a DNS name and IP addresses, Web Control performs a DNS query on the DNS host name and checks the result against the specified IP addresses. If it detects a match, Web Control doesn't perform rating or enforcement actions.

How safety ratings are compiled

A Trellix team develops safety ratings by testing criteria for each site and evaluating the results to detect common threats.

Automated tests compile safety ratings for a website by:

- Downloading files to check for viruses and potentially unwanted programs bundled with the download.
- Entering contact information into sign-up forms and checking for resulting spam or a high volume of non-spam email sent by the site or its affiliates.
- Checking for excessive pop-up windows.
- Checking for attempts by the site to exploit browser vulnerabilities.
- Checking for deceptive or fraudulent practices employed by a site.

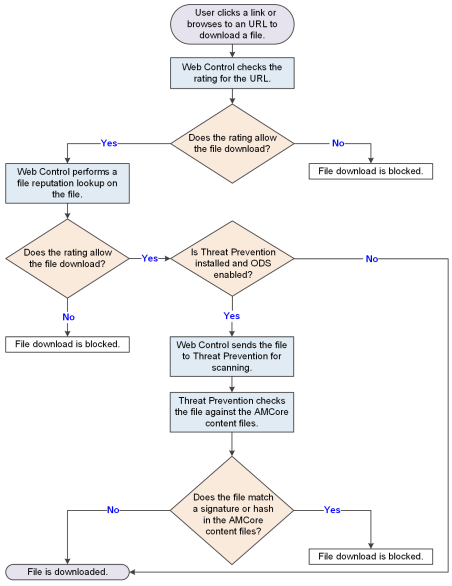
The team compiles test results into a safety report that can also include:

- Feedback submitted by site owners, which might include descriptions of safety precautions used by the site or responses to user feedback about the site.
- Feedback submitted by site users, which might include reports of phishing scams or bad shopping experiences.
- More analysis by Trellix experts.

The Trellix GTI server stores site ratings and reports.

How file downloads are scanned

Web Control sends file download requests to Threat Prevention for scanning before it allows files to be downloaded.



How Trellix GTI works

Trellix GTI stores site ratings and reports for Web Control. If you configure Web Control to scan downloaded files, the scanner uses Trellix GTI file reputation to check for suspicious files.

The scanner submits fingerprints of samples, or hashes, to a central database server hosted by Trellix Labs to determine if they are malware. By submitting hashes, detection might be available sooner than when Trellix Labs publishes the updated content file.

You can configure Trellix ENS to use a proxy server to retrieve Trellix GTI reputation information in the Common settings.

For frequently asked questions about Trellix GTI , see KB53735.

How Web Control works with Web Reporter

Web Reporter defines your browsing environment based on content categories and creates detailed reports on your organization's web use and trends.

Used with Web Control, Web Reporter provides the reports that help administrators manage access to the web. Use these reports to protect against liability exposure, productivity loss, bandwidth overload, and security threats. For detailed information about configuring and using Web Reporter to generate reports, see the Web Reporter documentation.

The Web Reporter server collects and processes log files and imports the data from the log file to the database. After the data is transferred to the database, reports are generated. Log files are generated by running a Web Control client task from the Trellix ePO - On-prem server on all managed systems.

Web Reporter groups

These groups of people are involved in the Web Reporter environment:

- **Web users** have installed and enabled in their browser.
- **Reporting users** create and view reports. Reporting users log on to the Web Reporter server with a web-based interface.
- **Reporting administrator** installs, configures, and maintains the Web Reporter server. The reporting administrator uses the web-based interface to manage how Web Reporter is used in the organization:
    - Creating logon accounts
    - Managing delegated reporting
    - Configuring email settings
    - Managing mapped columns
    - Managing the database, directories, and log sources

Web Reporter environment

The Web Reporter environment comprises these areas:

- **Web Reporter** is the server-based software with a web-based interface and configuration settings that create detailed reports.
- **Log sources** are devices on the network that generate or store log files. Log files contain web filtering data, including information such as user names, IP addresses, URLs, time stamps, and protocol types. Web Reporter collects and processes the log files, then imports the data into its database. A log source can be a directory on the Web Reporter server, an FTP server, or NetCache.
- **Database** stores data from each log source, and reports are generated using the data. Supported database platforms include Microsoft SQL 2000 and 2005, MySQL 5.0, and Oracle 9 and 10.

Information that the software sends to Trellix ePO - On-prem

Web Control sends information about browsing activity, including the actions taken, to the Trellix ePO - On-prem server. This information can be used in queries.

Web Control sends the following information:

- Type of event initiated by the managed system (site visit or download)
- Unique ID assigned to the managed system
- Time
- Domain
- URL
- Web Control rating for the event's site
- Whether the event's site or site resource is on the **Block and Allow List**
- Reason for action (allow, warn, or block) taken by the software
- Observe mode status (on or off)

The software sends the complete URL of the website to the Trellix GTI server.

When a managed system visits a website, Web Control tracks the URL. The URL is the smallest amount of information required for the software to uniquely identify the URL being rated for security. The focus of Web Control is protecting your managed systems; no attempt is made to track personal Internet use.

Note

Web Control doesn't send information about your company's intranet sites to the Trellix GTI server.

Web Control additions to Trellix ePO - On-prem

This managed product extends your ability to secure your network with these features and enhancements.

Important

You must have appropriate permissions to access most features.

Trellix ePO - On-prem feature	Addition	Management platform
Client tasks	Client tasks that you can use to automate management and maintenance on client systems. Use the **Send Web Reporter Logs** client task to transfer log files of browsing data from the client systems to the Trellix Web Reporter server.	All
Dashboards	• Dashboards and monitors that you can use to keep watch on your environment.	• All
	• Custom dashboards	• Trellix ePO - On-prem
Events and responses	• Events for which you can configure automatic responses. • Event groups and event types that you can use to customize automatic responses.	All
Managed system properties	Properties that you can review in the **System Tree** or use to customize queries.	All

Trellix ePO - On-prem feature	Addition	Management platform
Permissions sets	**Web Control** permission category, available in all existing permission set.	Trellix ePO - On-prem
Policies	• **Block and Allow List**, **Content Actions**, **Enforcement Messaging**, and **Options** policy categories in the **Endpoint Security Web Control** product group.	All
	• Custom policies	• Trellix ePO - On-prem
Queries and reports	Query names include the module name for easier filtering. • Default queries that you can use to run reports.	• All
	• Custom property groups based on managed system properties that you can use to build your own queries and reports.	• Trellix ePO - On-prem • Trellix ePO - SaaS

Permission sets and Web Control (Trellix ePO - On-prem)

Permission sets define rights for managed product functionality in Trellix ePO - On-prem.

Web Control adds the **Endpoint Security Web Control** and **Endpoint Security Web Control Query** permission groups to each permission set.

Permission groups define the access rights to the features. Trellix ePO - On-prem grants all permissions for all products and features to global administrators. Administrators then assign user roles to existing permission sets or create permission sets.

Your managed product adds these permission controls to Trellix ePO - On-prem.

Permissions sets	Default permissions
Executive Reviewer **Endpoint Security Web Control** and **Endpoint Security Web Control Query**	No permissions
Global Reviewer **Endpoint Security Web Control**	Views policy and task settings.
Global Reviewer Endpoint Security Web Control Query	No permissions
Group Admin **Endpoint Security Web Control** and **Endpoint Security Web Control Query**	No permissions
Group Reviewer **Endpoint Security Web Control** and **Endpoint Security Web Control Query**	No permissions

This managed product grants **No Permissions** by default.

Permissions must be granted for users to access or use permission-controlled features.

Permissions required per feature

Feature	Required permissions
Automatic Responses	**Automatic Responses**, **Event Notifications**, **Client Events**
Client events and client rules	**Systems**, **System Tree** access, **Threat Event Log**
Client tasks	**Endpoint Security Web Control: Tasks** in the **Endpoint Security Web Control** permission group
Dashboards and monitors	**Dashboards**, **Queries**

Feature	Required permissions
Policies	**Endpoint Security Web Control: Policy** in the **Endpoint Security Web Control** permission group
Queries	**Queries & Reports**
Server tasks	**Server Tasks**
System Tree	**Systems**, **System Tree** access
Threat Event Log	**Systems**, **System Tree** access, **Threat Event Log**

For information about managing permission sets, see the Trellix ePO - On-prem documentation.

Client tasks and Web Control

Automate management or maintenance on managed systems using client tasks.

Your managed product adds these client tasks to the **Client Task Catalog**. You can use client tasks as is, edit them, or create new ones.

Client task	Description
Send Web Reporter Logs	Sends logs to the configured Web Reporter server. Web Control collects logs of page view and file downloads. Then, Web Control sends this data to the configured Web Reporter server using the **Send Web Reporter Logs** client task. **Note:** Because large amounts of data that can be transferred when the logs are sent, we recommend setting the client task to run on a randomized schedule. See the settings for **Event Logging** in the **Options** policy to configure the Web Reporter server settings.

Web Control leverages the following default Trellix Agent client tasks.

Trellix Agent default client tasks

Client task	Description	Management platform
Product Deployment	Deploys Trellix products to client systems.	Trellix ePO - On-prem
Product Update	Updates content files, engines, and all Trellix products automatically.	All

For information about client tasks and the **Client Task Catalog**, see the Trellix ePO - On-prem documentation.

Frequently asked questions

Here are answers to frequently asked questions.

Policy enforcement

How can users hide their browsing activity?

- Create an application that browses the web.
- Create a frame page to load websites in a frame.
- Disable Web Control in Edge, Chrome, or Firefox by managing add-ons or extensions in the browser.
- Disable the plug-in from the **Choose Add-ons** pop-up window that Internet Explorer displays after Web Control is installed.

To protect against these situations:

- Use queries that track browsing behavior and usage. Queries alert you when managed systems show no browsing data or less browsing data than expected.
- Check the compliance status of the client software using the **Endpoint Security Web Control: Compliance Status** query. This query indicates when the software is disabled.

By setting up monitors that use the applicable queries, or frequently checking reports generated by queries, you know when users circumvent policy settings. You can then take immediate steps to ensure compliance.

Depending on the browser, use these additional steps to prevent disabling Web Control:

Edge

Add the Web Control extension Package Family Name (PFN) to the **Prevent turning off required extensions** Windows group policy.

The Web Control extension PFN is:

```
5A894077.McAfeeEndpointSecurityWebControl_wafk5atnkzcwy
```

For information about enabling this group policy, see *Prevent turning off required extensions* in Microsoft Edge Deployment.

Internet Explorer

Prevent users from disabling Web Control:

1. Enable Self Protection for Web Control in the Common **Options** policy.
2. Enable **Prevent users from uninstalling or disabling browser plug-in** in the Web Control **Options** policy.

Firefox and Chrome

Assign a policy to a group to automatically enable the Web Control plug-in.

For information, see KB87568.

Information tracking and reporting

If Edge or Internet Explorer is the only browser installed on a managed system when Web Control is deployed, must I redeploy the software after installing Firefox or Chrome?

No. Web Control detects both Firefox and Chrome when they are installed and immediately begins to protect searching and browsing activities in that browser, while continuing to protect Edge or Internet Explorer.

Color coding

Why is the Web Control button gray?

Several causes are possible:

- The site is not rated.
- The client software is disabled.

General

Is it safe to use Web Control as my only source of security against web-based threats?

No. Web Control tests many threats, and constantly adds new threats to its testing criteria, but it can't test for all threats. Users must continue to use traditional security defenses, such as virus and spyware protection, intrusion prevention, and network access control.

Adaptive Threat Protection

How file and certificate reputations control access

File and certificate reputations are based on their content and properties. The Adaptive Threat Protection settings determine whether items are blocked, contained, or allowed in your environment based on reputation levels.

Choose from three security levels depending on how you want to balance the rules for particular types of systems. Each level is associated with specific rules that identify malicious and suspicious files and certificates.

- **Productivity** — Systems that change frequently, often installing and uninstalling trusted programs and receiving frequent updates. Examples of these systems are computers used in development environments. Fewer rules are used with this setting. Users see minimum blocking when new files are detected.
- **Balanced**— Typical business systems where new programs and changes are installed infrequently. More rules are used with this setting. Users experience more blocking.
- **Security** — IT-managed systems with tight control and little change. Examples are systems that access critical or sensitive information in a financial or government environment. This setting is also used for servers. The maximum number of rules are used with this setting. Users experience even more blocking.

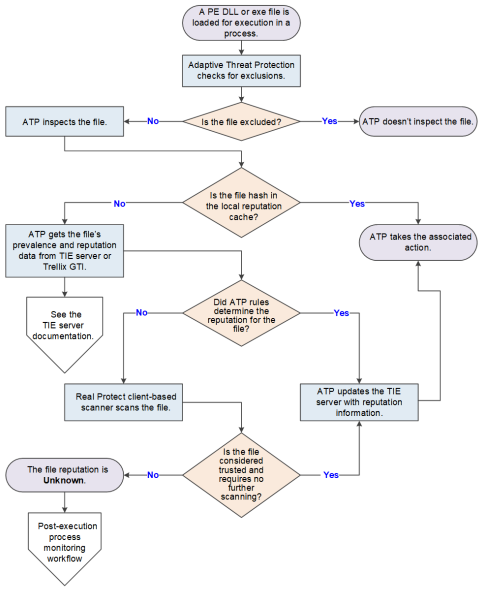
When determining which security level to assign, consider the type of system, and how much blocking you want the user to experience. Set the security level in the **Options** policy.

To view and change the state of specific rules associated with each security level, select **Menu** → **Server Settings**. From the **Setting Categories** list, select **Adaptive Threat Protection**.

How a reputation is determined

When determining the reputation of a file or certificate, Adaptive Threat Protection uses pre-execution scanning and post-execution monitoring.

Pre-execution process scanning



1. A portable executable (PE) DLL or exe file is loaded for execution in a process.
2. ATP checks the exclusions to determine whether to inspect the file.

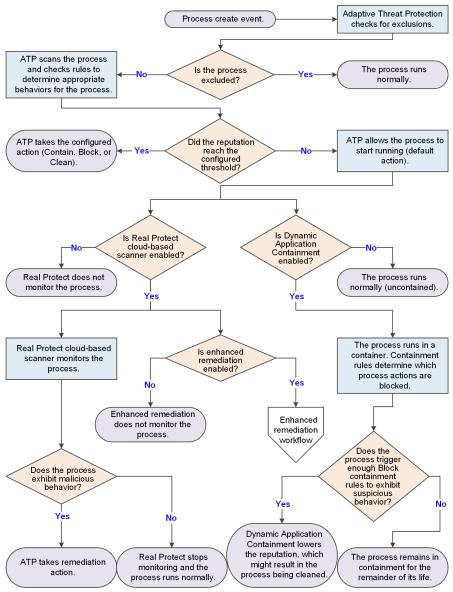
3. ATP inspects the file and gathers file and local system properties.
4. ATP checks the local reputation cache for the file hash.
    - If the file hash is in the local reputation cache, ATP gets the file's prevalence and reputation data from the cache and takes the associated action.
    - If the file hash isn't in the cache, ATP gets the file's prevalence and reputation data from the TIE server or Trellix GTI . For information, see the TIE server documentation.
    - If Sandbox server is present and enabled, see *If sandboxing is enabled* below.

    Note

    The Sandboxing option is available in Trellix ePO - SaaS only if TIE is licensed.

5. If ATP rules determine the reputation, ATP updates the TIE server with the latest reputation information and takes the associated action.
6. If ATP doesn't have the reputation, the Real Protect client-based scanner scans the file.
    - If the Real Protect client-based scanner determines the reputation, ATP updates the TIE server with the latest reputation information and takes the associated action.
    - If the Real Protect client-based scanner doesn't determine the reputation, the file reputation is **Unknown** (50). ATP might prompt the user, then allows the process to start and starts post-execution monitoring.

Post-execution process monitoring



1. The process is created and an event sent.
2. ATP checks the exclusions to determine whether to scan the process.

3. ATP scans the process and checks the Adaptive Threat Protection rules (listed in **Server Settings**) for the defined appropriate behaviors for the process.
4. If the process reputation reaches the configured threshold, ATP takes the configured action (Contain, Block, or Clean).
5. If the reputation remains below the configured threshold or ATP is in Observe mode, ATP allows the process to start running, monitoring it and preventing it from performing malicious behaviors.
6. If enabled, the Real Protect cloud-based scanner monitors the running process.
    - If the process exhibits malicious behavior, ATP takes remediation action. Otherwise, Real Protect cloud-based scanner continues monitoring the process until it determines the process is not malicious.
    - If the reputation is **Unknown** and enhanced remediation is enabled, it starts monitoring the behavior of the process and backs up changes that it makes to the system. See the *Enhanced remediation workflow* diagram. Real Protect continues monitoring the process until it determines the process is not malicious.
7. If Dynamic Application Containment is enabled, the process runs in a container. Containment rules determine the actions that the process can take. If the process triggers enough Block containment rules to exhibit suspicious behavior, Dynamic Application Containment lowers the reputation, which might result in the process being stopped and cleaned.

If sandboxing is enabled (Managed systems)

Note

The Sandboxing option is available in Trellix ePO - SaaS only if TIE is licensed.

If Sandbox server is present and enabled, the following process occurs.

1. If the file reputation is **Unknown** and the TIE server has access to Sandbox server, the TIE server sends the file to Sandbox server for scanning. Then, the TIE server keeps polling for analysis reports until they are available.
2. Sandbox server scans the file and sends file reputation results to the TIE server through the Trellix DXL . The server also updates the database and sends the updated reputation information to all ATP-enabled systems to immediately protect your environment. ATP or any other Trellix product can initiate this process. The TIE server processes the reputation and saves it in the database.

If Skyhigh Secure Web Gateway (SWG) for On-Prem is present (Managed systems)

If Skyhigh Secure Web Gateway (SWG) for On-Prem is present, the following occurs.

- When downloading files, Skyhigh Secure Web Gateway (SWG) for On-Prem sends a report to the TIE server that saves the reputation score in the database.
- When the server receives a file reputation request from the module, it returns the reputation received from Skyhigh Secure Web Gateway (SWG) for On-Prem and other reputation providers.

If Trellix Endpoint Security (ENS) Web Control is present

- When you download a file, Trellix Endpoint Security (ENS) Web Control sends a message to the TIE server with the URL of the download location, the URL reputation from Trellix GTI , and the hash value of the file. The information is available on the **Associated URL** tab on the hash information page.
- When the TIE server receives a file reputation request, it returns this information as part of its response.

File reputation versus process reputation

File reputation indicates the reputation of a file. Process reputation indicates the reputation of a running process and can change over time.

Pre-execution scanning and reputation sources, such as the TIE server and Trellix GTI , determine the reputation of a file. Multiple factors, including the reputation of the primary executable of the process and its parent, and post-execution scanning, determine the reputation of a process. Post-execution scanning includes Real Protect behavioral scanning, ATP rules, Dynamic Application Containment, and reputation updates from the TIE server.

The reputation of a process starts as the lowest local reputation of the primary executable of the process and its parent. For example, if a processes' parent has a reputation of **Unknown** (50) and its primary executable has a reputation of **Known Trusted** (99), the reputation of the process is **Unknown** (50).

A processes' reputation changes over time due to reputation update events and usually goes down. For example, if a process loads a library that initially has a local file reputation of **Unknown** (50), the reputation of the process is reduced to **Unknown** (50). Similarly, if post-execution scanning later deems the file **Known Malicious** (1), the scanner recalculates the process reputation to **Known Malicious** (1) and ATP takes the configured action for that reputation level for the process.

If ATP scanning is blocking processes that you want to allow to run, you can exclude them from scanning. If the TIE server is available, you can change the reputation of the file to a level that allows it to run, like **Known Trusted** (99), instead of creating exclusions.

When is the cache flushed?

Rule configuration defines when to flush the entire cache. Object state, reputation, or expiration date defines when to flush individual objects in the cache.

The whole Adaptive Threat Protection cache is flushed when the rule configuration changes:

- The state of one or more rules has changed, for example from **Enabled** to **Disabled**.
- The rule set assignment has changed, such as from **Balanced** to **Security**.

An individual file or certificate cache is flushed when:

- The file has changed on the disk.
- The TIE server publishes a reputation change event.
- The object expires. By default, items in the cache are flushed between 1 hour and 1 week, depending on type and reputation. Sometimes, the expiration time for an item might differ from the default.
    - The cache is full. Recently accessed cache items are retained; older items expire and are removed.
    - Time to live is set in the AMCore Content file or by the reputation provider.
    - Connection status in effect when the object was added to the cache. If an object was added when the reputation provider was not connected to the TIE server or Trellix GTI , the reputation is updated when connectivity is restored.

After the item is flushed from the cache, the next time Adaptive Threat Protection receives notice for the file, the reputation is recalculated.

How content files work

AMCore content files include updates to scanners, engines, and rules that Adaptive Threat Protection uses to dynamically compute the reputation and acceptable behavior of files and processes on client systems.

Trellix Labs adds rules to the content files. With the rules, content files include information about preventing malware behaviors. New threats appear, and Trellix Labs releases updated content files, regularly.

Trellix ENS stores the currently loaded content file and the previous two versions in the Program Files\Common Files\McAfee\Engine\content folder. If needed, you can revert to a previous version.

If Adaptive Threat Protection determines that a detection is a false positive, Trellix Labs might release a negative Extra.DAT file to suppress the detection until the next content update. Deploying a negative Extra.DAT is optional. If the TIE server is present, you can change the reputation score to eliminate the false positive. For information, see KB82922.

AMCore content package

Trellix Labs releases AMCore content packages daily by 7 p.m. / 19:00 (GMT/UTC). If a new threat warrants it, daily AMCore content files might be released earlier and, sometimes, releases might be delayed.

To receive alerts regarding delays or important notifications, subscribe to the Support Notification Service (SNS). See KB67828.

The AMCore content package includes these ATP components:

- **Adaptive Threat Protection — Scanner and rules** Contains updates to the scanner and ATP rules to dynamically compute the reputation of files and processes on the client systems. These rules appear in Trellix ePO - On-prem in the **Server Settings** → **Adaptive Threat Protection** page. You can change the state, for example **Enabled** or **Disabled** of non-**Mandatory** rules only. For information about ATP rules, including rule IDs and their corresponding rule names and descriptions, see KB82925. For information about the latest ATP content, see the Trellix TIE and ATP Security Content Release Notes.
- **Real Protect — Engine and content** Contains updates to the Real Protect scan engine and rules based on results of ongoing threat research. Real Protect is a component of the ATP module. To make sure that Trellix ENS uses the latest content files and engine, retrieve these files from Trellix and update your systems daily.

The version numbers for Adaptive Threat Protection content and Real Protect content appear in Trellix Endpoint Security (ENS) Client in the **About** page.

Best practice For answers to frequently asked questions about AMCore content files (V3 DAT), see KB82396.

Rules for ATP and the Threat Intelligence Exchange module for Trellix ENS or Threat Prevention

If you manage clients running Adaptive Threat Protection and the Threat Intelligence Exchange module for Trellix ENS or Threat Prevention from the same Trellix ePO - On-prem server, the rules displayed in the **Server Settings** page depend on the content checked in to the **Main Repository**. If the **AMCore Content Package** is checked in, ATP displays rules from that

package. Otherwise, ATP displays rules from the **Threat Intelligence Exchange module Content**. If neither are present in the **Main Repository**, the **Server Settings** page for Adaptive Threat Protection is blank.

ATP displays rules from only one content source.

Note

If an update to **Threat Intelligence Exchange module Content** includes changes to rules, those changes don't appear in **Server Settings** (and can't be edited) until **AMCore Content Package** is updated with those changes.

How ATP remediates threats

Adaptive Threat Protection monitors the behavior of files and processes with a reputation of **Unknown** (50) or lower. If a process exhibits malicious behavior, ATP performs remediation.

When the file or process reaches the configured reputation threshold, ATP performs the **Clean** action.

1. ATP traverses the process tree, stopping the last process that the convicted process created (such as the child or grandchild) and continuing to the process' ancestors (parent or grandparent). ATP doesn't stop processes that are:
    - Considered critical processes, such as services.exe and wininit.exe. ATP doesn't stop critical processes. If the critical process reputation is greater than 85 (**Most Likely Trusted**), ATP stops traversing the process tree, leaving the ancestor processes running. If the reputation is less than 85, ATP skips the critical process, but stops the ancestor processes.
    - Excluded in the Threat Prevention **On-Access Scan** → **Standard** exclusions settings. ATP doesn't stop excluded processes, but does stop the process' ancestors.
2. If enhanced remediation is enabled, ATP rolls back changes that the process made to the system.
3. ATP then stops the convicted process if it has a reputation of 50 or lower.
4. To prevent threats from persisting, ATP removes references to the convicted process, its ancestors, and descendants. Registry and file objects that ATP examines include registry keys, scheduled tasks (Windows Task Scheduler), services, shortcut files, and WMI (Windows Management Instrumentation) triggers and filters.
5. ATP quarantines objects that were removed from the registry associated with a convicted process so you can delete or restore them using a Trellix ePO - On-prem client task or from the **Quarantine** page of the Trellix Endpoint Security (ENS) Client.

Trellix ENS remediates threats differently, depending on whether the threat is a file or process (portable executable or DLL).

- **File remediation** If the detection is a file, the Threat Prevention on-access scanner or on-demand scanner handles the threat according to configuration settings. For example, Threat Prevention quarantines the file and you can delete or restore it. If the file is a portable executable (PE), ATP stops all processes (descendants and ancestors) associated with the PE file. If the PE file is a DLL, ATP also locates all processes that loaded the DLL and tries to eject the DLL from those processes. If the ejection is unsuccessful, ATP stops the processes, descendants, and ancestors.
- **Process remediation** ATP stops the process, its descendants, and ancestors.

How enhanced remediation protects systems

Enhanced remediation monitors the behavior of unknown processes and backs up changes that they make to the system. If a monitored process exhibits malicious behavior, enhanced remediation stops the process, its children, and ancestors, and rolls back the changes that it made, restoring the system as close as possible to its original state before the process ran.

With enhanced remediation, you can allow unknown processes to run in your environment, without being delayed or blocked, until the process shows malicious behavior. Allowing unknown processes to run in a controlled manner also enables the Real Protect machine-learning system to collect behavioral information for further malware analysis and reputation improvements.

For ATP to provide the backup and restore functionality, you must enable these two options in the Adaptive Threat Protection **Options** policy:

- **Clean when reputation threshold reaches**
- **Enable enhanced remediation**

Note

If enhanced remediation is *not* enabled, ATP stops convicted processes, descendants, and ancestors, deletes the main module of convicted processes, removes references from the registry and objects such as WMI, scheduled tasks, and shortcuts. It doesn't roll back changes that the process made.

What does enhanced remediation monitor?

Enhanced remediation monitors processes with a reputation of **Unknown** (50) or lower, unless excluded from ATP scanning.

If a process' reputation drops to 50 or lower while running, enhanced remediation starts monitoring the process. The reputation for a process can change when the ATP scanner detects that an unknown or malicious DLL was loaded into the process or if the reputation at the TIE server changes to **Unknown** or **Known Malicious**. For example, if the scanner detects that a malicious DLL is loaded into a trusted process, and its reputation drops to 50 or lower, enhanced remediation deletes the DLL, rolling back the changes to the process.

Enhanced remediation doesn't monitor:

- Processes with a reputation greater than 50
- Process path or file name exclusions specified in the Threat Prevention **On-Access Scan** → **Standard** exclusions settings
- Trusted installers, if **Scan trusted installers** is disabled in the Threat Prevention **On-Access Scan** settings
- Processes started from network locations

Note

If a monitored process starts a child process, enhanced remediation monitors that process even if its reputation is greater than 50 or it's excluded. The child process is not monitored if it's a trusted installer and **Scan trusted installers** is disabled.

How enhanced remediation works

If an unknown process is allowed to run based on other settings, enhanced remediation monitors the process and backs up changes that the process makes to the system, specifically:

- All files that the process creates.
- All files that the process changes or deletes (if the **Monitor and remediate deleted and changed files** option is enabled).
- All changes that the process makes to non-file objects, such as registry items, Windows Task Scheduler, Windows Services, and WMI (Windows Management Instrumentation) triggers and filters.

Note

If **Monitor and remediate deleted and changed files** is disabled and the malicious process *renames* a file, ATP deletes the file, during remediation. The reason for this is that the rename operation is actually a file-delete, which enhanced remediation doesn't monitor, and a file-create, which enhanced remediation does monitor.

As it runs, the ATP scanner and Real Protect scanner inspect the process. After a limited period, if the scanners don't detect malicious behavior, enhanced remediation stops monitoring the process.

If the scanners detect malicious behavior, enhanced remediation:

- Stops the process and rolls back the changes made by the convicted process.
- Rolls back tracked changes made by any *descendants* (such as the child or grandchild) that the convicted process started that meet the criteria for monitoring.
- Stops processes and rolls back changes for any *ancestor* (such as the parent or grandparent) of the convicted process that has a reputation of 50 or lower, unless they are considered critical processes.

For the convicted process and its family, enhanced remediation:

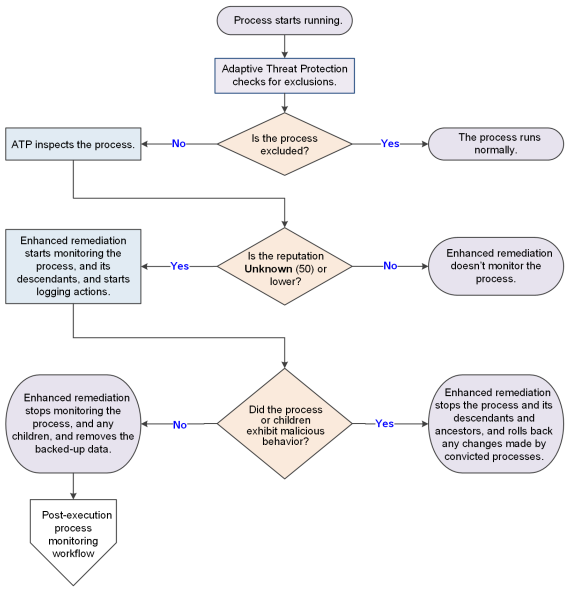
- Deletes all files created by the processes.
- Rolls back file changes made by the processes, if **Monitor and remediate deleted and changed files** is enabled.
- Restores files deleted by the processes, if **Monitor and remediate deleted and changed files** is enabled.
- Rolls back all changes that the processes made to non-file objects, such as registry items and Windows services.

ATP quarantines any files associated with the convicted process, so you can restore or clean.

If Observe mode is enabled, ATP reports the convicted process and the objects that would have been rolled back.

If the system restarts, enhanced remediation resumes any interrupted monitoring, backup, or rollback.

Enhanced remediation workflow



Enhanced remediation example

A process with a reputation of **Unknown** starts running on the system. Enhanced remediation starts monitoring the process and logging the changes that the process makes to the system. The process spawns several child processes, then encrypts 100 files. Real Protect observes the malicious behavior and recalculates the reputation of the process. When the reputation reaches **Known Malicious**, enhanced remediation stops the process and its descendants and ancestors, and rolls back all changes made to the system, including restoring the encrypted files.

Quarantine

When ATP performs the **Clean** action and enhanced remediation rolls back changes made by the convicted process, ATP quarantines objects associated with the convicted process, its ancestors, and descendants, including:

- The file associated with convicted process itself
- All objects that the processes created
- All objects that the processes changed, if **Monitor and remediate deleted and changed files** is enabled
- References to the process that ATP deleted from the registry

ATP doesn't quarantine objects that the convicted processes deleted. Instead, enhanced remediation restores them to their original locations on the system.

ATP places the objects in the Quarantine folder configured in the Threat Prevention **Options** settings.

Remediation backups and storage space considerations

Enhanced Remediation creates a folder called $MfeDeepRem to store the backup files.Because backing up all file changes might consume significant disk space and negatively impact performance, by default, enhanced remediation backs up only files that the process creates. To also back up changed and deleted files, enable the **Monitor and remediate deleted and changed files** option. Enabling this option can increase the amount of disk space that monitoring consumes and negatively impact

performance. With this option disabled, enhanced remediation can't roll back file changes and deletions. In addition, ATP deletes any files renamed by the malicious process.

Best practice: Disable **Monitor and remediate deleted and changed files** on server systems to reduce the disk space consumed by remediation backups.

ATP limits the amount of disk space that the remediation backups consume by purging the backups every 6 hours. When $MfeDeepRem folder size occupies more disk space, perform one of these actions to delete the folder:

- Disable **Self Protection** and delete the $MfeDeepRem folder to delete the folder temporarily. This folder regenerates while Enhanced Remediation is enabled for ATP.
- Disable **Enhanced Remediation** and delete the $MfeDeepRem folder to delete the folder permanently. This folder regenerates when you enable Enhanced Remediation.

ATP provides remediation details in the **Quarantine** page of the Trellix Endpoint Security (ENS) Client and in the activity log files on the client system (%ProgramData%\McAfee\Endpoint Security\Logs by default). ATP retains Story Graph details for up to 100 events for up to 90 days in the %ProgramData%\McAfee\Endpoint Security\ATP folder. See KB90859 for information on changing the event limit.

What happens when you disable enhanced remediation?

When you disable enhanced remediation:

- All backed-up data and disk usage are deleted.
- Because no backups are created, no rollback to previous states can happen.

Disabling **Clean when reputation threshold reaches** also disables enhanced remediation.

Even with enhanced remediation disabled, ATP stops the convicted process, its ancestors and descendants, and removes references to the convicted process from the registry and file objects, including registry keys, WMI, services, shortcuts, and scheduled tasks.

How false positive mitigation works

Trellix ENS and AMCore use false positive mitigation to prevent files from being incorrectly considered a threat (or convicted). This feature is available when either Threat Prevention or Adaptive Threat Protection are installed.

Some heuristic-based reputations providers might assess reputation scores that introduce false positives, such as when the reputation of a file is above **Unknown** (50), but below a trusted reputation level.

When Threat Prevention detects a threat, AMCore checks the reputation of the convicted file to determine whether to suppress the conviction. If the file has the reputation of **Might Be Trusted** (70) or higher, false positive mitigation suppresses the conviction. Trellix ENS also uses telemetry data in AMCore Content updates, which can include information from other sources, such as Trellix GTI and Trust DATs, to further mitigate false positives.

When false positive mitigation suppresses a conviction, Threat Prevention generates a False Positive Mitigation event (34928), displays it in the **Event Log** in Trellix Endpoint Security (ENS) Client, and sends it to the Trellix ePO - On-prem **Threat Event Log**.

False positive mitigation is always enabled by default. Disabling ATP or enabling ATP Observe mode doesn't disable false positive mitigation.

How Real Protect scanning monitors activity

The Real Protect scanner inspects suspicious files and activities on client systems to detect malicious patterns using machine-learning techniques. The scanner uses this information to detect zero-day malware.

The Real Protect technology is not supported on some Windows operating systems. See KB82761 for information.

The Real Protect scanner provides two options for performing automated analysis:

- On the client system
- In the cloud

Tip

Enable both client and cloud Real Protect options unless Technical Support advises you otherwise.

No personally identifiable information (PII) is sent to the cloud.

Client-based scanning

Client-based Real Protect uses machine learning on the client system to determine whether the file matches known malware. If the client system is connected to the Internet, Real Protect sends telemetry information to the cloud, but doesn't get automated analysis data from the cloud.

The client-based scanning sensitivity levels, which are based on mathematical formulas, assign "tolerance" to suspicious activity to assess whether the file matches known malware. The higher the sensitivity level, the more malware matches. But, allowing more detections might result in more false positives.

Sensitivity level	Recommended use
Low	Systems, such as servers, that rarely connect to the Internet or only to trusted websites (lower risk of infection). This setting results in fewer false positives.
Medium	Systems that don't meet the other criteria. (Default)
High	Systems with multiple users and unfiltered network access (higher risk of infection). This setting results in more false positives.

Client-based scanning requires Adaptive Threat Protection or TIE server connectivity unless offline scanning is enabled.

Tip

Because offline scanning might result in increased false positives, enable this option only for systems without connectivity to Trellix GTI or the TIE server.

Cloud-based scanning

Cloud-based Real Protect collects and sends file attributes and behavioral information to the machine-learning system in the cloud for malware analysis.

Cloud-based scanning requires connectivity to realprotect1.mcafee.com. See KB79640.

Tip

Disable cloud-based Real Protect on systems that aren't connected to the Internet.

How enhanced script scanning improves security

Real Protect enhanced script scanning includes integration with Antimalware Scan Interface (AMSI) to provide protection against non-browser-based scripts, such as PowerShell, JavaScript, and VBScript.

AMSI is a generic interface standard provided by Microsoft and supported on Windows 10, Windows Server 2016, and Windows 2019 systems. It allows applications and services to integrate with Adaptive Threat Protection, providing better protection against malware.

Tip

For the best protection against script-based threats, enable enhanced script scanning with Threat Prevention AMSI and ScriptScan, which scans browser-based scripts.

Supported operating systems

With enhanced script scanning enabled, the operating system determines how this feature analyzes the script:

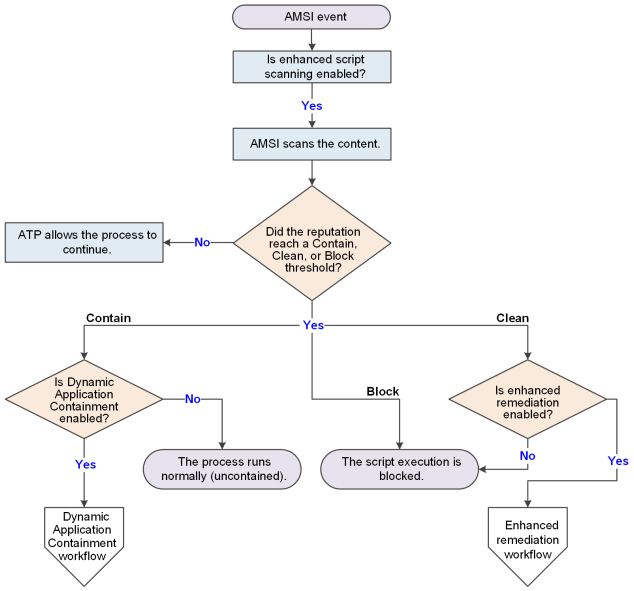
- Windows 10, Windows Server 2016, and Windows Server 2019 — AMSI blocks the script before execution.

Actions and exclusions

Enhanced script scanning uses settings from both Adaptive Threat Protection and Threat Prevention.

To specify:	Location	Module	Notes
Actions	**Action Enforcement** section in the **Options** settings	Adaptive Threat Protection	
Exclusions	**Standard** process types in the **Process Settings** section in the **On-Access Scan** settings	Threat Prevention	Most files that are excluded from on-access scans are also excluded from enhanced script scanning. Some scripts, such as PowerShell, are fileless and are not excluded from enhanced script scanning.

Enhanced script scanning workflow



Test Real Protect scanning

You can verify that Real Protect scanning features are installed correctly and that systems can communicate with Trellix cloud for detections.

Before you begin

- On endpoints managed with Trellix ePO - On-prem and Trellix ePO - SaaS — Verify that Real Protect can connect to Trellix GTI or the TIE server to send queries to the domain: realprotect1.mcafee.com.
- On unmanaged endpoints — Verify that Real Protect can connect to Trellix GTI to send queries to the domain: realprotect1.mcafee.com.

This test uses password-protected files to check Real Protect client-based and cloud-based detections. Although they are designed to be detected as threats, they are harmless.

You need to download the test files to a different location each time you run this test. Real Protect does not detect the files on subsequent attempts to run them from the same location.

Task

1. Make sure that Trellix ENS and Adaptive Threat Protection are running.
2. On the client system, download the compressed test file from this location: KB88828.
3. Navigate to the folder where you downloaded the file, then unzip the file.
   The password for the .zip file is `clean`. Password protection ensures that the .zip file is not blocked if you send it in an email.
4. To test client detections, double-click RP-S TestFile.exe.
   If Real Protect client scanning is functioning correctly in Trellix ENS, it detects the file and prevents the file from running.
5. To test cloud detections:

   Caution

   Don't disable the **Clean when reputation threshold reaches** option. If you disable this option, all active process detection including Real Protect cloud-based detection will not occur.

   a. In the Adaptive Threat Protection **Options** policy, under **Action Enforcement**, enable **Clean when reputation threshold reaches**. This option must be enabled for a Threat Event for RP-D to be generated on the endpoint.
   b. Double-click RP-D TestFile.exe.

   The RP-D TestFile.exe must run for a minute for the detection to trigger.
   If Real Protect cloud scanning is functioning correctly in Trellix ENS, it detects the file and prevents the file from running.

Results

If Real Protect does not detect the file and prevent it from running, check the Adaptive Threat Protection Activity log file and troubleshoot the problem, then run the test again. AdvancedThreatProtection_Activity.log is saved at this location by default: %ProgramData%\McAfee\Endpoint Security\Logs.

Real Protect test scan result codes

To verify that the Real Protect scanning feature is installed and working correctly, you can schedule a scan, then check that it completed successfully. Each time Real Protect completes a scan of a file, it creates an entry in the AdaptiveThreatProtection_Activity.log file with an ID that indicates the result of the scan.

AdvancedThreatProtection_Activity.log is saved at this location by default: %ProgramData%\McAfee\Endpoint Security\Logs

Real Protect ID	Description
0	Process found with clean reputation
1	Process found with unknown reputation
2	Time out
3	Unknown failure
4	Unsupported version of Real Protect
5	Not enough events
6	Managed product request does not scan
7	Phase 1 remediation is over
8	Process terminated
9	No network detected
10	Process restarted multiple times during a short period of time and no scan was performed
11	Process is cached with unknown reputation
12	ETW session is not available
13	Multiple DLL scan requests are issued for the same process

How Credential Theft Protection works

Credential Theft Protection (CTP) is designed to cease attacks that specifically targets Local Security Authority Subsystem Service (LSASS) or the lsass.exe process on Windows systems.

LSASS is responsible for enforcing security policy on Windows systems. It also stores credentials to:

- Verify users logging on to a Windows computer or server.
- Handles password changes.
- Creates access tokens.

The caching of credentials makes LSASS a potential target for credential theft; especially in the Windows 7 operating system, where credentials are stored in clear text format. Certain hacker tools explicitly target LSASS memory. CTP helps to curb the exposure of LSASS memory by blocking or redirecting attempts to open the lsass.exe process for reading.

How Adaptive Threat Protection protects against fileless attack methods

ATP and Threat Prevention provide technologies that protect against fileless attack methods in which no persistent malware file exists. Fileless attacks include network streaming of payloads and commands, abuse of dual-use applications, and live-off-the-land techniques.

Protection against fileless attack methods requires security around behaviors and activities instead of files and objects. Trellix ENS technologies offer layered security that enables you to catch fileless attacks at multiple points in the attack chain.

Detect malicious behaviors and activities with attack behavior blocking rules

ATP identifies fileless threats by observing suspicious behaviors and activities and blocking those activities. When ATP determines that the context of an execution is malicious, it blocks the malicious activity, and if necessary, remediates.

A set of ATP attack behavior blocking rules determines what processes can and can't do within a specific context to protect against fileless attack methods. For example, Microsoft Office applications generally aren't allowed to start script interpreting programs such as PowerShell and WScript because that's not a context in which IT administrators would start those types of programs.

Trellix releases new ATP rules in AMCore content. For information about the latest ATP content, see the Trellix TIE and ATP Security Content Release Notes.

For information about ATP rules, including rule IDs and their corresponding rule names and descriptions, see KB82925.

Scan obfuscated scripts

The Real Protect scanner inspects suspicious activities on client systems and uses machine-learning techniques to detect malicious patterns. The Real Protect scanner can scan a network-streamed script, determine if it's malicious, and if necessary, stop the script.

Real Protect script scanning integrates with AMSI to protect against non-browser-based scripts, such as PowerShell, JavaScript, and VBScript.

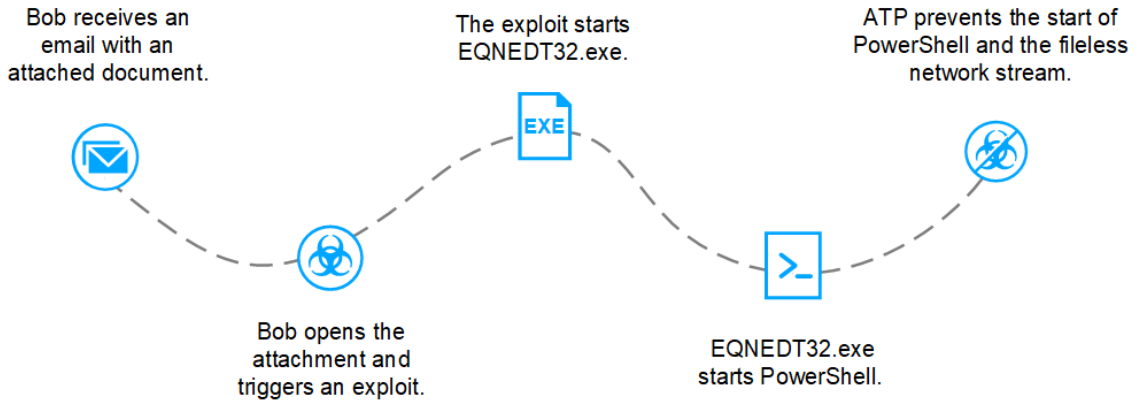
Visualize fileless threat detections

The Story Graph in the **Threat Event Log** provides a visual representation of fileless threat detections. You can examine the context of threats by reviewing the details of events leading up to a detection. The Story Graph helps you to identify what was executed, why ATP thinks it's malicious, where it came from, and where in the attack chain ATP stopped the threat.

Fileless attack example

Here's an example of a fileless attack:

1. Bob (user) receives a Microsoft Word document as an email attachment.
2. Bob opens the attachment and the malicious content triggers an exploit.
3. The exploit starts the Microsoft Equation Editor (EQNEDT32.exe).
4. EQNEDT32.exe uses the Command Prompt to start PowerShell to network stream payloads and commands to PowerShell.
5. ATP detects that EQNEDT32.exe starting PowerShell is not a normal activity and prevents the start of PowerShell. ATP stops the attack before the fileless network stream can start.



Trellix delivers updates to fileless protection technologies in AMCore content updates.

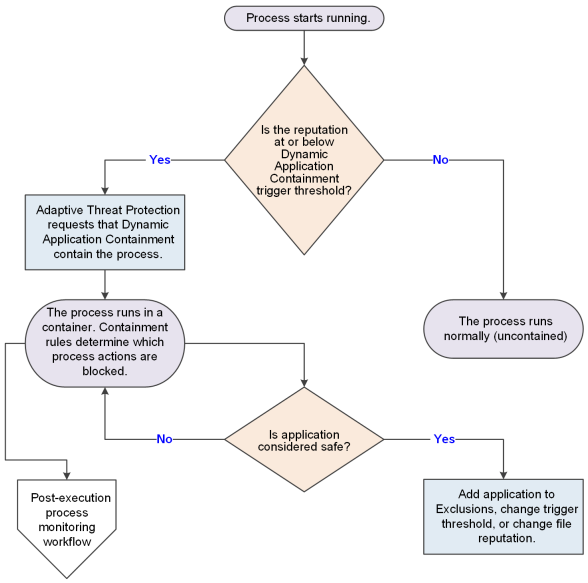
How Dynamic Application Containment works

Adaptive Threat Protection uses an application's reputation to determine whether Dynamic Application Containment runs the application with restrictions. Dynamic Application Containment blocks or logs unsafe actions of the application, based on containment rules.

As applications trigger containment block rules, Dynamic Application Containment uses this information to contribute to the overall reputation of contained applications.

Other technologies, such as McAfee® Active Response, can request containment. If multiple technologies registered with Dynamic Application Containment request to contain an application, each request is cumulative. The application remains contained until all technologies release it. If a technology that has requested containment is disabled or removed, Dynamic Application Containment releases those applications.

Dynamic Application Containment workflow



1. The process starts running.
2. If the reputation for the process, or a DLL dynamically loaded into the process, is at or below the containment reputation threshold, ATP notifies Dynamic Application Containment that the process has started and requests containment. If a DLL with a reputation at or below the containment threshold is dynamically loaded into the process ATP requests containment for the process, regardless of the process reputation.
3. Dynamic Application Containment contains the process.
   If configured, Dynamic Application Containment updates the **Event Log** in the Trellix Endpoint Security (ENS) Client and sends an event to Trellix ePO - On-prem, if applicable, to notify when:

   - An application has been contained.
   - A contained application attempts to violate the containment rules.

   You can view Dynamic Application Containment events in the **Threat Event Log** in Trellix ePO - On-prem.
4. If the contained application is considered safe, you can allow it to run normally (not contained).

Adaptive Threat Protection additions to Trellix ePO - On-prem

This managed product extends your ability to secure your network with these features and enhancements.

Important

You must have appropriate permissions to access most features.

Trellix ePO - On-prem feature	Addition	Management platform
Dashboards	• Dashboards and monitors that you can use to keep watch on your environment.	• Trellix ePO - On-prem • Trellix ePO - SaaS
	• Custom dashboards	• Trellix ePO - On-prem
Events and responses	• Events for which you can configure automatic responses. • Event groups and event types that you can use to customize automatic responses.	• Trellix ePO - On-prem • Trellix ePO - SaaS
Managed system properties	Properties that you can review in the **System Tree** or use to customize queries.	• Trellix ePO - On-prem • Trellix ePO - SaaS
Permissions sets	**Endpoint Security Adaptive Threat Protection** and **Endpoint Security Adaptive Threat Protection Query** permission categories, available in all existing permission sets.	Trellix ePO - On-prem
Policies	• **Dynamic Application Containment** and **Options** policy categories in the **Endpoint Security Adaptive Threat Protection** product group.	• Trellix ePO - On-prem • Trellix ePO - SaaS
	• Custom policies	• Trellix ePO - On-prem
Queries and reports	Query names include the module name for easier filtering.	• Trellix ePO - On-prem • Trellix ePO - SaaS

Trellix ePO - On-prem feature	Addition	Management platform
	• Default queries that you can use to run reports. • Custom property groups based on managed system properties that you can use to build your own queries and reports.	
Server settings	**Adaptive Threat Protection Server Settings** that you can use to customize settings for your managed product server.	• Trellix ePO - On-prem • Trellix ePO - SaaS
Adaptive Threat Protection Events	**Adaptive Threat Protection Events** under **Reporting** displays recent and past events for systems (devices), files, rules, and certificates.	• Trellix ePO - On-prem • Trellix ePO - SaaS

For information about these features, see the Trellix ePO - On-prem documentation.

Permission sets and Adaptive Threat Protection (Trellix ePO - On-prem)

Permission sets define rights for managed product functionality in Trellix ePO - On-prem.

Adaptive Threat Protection adds the **Adaptive Threat Protection** and **Adaptive Threat Protection Query** permission groups to each permission set.

Permission groups define the access rights to the features. Trellix ePO - On-prem grants all permissions for all products and features to global administrators. Administrators then assign user roles to existing permission sets or create permission sets.

Your managed product adds these permission controls to Trellix ePO - On-prem.

Permissions sets	Default permissions
Executive Reviewer **Endpoint Security Adaptive Threat Protection** and **Endpoint Security Adaptive Threat Protection Query**	No permissions
Global Reviewer	Views policy and task settings.

Permissions sets	Default permissions
Endpoint Security Adaptive Threat Protection	
Global Reviewer **Endpoint Security Adaptive Threat Protection Query**	No permissions
Group Admin **Endpoint Security Adaptive Threat Protection** and **Endpoint Security Adaptive Threat Protection Query**	No permissions
Group Reviewer **Endpoint Security Adaptive Threat Protection** and **Endpoint Security Adaptive Threat Protection Query**	No permissions

This managed product grants **No Permissions** by default.

Permissions must be granted for users to access or use permission-controlled features.

Permissions required per feature

Feature	Required permissions
Automatic Responses	**Automatic Responses**, **Event Notifications**, plus any feature-specific permissions depending on the feature used (such as **System Tree** or queries).
Dashboards and monitors	**Dashboards**, **Queries**
Policies	Adaptive Threat Protection Policy
Queries	**Queries & Reports**
Server tasks	**Server Tasks**
System Tree	Systems, **System Tree** access

Feature	Required permissions
Threat Event Log	Systems, **System Tree** access, **Threat Event Log**

For information about managing permission sets, see the Trellix ePO - On-prem documentation.

Server settings and Adaptive Threat Protection

Server settings provide options for configuring and customizing this managed product.

Your managed product adds these server settings to the Trellix ePO - On-prem server.

Server setting	Description
Adaptive Threat Protection	Displays the rules, and order they run, for each security level — Productivity, Balanced, and Security. You can set individual rules to **Enabled**, **Disabled**, or **Observe**.

Client tasks and Adaptive Threat Protection

Automate management or maintenance on managed systems using client tasks.

Depending on your permissions, you can use default client tasks as is, edit them, or create client tasks using Trellix ePO - On-prem.

Adaptive Threat Protection leverages the following default Trellix Agent client tasks.

Trellix Agent default client tasks

Client task	Description	Management platform
Product Deployment	Deploys Trellix products to client systems.	Trellix ePO - On-prem
Product Update	Updates content files, engines, and all Trellix products automatically.	• Trellix ePO - On-prem • Trellix ePO - SaaS

For information about client tasks and the **Client Task Catalog**, see the Trellix ePO - On-prem documentation.

Using Adaptive Threat Protection in your environment

You can configure settings and run Adaptive Threat Protection in Observe mode to determine how often a file is seen in your environment. You can then adjust settings or reputations, as needed.

1. Configure Adaptive Threat Protection settings to determine what is blocked, allowed, or contained.
2. Run Adaptive Threat Protection in Observe mode to build file prevalence and see what Adaptive Threat Protection detects in your environment. Adaptive Threat Protection generates `Would Block`, `Would Clean`, and `Would Contain` events to show what actions it would take. File prevalence indicates how often a file is seen in your environment. Observe mode applies to all Adaptive Threat Protection features, including Real Protect and Dynamic Application Containment.

   Caution

   Because enabling this mode causes Adaptive Threat Protection to generate events but not enforce actions, your systems might be vulnerable to threats.

3. Monitor and adjust settings, or individual file or certificate reputations, to control what is allowed in your environment.

Building file prevalence using Observe mode

You can build file prevalence to determine how often unknown files are seen in your environment.

You can see what is running in your environment and add file and certificate reputation information to the TIE server database. This information also populates the graphs and dashboards in Trellix ePO - On-prem where you view detailed reputation information about files and certificates.

To get started, configure Adaptive Threat Protection settings on a few systems in your environment. The settings determine:

- When a file or certificate with a specific reputation is allowed to run on a system
- When a file or certificate is blocked
- When an application is contained
- When or if users are prompted for what to do
- When a file is submitted to Sandbox server for further analysis

While building file prevalence, you can enable Observe mode on client systems. File and certificate reputations are added to the database and `Would Block`, `Would Clean`, and `Would Contain` events are generated, but no action is taken. You can see what Adaptive Threat Protection blocks, allows, or contains if the settings were enforced.

Monitoring and making adjustments

You can see files and certificates that are blocked, allowed, or contained based on the policies using dashboards and event views. If you have TIE server in your environment, you can use the TIE server extension in Trellix ePO - On-prem to view and change reputations.

You can view detailed information by endpoint, file, rule, or certificate, and quickly see the number of items identified and the actions taken. You can drill down by clicking an item, and adjust the reputation settings for specific files or certificates so that the appropriate action is taken.

For example, if a file's default reputation is suspicious or unknown but you know it's a trusted file, you can either exclude it from scanning or change its reputation to trusted. The application is then allowed to run in your environment without being blocked or prompting the user for action. You might change the reputation for internal or custom files used in your environment.

- Use the **TIE Reputations** feature to search for a specific file or certificate name. You can view details about the file or certificate, including the company name, SHA-1 and SHA-256 hash values, MD5, description, and Adaptive Threat Protection information. For files, you can also access VirusTotal data directly from the **TIE Reputations** details page to see additional information (see About VirusTotal).
- Use the **Reporting Dashboard** page to see several types of reputation information at once. You can view the number of new files seen in your environment in the last week, files by reputation, files whose reputations recently changed, systems that recently ran new files, and more. Clicking an item in the dashboard displays detailed information.
- If you identified a harmful or suspicious file, you can quickly see which systems ran the file and might be compromised.
- Import file or certificate reputations into the database to allow or block specific files or certificates based on other reputation sources. This allows you to use the imported settings for specific files and certificates without having to set them individually on the server.
- The **Composite Reputation** column on the **TIE Reputations** page shows the most prevalent reputation and its provider (TIE server 2.0 and later).
- The **Latest Applied Rule** column on the **TIE Reputations** page shows and tracks reputation information based on the latest detection rule applied for each file at the endpoint. You can customize this page by selecting **Actions** → **Choose Columns**.

For more information, see the TIE server documentation.

You can also use the Trellix GetClean tool, which uses Trellix GTI to report on files that are unknown to Trellix Labs, or falsely classified. Using GetClean, you can submit samples or metadata to Trellix Labs for whitelisting by Trellix GTI .

Submitting files for further analysis

If a file's reputation is unknown, you can submit it to Sandbox server for further analysis. Use the TIE server settings to specify which files you submit.

Sandbox server detects zero-day malware and combines anti-virus signatures, reputation, and real-time emulation defenses. You can send files automatically from Adaptive Threat Protection to Sandbox server based on their reputation level and file size. File reputation information sent from Sandbox server is added to the TIE server database.

Trellix GTI telemetry information

The file and certificate information sent to Adaptive Threat Protection is used to understand and enhance reputation information. See the table for details about the information provided by Adaptive Threat Protection for files and certificates, file-only, or certificate-only.

Category	Description
File and certificate	• TIE server and module versions • Reputation override settings made with the TIE server • External reputation information, for example from Sandbox server
File-only	• File name, type, path, size, product, publisher, and prevalence • SHA-1, SHA-256, and MD5 information • Operating system version of the reporting computer • Maximum, minimum, and average reputation set for the file • Whether the reporting module is in Observe mode • Whether the file was allowed to run, was blocked, contained, or cleaned • The product that detected the file, for example Sandbox server or Threat Prevention
Certificate-only	• SHA-1 information • The name of the certificate's issuer and its subject • The date the certificate was valid and its expiration date

Trellix does not collect personally identifiable information, and does not share information outside of Trellix.

Configuring with Trellix ePO - On-prem

Configuring common features

Policies and Common

Policies let you configure, apply, and enforce settings for managed systems in your environment.

Policies are collections of settings that you create, configure, and apply, then enforce. Most policy settings correspond to settings that you configure in the Trellix Endpoint Security (ENS) Client. Other policy settings are the primary interface for configuring the software.

Your managed product adds these categories to the **Policy Catalog**. The available settings vary in each category.

Common categories

Category	Description
Options	Configures general settings, including: • Specify client interface mode. • Require a password to uninstall the client. • Configure a time-based password. • Configure the client interface language. • Enable and disable Self Protection. • Specify processes to exclude from AAC. • Allow certificate authentication and upload third-party certificates. • Set up logging for client activity. • Configure proxy server settings. • Enable and disable default client updates. • Display managed custom tasks.

Customizing policies (Trellix ePO - On-prem)

Each policy category includes default policies.

You can use default policies as is, edit the **My Default** default policies, or create policies.

Common default policies

Policy	Description	Management platform
Trellix Default	Defines the out-of-the-box policy that takes effect if no other policy is applied. You can duplicate this policy, but you can't delete or change it.	All
My Default	Defines the customizable default policy for your environment. **Tip:** Modify this policy to create your own customized default.	Trellix ePO - On-prem

Comparing policies

In Trellix ePO - On-prem 5.0 and later, you can compare policies within the same policy category using **Policy Comparison**.

For information about policies and the **Policy Catalog**, see the Trellix ePO - On-prem documentation.

Protect services and files

One of the first things that malware attempts to do during an attack is to disable your system security software. To prevent services and files from being stopped or modified, configure Self Protection.

Caution

Disabling Self Protection leaves your system vulnerable to attack.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. From **Self Protection**, verify that **Self Protection** is enabled.
5. Specify the action for each of the following resources:
    - **Files and folders** — Prevents users from changing the Trellix database, binaries, safe search files, and configuration files.

- **Registry** — Prevents users from changing the Trellix registry hive, COM components, and uninstalling using the registry value.
- **Processes** — Prevents stopping Trellix processes.

6. Click **Save**.

Set up logging for client activity

You can configure activity, debug, and event logging, which you can use to determine if you need to change settings to enhance protection or improve system performance.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Configure **Client Logging** settings on the page.

   For more information on the **Client Logging** settings, see Advanced options in the *Trellix Endpoint Security (ENS) 10.7.x Interface Reference Guide*.

6. Click **Save**.

Control access to the client interface

You can set a password to control access to the Trellix Endpoint Security (ENS) Client.

⚠ Caution

Client Interface Mode is set to **Full access** by default, allowing users to change their security configuration, which can leave systems unprotected from malware attacks.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Configure **Client Interface Mode** settings on the page.
   Best practice: To improve security, change **Client Interface Mode** to **Standard** or **Lock client interface**. Both of these options require an Administrator password to access Trellix Endpoint Security (ENS) Client settings.
   Changing the Administrator password invalidates the time-based password. If you change the Administrator password, save the policy, then generate a new time-based password.
5. Click **Save**.

Effects of setting an administrator password

When you set the interface mode to **Standard access** or **Lock client interface**, you must also set an administrator password. The administrator can also generate a time-based password that users can enter for temporary access to the Trellix Endpoint Security (ENS) Client.

Setting the interface mode to **Standard access** or **Lock client interface** affects the following users:

All users	In **Lock client interface** mode, users must enter the administrator or temporary password to access the Trellix Endpoint Security (ENS) Client.In **Lock client interface** mode, users must enter the administrator password to access the Trellix Endpoint Security (ENS) Client. Once entered, the user has access to the whole interface, including configuration settings on the **Settings** page.
Non-administrators (users without administrator rights)	In **Standard access** mode, non-administrators can: • Get information about which Trellix products are installed, including version and status. • Check for updates (if enabled). • View the **Event Log**. • Get help and access the FAQ and Support pages. In **Standard access** mode, non-administrators can't view or change configuration settings on the **Settings** page.
Administrators (users with administrator rights)	In **Standard access** mode, administrators must enter the administrator or temporary password. In **Standard access** mode, administrators must enter the administrator password. Once entered, the administrator has access to the whole interface, including configuration settings on the **Settings** page.

Configure temporary access to the client interface

You can give temporary Administrator access to the client interface by generating a time-based password. Enable the time-based password for a limited set of systems to troubleshoot problems.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Standard access** or **Lock client interface**.

Tip

Best practice: During a security incident, disable the time-based password. After a security incident, change the Administrator password and regenerate the time-based password.

Changing the Administrator password invalidates the time-based password. If you change the Administrator password, save the policy, then generate a new time-based password.

If you enable a time-based password after a connectivity failure, then the Trellix Endpoint Security (ENS) Client will not accept the password.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the **Time-Based Administrator Password** section, select **Enable time-based password in client interface** and specify an expiration date and time. The maximum expiration time is 14 days.
   The expiration time is relative to the Trellix ePO - On-prem server. For example, if you set the expiration time to 1:00 p.m. PST, the password expires at 4:00 p.m. on client systems in the EST time zone.
6. Click **Generate New Password**.
   Two passwords are generated, one for Trellix ENS 10.5 and one for Trellix ENS 10.6 and later.
7. Write down the auto-generated password and provide it to users to allow temporary access.
8. Click **Save**.

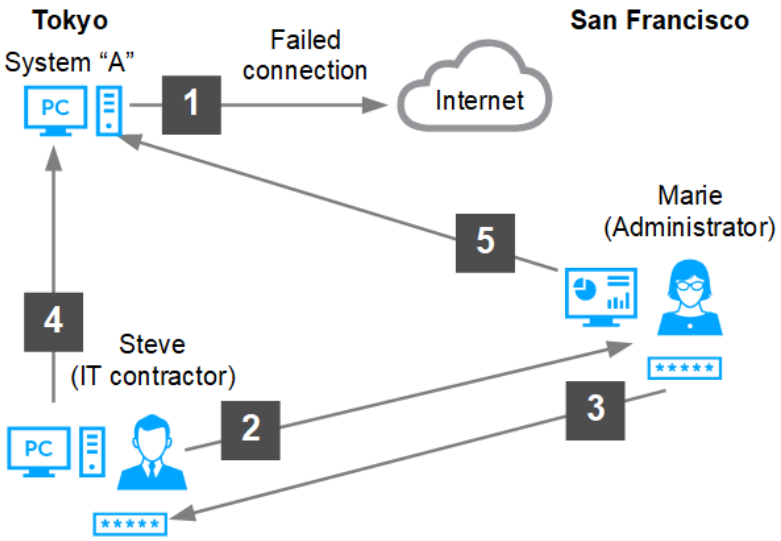
Example workflow for using a temporary password

In large organizations, IT contractors use endpoints for troubleshooting but do not have **Full access** rights for security reasons. Instead, the interface runs in **Standard access** mode.

In this example, the administrator provides a temporary time-based password so that the IT contractor can troubleshoot a connection issue. The administrator temporarily provides a password, granting **Full access** rights so that the contractor can view and change settings.

Note

This specific example covers a network connectivity issue, but using time-based passwords are useful for troubleshooting any configuration issues.



1. A new application is installed on System A in Tokyo, but it fails to connect to the Internet.
2. To troubleshoot the issue, Steve (IT contractor) contacts Marie (administrator in San Francisco).
3. From Trellix ePO - On-prem, Marie creates a time-based password, then sends it to Steve.
4. Steve uses the time-based password to disable the firewall and determines that a specific port must be open for the application to function properly.
5. Marie creates a special policy using the specific port number and assigns it to System A to solve the connection issue.

The time-based password expires and the restricted local access returns to normal.

Configure client interface lockout behavior

You can configure the number of failed passwords a user can enter before the user's account is temporarily locked out of the client interface.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Standard access** or **Lock client interface**.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the **Client Interface Mode** section, select **Enable client interface lockout**, then specify the maximum number of incorrect passwords and maximum lockout time.
   The client interface automatically unlocks after the maximum lockout time expires.
6. Click **Save**.

Unlock the client interface from Trellix ePO - On-prem

You can unlock user accounts that have been locked out of the interface due to multiple failed password attempts.

Before you begin

Make sure that the **Enable client interface lockout** option in the Common settings is enabled.

Task

1. Select **Menu** → **Reporting** → **Queries & Reports**.
2. From the list, select the **Endpoint Security: Locked Client Systems Due to Failed Password Attempts** query, then click **Actions** → **Run**.
3. Select the user accounts you need to unlock.
4. Click **Actions** → **Unlock Client Interface**.

Results

The interface is unlocked for the selected users.

Prevent AAC from blocking trusted programs

If a trusted program is blocked, exclude the process from AAC by creating a temporary global exclusion in the Common settings.

⚠ Caution

To avoid security risks, remove a global exclusion immediately after use. Failure to remove a global exclusion leaves your systems vulnerable to malware attacks.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the **Exclusions** section, click **Add**.
6. Enter the full process path.
   You can enter a local or UNC path. You can also include environment variables.
7. Enter at least one identifier.
   - **Process MD5 hash**
     - Open a command prompt.
     - Type `certutil.exe -hashfile "full process path" MD5`. For example: `certutil.exe -hashfile "c:\Windows\System32\icacls.exe" MD5`
     - Copy the MD5 hash and paste it in the **Process MD5 hash** field. Here is an example process MD5 hash: 24084debc1369b35e57f8efe0500a83d You might need to remove spaces inserted by certutil.exe.
   - **Signer certificate MD5 hash**
     - Open a command prompt with administrator rights.

- Type `"c:\Program Files\Common Files\McAfee\SystemCore\vtpinfo.exe" /validatemodule "full process path"`. For example: `"c:\Program Files\Common Files\McAfee\SystemCore\vtpinfo.exe" /validatemodule "c:\Windows\System32\icacls.exe"`
- Copy the signer certificate MD5 and paste it in the **Signer certificate MD5 hash** field. Here is an example signer certificate MD5 hash: 708ac5123ae46b4557a24225d3a8dbfc

8. Click **OK**, then click **Save**.

Excluding processes from AAC

Trellix ENS protection features, such as Self Protection and Access Protection, and other Trellix product protection rules, are enforced by a technology called Arbitrary Access Control (AAC). AAC rules protect objects, such as files, processes, and registry data, from being accessed by malware and untrusted programs.

For troubleshooting, you can temporarily exclude processes from all AAC rules by configuring a global exclusion policy setting. Use global exclusions only for specific troubleshooting and support purposes.

For example, to set up auditing on your Windows systems where specific Windows executables must have read/write access to the target directories, you can temporarily exclude those executables from the AAC rules.

Best Practice: For information about troubleshooting blocked third-party applications, see KB88482.

Considerations when specifying global exclusions

- You must specify at least one identifier: **Process MD5 hash** or **Signer certificate MD5 hash**.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match, the exclusion is invalid. For example, the file name and MD5 hash don't apply to the same file.
- Exclusions are case insensitive.
- Wildcards are not allowed.

Configure proxy server settings

You can specify proxy server options to redirect web traffic to a proxy server.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Configure **Proxy Server** settings on the page.

   When you select **Use system proxy settings**, the client system uses the proxy settings configured in Internet Explorer, including support for PAC files.

   Best practice: Exclude the Trellix GTI addresses from the proxy server. For information, see KB79640.

Note

While configuring the proxy server, enter the username in the format **username@domain.com**.

6. Click **Save**.

Results

Configure default behavior for updates

You can specify the default behavior for updates initiated from the Trellix Endpoint Security (ENS) Client in the Common settings.

Use these settings to:

- Show or hide the **Update** button in the client.
- Enable or disable the schedule for the **Default Client Update** task.
- Specify what to update when the user clicks the button or the **Default Client Update** task runs.

By default, the **Default Client Update** task runs every day at 1:00 a.m. and repeats every four hours until 11:59 p.m.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Configure **Default Client Update** settings on the page.
6. Click **Save**.

How the Default Client Update task works

The **Default Client Update** task downloads the most current protection to the Trellix Endpoint Security (ENS) Client.

Trellix ENS includes the **Default Client Update** task that runs every day at 1:00 a.m. and repeats every four hours until 11:59 p.m.

The **Default Client Update** task:

1. Connects to the first enabled source site in the list. If this site isn't available, the task contacts the next site until it connects or reaches the end of the list.
2. Downloads an encrypted CATALOG.Z file from the site. The file contains information required to perform the update, including available files and updates.
3. Checks the software versions in the file against the versions on the computer and downloads any new available software updates.

If the **Default Client Update** task is interrupted during the update:

Updates from...	If interrupted...
HTTP, UNC, or a local site	Resumes where the update left off the next time the update task starts.
FTP site (single-file download)	Doesn't resume if interrupted.
FTP site (multiple-file download)	Resumes before the file that was being downloaded at the time of the interruption.

Protecting Trellix processes from third-party DLLs

Software applications that run in Microsoft Windows environments can inject code into a third-party process. Trellix software considers third-party DLLs that are injected into Trellix processes to be *untrusted* because the code might be compromised or used maliciously.

Third-party DLL activity appears to originate from the injected Trellix process. If this activity is malicious, it looks like Trellix software is performing these malicious operations.

Trellix uses these technologies to protect against DLL injections:

- **Validation and Trust Protection (VTP) service** — Inspects DLLs and running processes that interact with Trellix code to verify whether objects are trusted.
- **Arbitrary Access Control (AAC) rules** — Determines whether to block or allow access to objects.

How the Validation and Trust Protection service works

The VTP service (MFEVTPS.exe) inspects DLLs and running processes that interact with Trellix code to verify whether objects are trusted.

An object is a network, file, registry, or process. Trusted means the third-party process is allowed to access Trellix objects. For example, a trusted third-party process is allowed to be injected into Trellix processes or to read Trellix registry keys.

To function properly, the VTP service depends on:

- Microsoft Cryptographic service (CryptSvc)
- Trust-related APIs
- Health of the certificate store or catalog files

Here's how the VTP service works:

1. A validation check runs when Trellix code needs to verify that the acting process is trusted, the target object is trusted, or both.

2. When Trellix processes are initialized, the VTP service validates that Trellix is loading trusted code. AAC makes sure that Trellix loads only trusted DLLs.

Only Trellix and Microsoft code are implicitly trusted.

Caching

The VTP service caches the results of a validation check to improve the performance of future validation checks. The VTP service always examines the cache first when performing a validation check.

- If a validation check returns a result that the object is not trusted, that object is cached as untrusted.
- If an object is cached incorrectly as untrusted, only a cache reset can correct it.

The cache resets when a system restarts in Safe Mode or by running this command:

`VTPInfo.exe /ResetVTPCache`.

You can also reset the cache from the DAT.

Trust failures

A trust failure is a VTP service validation check that results in "untrusted" when the expected result was "trusted." Trust failures occur because AAC denies access to untrusted code. The process is not allowed to access Trellix processes as a form of self-protection.

Here are some examples of trust failures:

- A Trellix process was injected by an untrusted third party, so the process fails a validation check.
- A Microsoft catalog-signed file has invalid signing information, so it can't be verified and fails to load by a Trellix process.
- A valid DLL file was cached incorrectly as "untrusted," and subsequent attempts to load it are denied.

All of these examples can cause the affected Trellix processes to fail.

How AAC works

AAC operates from the Windows kernel and can block access to network, file, registry, and process objects. Use AAC rules to determine what to block and allow.

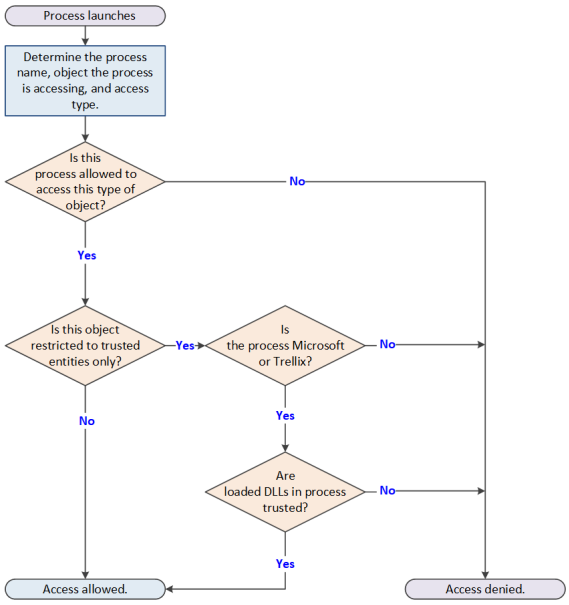
AAC rules can describe unsafe behaviors that must be blocked or denied.

AAC rules can be:

- Enabled or disabled
- Set to **Report only**
- Modified to add other processes to protect or to protect against
- Excluded to no longer block a certain process from violating the rule

Some rules are not exposed in the interface because they are critical to the operational health of the product.

AAC sees an operation that is attempting to run and follows this process.



If a validation check fails or produces an untrusted result, Trellix internal protections might block Trellix processes from accessing objects.

Validation failures

All code written by Trellix and Microsoft is inspected and validated. If those inspections result in a validation failure, it is possible that AAC might block Trellix processes. A validation failure can include certain trust failures and other types of unexpected failures.

Validation failure scenarios

When a Trellix process loads a third-party DLL, it contains third-party functions and can execute the third-party code. The third-party code resides in the Trellix process and can cause the Trellix process to perform unintended operations and result in a validation failure.

Validation failures can produce several symptoms, including these scenarios.

- A third-party process is blocked from accessing Trellix-protected files or processes.
- A third-party process that loads Trellix DLLs is blocked from accessing other Trellix processes, files, or folders. For example, Microsoft Outlook is blocked when it tries to access other Trellix processes.
- A Trellix process fails to start properly. For example, you are unable to start the Trellix Endpoint Security (ENS) Client despite installation logs indicating that startup was a success.
- A Trellix process is running, but is only partially operational. For example, a Trellix product loads successfully but indicates that other services are not running properly, yet the Trellix service is running.

- A Trellix process is blocked from accessing other files and folders belonging to a different Trellix product.

Failure to validate Trellix or Microsoft code indicates one of these scenarios occurred. If you experience one of these issues, contact technical support for help troubleshooting and to discuss solutions.

Managing third-party certificates

A process, called MFECanary.exe, runs as a child process to MFEEsp.exe and captures digital certificate detail for any DLL that attempts to inject into the MFECanary.exe process. The information is sent to Trellix ePO - On-prem from an agent event, which is processed by the Trellix ePO - On-prem server. It is then sent to the Trellix Endpoint Security (ENS) Common policy. From the policy, you can decide whether client systems trust or do not trust the third-party certificate. To trust it, you must add the digital signature to the certificate store.

Technical support can help in identifying the third-party certificate, obtaining the certificate file (.cer), and trusting a third-party digital certificate with signed third-party DLLs that are injected into Trellix processes.

For information about opening a Service Request or to expedite the processing of an escalation, see KB88085. For technical support contact details, go to ServicePortal and select your country from the drop-down list.

Considerations when trusting a third-party certificate

Trusting a third-party certificate can result in increased security risks.

The security implications of trusting a third-party certificate include:

- Code signed by the third-party certificate is trusted to interact with Trellix processes, files, registry, and all other Trellix-protected objects.
- File activity generated by processes signed with the third-party certificate might not be scanned.
- Any product or code releases from the same vendor using the same digital certificate automatically inherit the same trust or untrusted state.
- Any product or code releases from the same vendor using a different digital certificate must be trusted.

Tip

Best Practice: If the Endpoint Security Platform stops running, a third-party injection into Trellix code might be the cause. For information about troubleshooting this error, see KB88029.

Upload a third-party certificate

If you trust an uploaded certificate, the DLL of the certificate is allowed to be injected into a Trellix process.

Otherwise, the DLL of the certificate is not allowed to be injected into a Trellix process.

The certificate must be in one of these formats:

- .cer files (Base-64 encoded X.509 certificate)

- Plain text certificate content in Base-64 encoded X.509

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Click **Show Advanced**.
5. In the **Certificates** section, click **Upload Client Certificate**.
6. Select a certificate file (.cer) or provide certificate text in Base-64 encoded X.509 format.
7. Click **Save**.

Allow certificate authentication

Certificates allow a vender to run code within Trellix processes.

When a process is detected, an event is sent to Trellix ePO - On-prem and the certificate table is populated with the vendor, subject, and hash of the associated public key.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the **Certificates** section, select **Allow**.

Caution

This setting might result in compatibility issues and reduced security.

6. Click **Save**.

Results

The certificate information appears in the table.

Delete certificates from the certificate store

You can delete a trusted certificate from the certificate store when it's no longer used by other policies.

Important

When you remove a certificate from a duplicated policy, it is still used by other policies. To remove it from the certificate store, you must remove it from all policies where it is used.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Common** from the **Products** list in the left pane.

2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Click **Show Advanced**.
5. In the **Certificates** section, select the certificate you want to remove and click **Delete**.
6. Click **Save**.

Configuring Threat Prevention

Policies and Threat Prevention

Policies let you configure, apply, and enforce settings for managed systems in your environment.

Policies are collections of settings that you create, configure, and apply, then enforce. Most policy settings correspond to settings that you configure in the Trellix Endpoint Security (ENS) Client. Other policy settings are the primary interface for configuring the software.

Your managed product adds these categories to the **Policy Catalog**. The available settings vary in each category.

Threat Prevention categories

Category	Description
Access Protection	Prevents unwanted changes to the client system by restricting access to specified files, shares, registry keys, registry values, processes, and services.
Exploit Prevention	• Prevents unwanted changes to the client system by restricting access to files, shares, registry keys, registry values, processes, and services. • Prevents applications from executing arbitrary code. • Detects and prevents known network-based attacks.
On-Access Scan	Configures scheduled scanning of all processes, including maximum scan time and threat-detection message configuration.
On-Demand Scan	Configures preconfigured scans that run on the client system, including: • **Full Scan** and **Quick Scan** from the Trellix Endpoint Security (ENS) Client • **Right-Click Scan** on the client system

Category	Description
	• **Custom On-Demand Scan** client tasks, scheduled from Trellix ePO - On-prem
Options	Configures the settings that apply to both the on-access scanner and on-demand scanner.

Customizing policies (Trellix ePO - On-prem)

Each policy category includes default policies.

You can use default policies as is, edit the **My Default** default policies, or create policies.

Threat Prevention default policies

Policy	Description	Management platform
Trellix Default	Defines the default policy that takes effect if no other policy is applied. You can duplicate, but not delete or change, this policy.	All
My Default	Defines default settings for the category.	Trellix ePO - On-prem
On-Access Scan for Exchange	Defines an on-access scan policy with exclusions for Microsoft Exchange Server. This policy isn't applied until you assigned it to systems. For information, see Knowledge Base article KB51471.	All

Comparing policies

In Trellix ePO - On-prem 5.0 and later, you can compare policies within the same policy category using **Policy Comparison**.

For information about policies and the **Policy Catalog**, see the Trellix ePO - On-prem documentation.

Preventing Threat Prevention from blocking trusted programs, networks, and services

Threat Prevention enables you to fine-tune your protection by specifying items to exclude.

For example, you might need to exclude some file types to prevent a scanner from locking a file used by a database or server. A locked file can cause the database or server to fail or generate errors.

Best practice: To improve performance of on-access and on-demand scans, use scan avoidance techniques rather than adding file and folder exclusions.

Exclusions in exclusion lists are mutually exclusive. Each exclusion is evaluated separately from the others in the list.

Trellix ENS treats all file and folder exclusions as case insensitive — all case variations of the specified locations are excluded. For example, if you exclude C:\Temp\ABC, Trellix ENS also excludes C:\temp\abc and C:\TEMP\Abc.

Note

To exclude a folder on Windows systems, append a backslash (\) character to the path.

For this feature...	Specify items to exclude	Where to configure	Exclude items by	Use wildcards?
Access Protection	Processes (for all rules or a specified rule)	**Access Protection**	Process file name or path	Yes (* and ?)
			MD5 hash	No
			Signer	No
Exploit Prevention.	Processes	**Exploit Prevention**	Process file name or path	Yes (* and ?)
			MD5 hash	No
			Signer	No
			User SID	No
			Group SID	No
			User name	No
			Group name	No

For this feature...	Specify items to exclude	Where to configure	Exclude items by	Use wildcards?
			Hostname	Yes (* and ?)
	Caller modules		Caller module file name or path	Yes (* and ?)
			MD5 hash	No
			Signer	No
	APIs		API name	No
	Signatures		Signature ID	No
	IP addresses		IP addresses or ranges (IPv4 format)	No
	Services		Service name	No
All scans	Detection names	**Options**	Detection name (Exact name and case)	Yes (* and ?)
	Potentially unwanted programs		Name	Yes (* and ?)
On-access scan • **Standard** • **High Risk** • **Low Risk**	Files, file types, and folders	**On-Access Scan**	File name or path	Yes (* and ?)
			File type (extension)	Yes (*)
			File age	No
	ScriptScan URLs		URL name Partial URL	No

For this feature...	Specify items to exclude	Where to configure	Exclude items by	Use wildcards?
On-demand scan • **Quick Scan** • **Full Scan** • **Right-Click Scan**	Files, folders, and drives	**On-Demand Scan**	File name or path	No
			File type (extension)	No
			File age	No
Custom on-demand scan	Files, folders, and drives	• Trellix ePO - On-prem — **Custom On-Demand Scan** client task • Trellix Endpoint Security (ENS) Client — **Tasks → Add Task → Custom scan** **Tasks → Add Task → Custom scan**	File name or path	Yes (* and ?)
			File type (extension)	Yes (*)
			File age	No

Best practices: Recommended exclusions for on-access scans

Microsoft provides recommendations for locations to exclude from file-level scanners, such as the Threat Prevention on-access scanner. For information about these recommendations, see these KB articles.

To ensure compatibility with...	See this KB article
Microsoft SQL Server	KB67211
Microsoft Exchange	KB51471
Windows Domain Controller with Active Directory or File Replication Service (FRS)/Distributed File System Replication (DFSR)	KB57308

Wildcards in exclusions

You can use the ? and * wildcards to represent 1 or more characters when excluding files, folders, detection names, and potentially unwanted programs.You can use the ? and * wildcards to represent 1 or more characters when excluding files and folders from scanning.

Valid wildcards

Wildcard character	Name	Represents	Example
?	Question mark	Single character in the exact location in the file, folder, or path name. You can use a single ? character as the root of a file path. For example, ?:\ABC matches the root-level ABC folder for all drives.	W?? excludes WWW, but doesn't exclude WW or WWWW.
*	Asterisk	Multiple characters, except backslash (\). Doesn't cross folder boundaries. **Note:** *\ at the beginning of a file path is not valid. Use **\ instead. For example: **\ABC*.	C:\Users\Will* matches path names, such as C:\Users\William, C:\Users\Willamina, and C:\Users\WillAnderson, but not subfolders of those names.
**	Double asterisk	One or more of any characters, including backslash (\). Crosses folder boundaries.	C:\Users\Will** matches path names, such as C:\Users\William, C:\Users\Willamina, and C:\Users\WillAnderson and all their subfolders.

Wildcard character	Name	Represents	Example
			C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ.
**\		One or more complete path components (including a single backslash), delimited by backslashes.	C:**\Favorites\ matches any folder named Favorites on drive C.

Wildcards can appear in front of a backslash (\) in a path. For example, C:\ABC*\XYZ matches C:\ABC\DEF\XYZ.

Wildcard examples

Example	Description
**\Temp\test.docx	Excludes a specific file in a folder named Temp anywhere on the system.
**\test.docx	Excludes a specific file anywhere on the system.
**\test.docx	Excludes a specific file in any folder on a specific drive.
Users**\Documents\Microsoft User Data\	Excludes any folder under Users and any folder under User Data, if you select **Also exclude subfolders**.
C:\Documents and Settings**\Favorites\	Excludes the Favorites folder for all users.
C:**\Favorites\	Excludes any folder named Favorites on the C: drive.
\Temp	Excludes the Temp folder in any location, on any drive, including: • C:\Temp • D:\Windows\temp

Example	Description
	• C:\Documents and Settings\Administrator\Local Settings\temp
**\Temp*.tmp	Excludes any file with a .tmp extension in a folder named Temp anywhere on the system.
***.html	Excludes any file with an .html extension anywhere on the system.
C:\Windows\Temp*\inifile?.*	Excludes all files named inifileX, where X is any valid character for a file name, in any folder name beginning with Temp under C:\Windows.
***.tmp	Excludes all files with the .tmp extension (*.tmp) in any folder on a specific drive.
D:***.tmp	Excludes any *.tmp files on the D: drive.

Environment variables in exclusions

In addition to wildcards, you can use system environment variables, such as %SystemRoot% in exclusions. Exclusions don't support user environment variables, such as %UserProfile%. The reason for this is that the on-access scanner runs under the Windows LocalSystem account and can only access the system environment variables.

Preventing threats from accessing systems

The first line of defense against malware is to protect your client systems from threats. Access Protection protects files, registry keys, registry values, processes, and services. Exploit Prevention prevents buffer overflow, illegal API use, and network exploits.

Trellix delivers Trellix-defined signatures in Exploit Prevention content updates. When the content file is updated, the signatures are updated if needed.

Access protection

Access protection prevents unwanted changes to client systems by restricting access to specified files, shares, registry keys, registry values, and preventing or restricting processes and services from executing threat behavior. .

Access protection uses both Trellix-defined rules (signatures) and user-defined rules (also called custom rules) to report or block access to items. Access Protection compares a requested action against the list of rules and acts according to the rule.

You can also create Expert Rules to restrict access to files, registry keys, registry values, processes, and services, using Trellix-provided syntax templates.

You can create expert rules to stop buffer overflow and illegal API use exploits.

Note

With Microsoft Window 8.1 and later, Access Protection rules no longer support operations for the **Services** subrule type. This is because Microsoft made services.exe a protected process in Windows 8.1 and later.

Buffer Overflow and Illegal API Use

Buffer overflow protection stops exploited buffer overflows from executing arbitrary code. This technology monitors applications in the application protection list and uses signatures in the Exploit Prevention content file to protect those applications. Exploit Prevention monitors user-mode API calls and recognizes when they are called as a result of a buffer overflow.

Illegal API use monitors the Windows Application Programming Interface (API) and protects against malicious API calls being made by unknown or compromised applications running on the system.

You can create Expert Rules to stop buffer overflow and illegal API use exploits, using Trellix-provided syntax templates.

You can create expert rules to stop buffer overflow and illegal API use exploits.

You can view Buffer Overflow and Illegal API Use events in Trellix ePO - On-prem on the **Exploit Prevention Events** page under **Reporting**.

Network IPS

Network Intrusion Prevention (Network IPS) protects against network denial-of-service attacks and bandwidth-oriented attacks that deny or degrade network traffic. Network IPS examines all data that flows between the client system and the rest of the network and compares it to the Trellix Network IPS signatures. When an attack is identified, the offending data is discarded or blocked from passing through the system.

You can't create Network IPS custom rules or Expert Rules.

Note

Host Intrusion Prevention 8.0 can be installed on the same system as Trellix ENS version 10.7. If the **Host IPS** or **Network IPS** options in McAfee Host IPS are enabled, **Exploit Prevention** and **Network Intrusion Prevention** are disabled even if enabled in the Threat Prevention settings.

How threats gain access

Threats gain access to your system using various access points.

Access point	Description
Macros	As part of word-processing documents and spreadsheet applications.
Executable files	Seemingly benign programs can include viruses with the expected program. Some common file extensions are .EXE, .COM, .VBS, .BAT, .HLP and .DLL.
Scripts	Associated with webpages and email, scripts such as ActiveX and JavaScript, if allowed to run, can include viruses.
Internet Relay Chat (IRC) messages	Files sent with these messages can easily contain malware as part of the message. For example, automatic startup processes can contain worms and trojan threats.
Browser and application Help files	Downloading these Help files exposes the system to embedded viruses and executables.
Email	Jokes, games, and images as part of email messages with attachments.
Combinations of all these access points	Sophisticated malware creators combine all these delivery methods and even embed one piece of malware in another to try to access the system.

Types of Access Protection rules

Use default Access Protection rules or create custom rules to protect your system's access points.

Default Trellix-defined rules are always applied before any user-defined rules.

Rule type	Description	You can...	You can't...
Trellix-defined rules	These rules prevent change to commonly used files and settings. Trellix delivers Trellix-defined signatures in Exploit Prevention content updates. When the content file is updated, the signatures are updated if needed.	• Enable and disable these rules. • Change the block and report settings for these rules. • Add excluded and included executables to these rules.	• Delete these rules. • Change the files and settings protected by these rules. • Add subrules or user names to these rules.
User-defined rules	These rules supplement the protection provided by Trellix-defined rules. • An empty **Executables** table indicates that the rule applies to all executables. • An empty **User Names** table indicates that the rule applies to all users.	• Enable and disable these rules. • Change the block and report settings for these rules. • Add and delete these rules. • Change the configuration of these rules.	

Exclusions

At the rule level, exclusions and inclusions apply to the specified rule. Otherwise, exclusions apply to all rules. Exclusions are optional.

Example rule to protect a process

Create an Access Protection rule to prevent the Command Prompt (cmd.exe) from being used to run PowerShell (powershell.exe):

1. Add the cmd.exe executable to the rule.
2. Add a subrule and select:
    - **Processes** subrule type
    - **Run** operation

3. Add a subrule target executable and specify "powershell.exe" as the file name.

Trellix-defined Access Protection rules

You can use Trellix-defined Access Protection rules to protect your computer from unwanted changes.

Tip

Best practice: Because some Access Protection rules can generate many events, we recommend that you enable **Report** for a few systems to determine the impact before deploying widely. Use the generated events to evaluate the impact of the rule and implement any needed exclusions to prevent false positives before setting rules to **Block**.

Trellix-defined rule	Description	Default setting	Benefits	Risks
Browsers launching files from the Downloaded Program Files folder	Prevents software from installing through the web browser.	**Report**	Prevents adware and spyware from installing and running executables from the downloads folder.	Might block installation of legitimate software. **Best practice:** Disable this rule before installing the application or add the blocked processes to the exclusion list.
Changing any file extension registrations	Protects the registry keys under HKEY_CLASSES_ROOT where file extensions are registered. This rule is a more restrictive alternative to **Hijacking .EXE and other executable extensions**.		Prevents malware from changing the file extension registrations to allow malware to execute silently.	Might block installation of legitimate software. **Best practice:** Disable this rule when installing valid applications that change file extension registrations in the registry.

Trellix-defined rule	Description	Default setting	Benefits	Risks
Changing user rights policies	Protects registry values that contain Windows security information.		Prevents worms from changing accounts that have administrator rights.	
Creating new executable files in the Program Files folder	Prevents the creation new executable files in the Program Files folder.		Prevents adware and spyware from creating new .EXE and .DLL files and installing new executable files in the Program Files folder.	Might block installation of legitimate software. **Best practice:** Disable this rule before installing the application or add the blocked processes to the exclusion list.
Creating new executable files in the Windows folder	Prevents the creation of files from any process, not just from over the network.		Prevents the creation of .EXE and .DLL files in the Windows folder.	Might block legitimate software from creating these files in the Windows folder. **Best practice:** Add processes that must place files in the Windows folder to the exclusion list.
Disabling Registry Editor and Task Manager	Protects Windows registry entries, preventing disabling the registry editor			**Best practice** In an outbreak, disable this rule to allow registry changes, or open Task Manager

Trellix-defined rule	Description	Default setting	Benefits	Risks
	and Task Manager.			to stop active processes.
Doppelganging attacks on processes	Prevents "Process Doppelgänging" attacks from changing processes.	• **Report** • **Block**	Prevents malware from loading and executing arbitrary code in the context of legitimate or trusted processes.	
Executing Mimikatz malware	Prevents executables named mimikatz from running.	• **Report** • **Block**	Protects against mimikatz malware by preventing it from executing.	**Best practice:** If you observe false positives, add the blocked processes to the exclusion list.
Executing scripts by Windows script host (CScript.exe or Wscript.exe) from common user folders	Prevents the Windows scripting host from running VBScript and JavaScript scripts in any folder with "temp" in the folder name.		Protects against many trojans and questionable web installation mechanisms used by adware and spyware applications.	Might block legitimate scripts and third-party applications from being installed or run. **Best practice:** If you observe false positives, add the blocked processes to the exclusion list.
Executing Windows Subsystem for Linux	Prevents an administrator user from running the Windows Subsystem for Linux (WSL).	• **Report** • **Block**	Prevents malware designed for Linux systems from attacking Windows computers.	

Trellix-defined rule	Description	Default setting	Benefits	Risks
Hijacking .EXE or other executable extensions	Protects .EXE, .BAT, and other executable registry keys under HKEY_CLASSES_ROOT and HKEY_LOCAL_MACHINE. This rule is a less restrictive alternative to **Changing any file extension registrations**.		Prevents malware from changing registry keys to run the virus when another executable runs.	
Installing Browser Helper Objects or Shell Extensions	Prevents Browser Helper Objects from installing on the host computer. The rule doesn't prevent installed Browser Helper Objects from working.		Prevents adware, spyware, and trojans from installing on systems.	Might block legitimate applications from installing Browser Helper Objects. **Best practice:** Allow legitimate custom or third-party applications to install Browser Helper Objects by adding them to the exclusion list.
Installing new CLSIDs, APPIDs, and TYPELIBs	Prevents the installation or registration of new COM servers.		Protects against adware and spyware programs that install themselves as a COM add-on Internet Explorer or	Might block installation of some common applications, like Adobe Flash. **Best practice:** Allow legitimate applications that register COM add-

Trellix-defined rule	Description	Default setting	Benefits	Risks
			Microsoft Office applications.	ons by adding them to the exclusion list.
Modifying core Windows processes	Prevents files from being created or executed with the most commonly spoofed names. This rule excludes authentic Windows files.		Prevents viruses and trojans from running with the name of a Windows process.	
Modifying Internet Explorer settings	Blocks processes from changing settings in Internet Explorer.		Prevents start-page trojans, adware, and spyware from changing browser settings, such as changing the start page or installing favorites.	
Modifying network settings	Prevents processes that aren't listed in the exclusion list from changing a system's network settings.		Blocks registry editors, common Microsoft user applications, such as explorer.exe, iexplore.exe, and script engines (except system processes), and Sysinternals applications from modifying the network-related registry keys and the hosts file.	Might block legitimate processes that need to change network settings. **Best practice:** Disable the rule while changes are made or add processes that must change network settings to the exclusion list.

Trellix-defined rule	Description	Default setting	Benefits	Risks
Protect Endpoint Security logs folder	Prevents unauthorized processes from taking create, edit, or delete file actions in the Trellix ENS logs folder. This rule also prevents hard links from the Endpoint Security logs folder.		Protects the Trellix ENS logs folder from tampering or modification.	Third party processes may need to load Trellix ENS DLLs (for example, AMSI or Web Control DLLs) for the purpose of Trellix ENS operations, including writing to Trellix ENS logs. If enabled, this rule will block logging done by Trellix ENS DLLs in the context of third party processes that have loaded the DLLs. To allow this logging, you can add an exclusion to the rule for any trusted third party process. **Best practice:** If configuring custom log location from policy, do not configure the Trellix ENS logs folder to common folders like C:\, C:\Program Files, or C:\Windows. Keep a separate folder

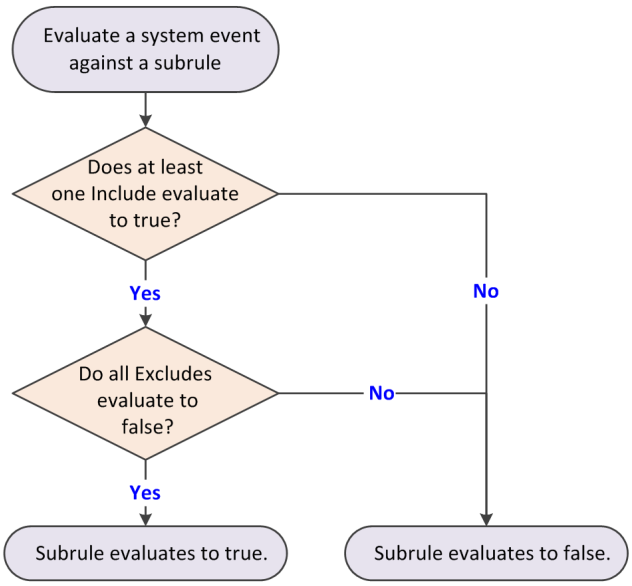
Trellix-defined rule	Description	Default setting	Benefits	Risks
				for Trellix ENS logs.
Registering of programs to autorun	Blocks adware, spyware, trojans, and viruses from trying to register themselves to load every time a system is restarted.		Prevents processes that aren't on the excluded list from registering processes that execute each time a system restarts.	Might block legitimate processes that need to register themselves to load at system startup. **Best practice:** Disable this rule before installing the application or add the blocked processes to the exclusion list.
Remotely accessing local files or folders	Prevents read and write access from remote computers to the computer. In a typical environment, this rule is suitable for workstations, but not servers.		Prevents a share-hopping worm from spreading.	Prevents updates from being installed to systems managed by pushing files. This rule doesn't affect the management functions of Trellix ePO - On-prem. **Best practice** Enable this rule only when computers are actively under attack.
Remotely creating autorun files	Prevents other computers from making a	• **Report** • **Block**	Prevents spyware and adware distributed on	

Trellix-defined rule	Description	Default setting	Benefits	Risks
	connection and creating or changing autorun (autorun.inf) files. Autorun files are used to automatically start program files, typically setup files from CDs.		CDs from being executed.	
Remotely creating or modifying files or folders	Blocks write access to all shares. In a typical environment, this rule is suitable for workstations, but not servers, and is only useful when computers are actively under attack.		Limits the spread of infection during an outbreak by preventing write access. The rule blocks malware that would otherwise severely limit use of the computer or network.	Prevents updates from being installed to systems managed by pushing files. This rule doesn't affect the management functions of Trellix ePO - On-prem.
Remotely creating or modifying Portable Executable, .INI, .PIF file types, and core system locations	Prevents other computers from making a connection and changing executables, such as files in the Windows folder. This rule affects only file types that viruses typically infect.		Protects against fast spreading worms or viruses, which traverse a network through open or administrative shares.	

Trellix-defined rule	Description	Default setting	Benefits	Risks
Running files from common user folders	Blocks any executable from running or starting from any folder with "temp" in the folder name.		Protects against malware that is saved and run from the user or system temp folder. Such malware might include executable attachments in email and downloaded programs.	Although this rule provides the most protection, it might block legitimate applications from being installed.
Running files from common user folders by common programs	Blocks applications from installing software from the browser or from the email client.		Prevents email attachments and executables from running on webpages.	Might block legitimate processes that use the Temp folder during installation. **Best practice:** Disable this rule before installing the application or add the blocked processes to the exclusion list.

How targets in subrules are evaluated

Each target is added with an **Include** or **Exclude** directive.



When evaluating a system event against a subrule, the subrule evaluates to *true* if:

- At least one *Include* evaluates to *true*. *and*
- All *Excludes* evaluate to *false*.

Exclude takes precedence over **Include**. Here are examples:

- If a single subrule both includes and excludes a file C:\marketing\jjohns, the subrule does not trigger for that file.
- If a subrule includes *all* files but excludes the file C:\marketing\jjohns, the subrule triggers if the file is not C:\marketing\jjohns.
- If a subrule includes file C:\marketing* but excludes C:\marketing\jjohns, the subrule triggers for C:\marketing\anyone, but doesn't trigger for C:\marketing\jjohns.

How buffer overflow exploits occur

Attackers use buffer overflow exploits to run executable code, which allows the attacker to take over the target computer or compromise its data.

Buffer overflow exploits overflow the fixed-size memory buffer reserved for an input process. A large percentage of attacks is buffer overflow attacks that try to overwrite adjacent memory in the stack frame.

The two types of buffer overflow exploits are:

- Stack-based attacks use the stack memory objects to store user input (most common).
- Heap-based attacks flood the memory space reserved for a program (rare).

The fixed-size stack memory object is empty and waiting for user input. When a program receives input from the user, the data is stored on top of the stack. The data includes the return address memory information required by the application when calling internal functions. When the stack is processed, the called application function processes the user's input stored on the stack.

The return address memory information is used to determine the code address of the caller that the application returns to once processing of the called function finishes.

The following process describes a stack-based buffer overflow attack:

1. **Overflow the stack.** When the program is written, a specific amount of memory space is reserved for the data. The stack overflows if the data written is larger than the space reserved for it in the memory stack. This situation is only a problem when combined with malicious input.
2. **Exploit the overflow.** The program waits for input from the user. If the attacker enters an executable command that exceeds the stack size, that command is saved outside the reserved space.
3. **Perform malicious actions.** The payload of the exploit, also called shellcode performs malicious actions on the system. These actions can include adding new users, changing user permissions, creating or changing files on the system, or downloading and running malware. Initially, the program starts to crash because of the buffer overflow. If the attacker provided a return memory address that references the malicious payload, the program tries to recover by using the return address. If the return address is valid, the malicious payload is executed.
4. **Exploit the permissions.** The payload now runs with the same permissions as the application that was compromised. Because programs usually run in kernel mode or with permissions inherited from a service account, the attacker can now gain full control of the operating system.

Excluding items from Exploit Prevention

If an Exploit Prevention violation event is a false positive, you can add an exclusion to prevent Exploit Prevention from blocking the item.

Each exclusion is independent: multiple exclusions are connected by a logical OR so that if one exclusion matches, the violation event doesn't occur. You can create exclusions to a specific rule. Exclusions are case insensitive.

Access Protection: Files, processes, and registry exclusions

For files, processes, and registry items, you can exclude by processes (file name or path, MD5 hash, or signer) or signatures. Specify these exclusions in either the **Access Protection** policy or together with the other exclusions in the **Exploit Prevention** policy.

When specifying exclusions, consider the following:

- You must specify at least one process: **File name or path**, **MD5 hash**, or **Signer**.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match, the exclusion is invalid. For example, the file name and MD5 hash don't apply to the same file.
- If you include signature IDs in an exclusion, the exclusion only applies to the process in the specified signatures. If no signature IDs are specified, the exclusion applies to the process in all signatures.
- Wildcards are allowed for all except MD5 hash.

Trellix ENS treats all file and folder exclusions as case insensitive — all case variations of the specified locations are excluded. For example, if you exclude C:\Temp\ABC, Trellix ENS also excludes C:\temp\abc and C:\TEMP\Abc.

Access Protection: Services exclusions

For Access Protection (services), you can exclude by the service name from the Services tab in Task Manager. Specify these exclusions in either the **Access Protection** policy or together with the other exclusions in the **Exploit Prevention** policy.

Buffer Overflow and Illegal API Use exclusions

When a Buffer Overflow or Illegal API Use violation event occurs, the event includes an associated process and a possible caller module, API, or signature. If you suspect the violation event is a false positive, you can add an exclusion that allows one or more of these identifiers. Specify these exclusions in the **Exploit Prevention** policy.

For example, suppose client behavior triggers Signature 2834, **Java - Creation of suspicious files in Temp folder**. This signature signals that the Java application is trying to create a file in the Windows Temp folder. An event triggered by this signature might be cause for alarm, because a Java application can be used to download malware to the Windows Temp folder. In this case, you might reasonably suspect that a trojan horse has been planted. But, if the process normally creates files in Temp, for example, saving a file using the Java application, create an exclusion to allow this action.

To completely exclude a process from Buffer Overflow or Illegal API Use protection either:

- Create an exclusion and specify only the process information.
- Set the inclusion status for the process to **Exclude** in the application protection list.
- Remove the process from the application protection list. (Not recommended)

In each of these cases, Exploit Prevention doesn't monitor the process.

If you want Buffer Overflow or Illegal API Use protection to monitor a process, except for a particular signature:

- Make sure that the process is in the application protection list with the inclusion status of **Include**.
- Create an exclusion and specify the process information and signature ID.

In these cases, Exploit Prevention monitors the process for all other signatures.

If you create an exclusion for a particular signature and specify ** for the process name, the effect is the same as disabling the signature.

You only need to create exclusions for processes that are in the application protection list with the inclusion status set to **Include**.

Exploit Prevention exclusions created in the Trellix Endpoint Security (ENS) Client are not sent to Trellix ePO - On-prem and might be overwritten when the administrator deploys an updated policy. Configure Exploit Prevention exclusions in the **Exploit Prevention** policy in Trellix ePO - On-prem. You can also create exclusions automatically from Exploit Prevention events from the **Exploit Prevention Events** page under **Reporting**.

When specifying exclusions, consider the following:

- You must specify at least one of **Process**, **Caller Module**, **API**, or **Signature**.
- Exclusions by **Caller Module** or **API** don't apply to Data Execution Prevention (DEP).
- If you specify more than one identifier, all identifiers apply.

- If you specify more than one identifier and they don't match, the exclusion is invalid. For example, the file name and MD5 hash don't apply to the same file.
- Wildcards are allowed for all except MD5 hash.
- If you include signature IDs in an exclusion, the exclusion only applies to the process in the specified signatures. If no signature IDs are specified, the exclusion applies to the process in all signatures.

Network IPS exclusions

For Network IPS protection, you can exclude by IP addresses (IPv4 format) or range. To exclude a range of IP addresses, enter the starting point and ending point of the range. For example:

```
203.0.113.0-203.0.113.255
```

```
192.168.254.0/24
```

Specify these exclusions in the **Exploit Prevention** policy.

Protect files, registry, processes, and services with Access Protection rules

Change the behavior of Trellix-defined rules or create custom rules to protect your system access points.

Tip

Best practice: For information about creating Access Protection rules to protect against ransomware, see KB89335, and KB89540.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Access Protection**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Change a Trellix-defined rule: In the **Rules** section, select the rule, then click **Edit**.
   a. On the **Rule** page, configure rule options.
   b. In the **Executables** section, click **Add**, configure executable properties, then click **Save** twice to save the rule.
6. Create a custom rule: In the **Rules** section, click **Add**.
   a. On the **Rule** page, configure the settings.
   b. In the **Executables** section, click **Add**, configure executable properties, then click **Save**.

      An empty **Executables** table indicates that the rule applies to all executables.

   c. In the **User Names** section, click **Add**, configure user name properties, then click **Save**.
      An empty **User Names** table indicates that the rule applies to all users.
   d. In the **Subrules** section, click **Add**, then configure subrule properties.

Note

With Microsoft Window 8.1 and later, Access Protection rules no longer support operations for the **Services** subrule type. This is because Microsoft made services.exe a protected process in Windows 8.1 and later.

e. In the **Targets** section, click **Add**, configure target information, then click **Save** three times.

7. Specify the behavior of the rule: In the **Rules** section, select **Block**, **Report**, or both for the rule.
   - To select or deselect all rules under **Block** or **Report**, click **Block All** or **Report All**.
   - To disable the rule, deselect both **Block** and **Report**.
8. Click **Save**.

Prevent Access Protection from blocking trusted programs

If a trusted program is blocked, you can exclude the process by creating a policy-based or rule-based exclusion.

Note

Access Protection exclusions don't apply to the Windows **Services** subrule type.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Access Protection**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Verify that **Access Protection** is enabled.
6. Perform one of the following:

To...	Do this...
Exclude items from all rules.	a. In the **Exclusions** section, click **Add** to add items to exclude from all rules. b. On the **Exclusion** page, configure the executable properties. c. Click **Save** twice to save the settings.
Specify processes for inclusion or exclusion in a user-defined rule.	a. Edit an existing user-defined rule or add a rule. b. On the **Rule** page, in the **Executables** section, click **Add** to add an executable to exclude or include. c. On the **Executable** page, configure the executable properties, including whether to

To...	Do this...
	include or exclude the executable from protection. d. Click **Save** three times to save the settings.

Configure Exploit Prevention settings to block threats

To prevent applications from executing arbitrary code on the client system, you can configure the Exploit Prevention exclusions, default signatures, and application protection rules.

You can set the action for Trellix-defined signatures. You can enable, disable, delete, and change the inclusion status of Trellix-defined application protection rules. You can also create and duplicate your own application protection rules. Any changes you make to these rules persist through content updates.

Enable and configure Exploit Prevention to prevent buffer overflow, illegal API use, and network exploits. Create Expert Rules to prevent buffer overflow and illegal API use exploits and to protect files, registry keys, registry values, processes, and services. For the list of processes protected by Exploit Prevention, see KB58007.

Note

Host Intrusion Prevention 8.0 can be installed on the same system as Endpoint Security version 10.7. If the Host IPS or Network IPS options in McAfee Host IPS are enabled, Exploit Prevention and Network Intrusion Prevention are disabled even if enabled in the Threat Prevention settings.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Configure the required settings in the **Exploit Prevention** page, then click **Save**.

Option definitions

Section	Option	Definition
EXPLOIT PREVENTION Exploit Prevention	Enable Exploit Prevention	Enables the Exploit Prevention feature.

Section	Option	Definition
		⚠ **Caution:** Failure to enable this option leaves your system unprotected from malware attacks.

Advanced options

Section	Option	Definition
Generic Privilege Escalation Prevention (GPEP)	**Enable Generic Privilege Escalation Prevention**	Enables Generic Privilege Escalation Prevention (GPEP) support. (Disabled by default) GPEP uses Signature ID 6052 in the Exploit Prevention Content to provide coverage for privilege escalation exploits in kernel mode and user mode. If this option is selected, Signature ID 6052 is automatically set to both **Block** and **Report**, but the **Signatures** section doesn't change to reflect the state. Because GPEP might generate false positive reports, this option is disabled by default.
Windows Data Execution Prevention (DEP)	**Enable Windows Data Execution Prevention**	Enables Windows Data Execution Prevention (DEP) integration. (Disabled by default) Select this option to: • Enable DEP for 32-bit applications in the Trellix application protection list, if not already enabled, and use it instead of Generic Buffer Overflow Protection (GBOP). Caller validation and Targeted API Monitoring are still enforced. • Monitor for DEP detections in the DEP-enabled 32-bit applications. • Monitor for DEP detections in 64-bit applications in the Trellix application protection list. • Log any DEP detections.

Section	Option	Definition
		• Log any DEP detections and send an event to Trellix ePO - On-prem. If this option is selected, Signature ID 9990 is automatically set to both **Block** and **Report**, but the **Signatures** section doesn't change to reflect the state. Disabling this option doesn't affect any processes that have DEP enabled as a result of the Windows DEP policy. Because DEP might generate false positive reports, this option is disabled by default. Exclusions with **Caller Module** or **API** don't apply to DEP.
Network Intrusion Prevention	**Enable Network Intrusion Prevention**	Enables Network Intrusion Prevention (Network IPS) and enforces network IPS signatures. Selecting this option enables the **Network IPS** filter and exposes Network IPS signatures in the **Signatures** list.
	Automatically block network intruders	Blocks intruder hosts for a specified number of seconds. Select this option to block all attempted actions from intruder hosts, even if the action for the Network IPS signature isn't set to **Block**. • **Number of seconds (1-9999) to block** — Specifies the number of seconds to automatically block intruders.
Blocked Hosts		Lists systems that Network IPS is blocking communication from. When **Automatically block network intruders** is selected, Network IPS automatically blocks systems when it detects an attack. • **Delete** — Deletes the selected system from the **Blocked Hosts** table. When you click **Apply**, the system is unblocked. • **Host** — Lists the IP address of the blocked system.

Section	Option	Definition
		• **Time Remaining (seconds)** — Indicates the number of seconds until Network IPS no longer blocks the system. • **Status** — Indicates whether the system is blocked or unblocked.
Exclusions		Specifies the process, caller module, API, signatures, or services to exclude. Exclusions with **Caller Module** or **API** don't apply to DEP.
	Add	Creates an exclusion and adds it to the list.
	Delete	Deletes the selected item.
	Double-click an item	Changes the selected item.
	Duplicate	Creates a copy of the selected item.
	Actions	• **Edit** — Changes the selected item. • **Duplicate** — Creates a copy of the selected item.
	Sort options	Sort the **Exclusions** list by: • **Type** • **Process Name** • **Caller Module Name** • **API Name** • **Signature IDs** • **Service Name** • **IP Addresses** • **Actions**
Signatures		Changes the action for Exploit Prevention signatures. To disable a signature, deselect **Block** and **Report**. By default, only high-severity signatures are set to **Block**.

Section	Option	Definition	
		The **Notes** column in the **Signatures** list refers to KB51504 for details about supported platforms. To view this article, you must first log on to the ServicePortal, then search the Knowledge Center for KB51504. You can't select **Block** or **Report** for Signature IDs 6052 and 9990. To enable Signature ID 6052, select **Enable Generic Privilege Escalation Prevention**. To enable Signature ID 9990, select **Enable Windows Data Execution Prevention**. The **Signatures** section doesn't change to reflect the state.	
	Filter options	Filters the **Signatures** list by:	
		Type	• **Buffer Overflow** • **Illegal API Use** • **Files** • **Services** • **Registry** • **Processes** • **Network IPS** The **Network IPS** filter is only available when **Enable Network Intrusion Prevention** is selected.
		Severity	• **High** • **Medium** • **Low** • **Others** (signatures with a severity of **Informational** or **Disabled**)
		Status	• **Enabled**

Section	Option	Definition	
			• **Disabled**
		Origin	• **Trellix-defined** • **User-defined**
		Quick find	Filters the list by specifying a term to search for. • **Apply** — Starts the search. • **Clear** — Deletes text from the **Quick find** field.
		Show selected rows	Filters out unselected rows, showing only selected rows.
		Show Filter/ Hide Filter	Displays or hides the filter options.
	Block (only)	Blocks behavior that matches the signature without logging.	
	Report (only)	Logs behavior that matches the signature without blocking.	
	Block and **Report**	Blocks and logs behavior that matches the signature.	
	Block All	Selects or deselects **Block** for all signatures.	
	Report All	Selects or deselects **Report** for all signatures.	
	Add Expert Rule	Creates an Expert Rule to: • Protect files, registry keys and values, processes, or services.	

Section	Option	Definition
		• Prevent buffer overflow or illegal API use exploits. You can't create Network IPS Expert Rules. To check for syntax errors, select a user-defined Expert Rule and click **Add Expert Rule**. **Expert Rule Checker** opens so you can change, check, and enforce the Expert Rule.
	Delete	Deletes the selected item.
	Double-click an item	Changes the selected item. (User-defined rules only)
	Actions → **Export Table**	Exports all signatures in the list to a defined format.
	Actions	• **Edit** — Changes the selected item. (User-defined rules only) • **View** — Displays the signature description for the selected item. (Trellix-defined rules only)
Application Protection Rules		Specifies the applications that Exploit Prevention monitors. Exploit Prevention only monitors the processes in the Application Protection list with the inclusion status of **Include**.
	Add	Creates an Application Protection rule and adds it to the list.
	Delete	Deletes the selected item. (User-defined rules only)
	Double-click an item	Changes the selected item. (User-defined rules only)

Section	Option	Definition
	Duplicate	Creates a copy of the selected item. (User-defined rules only)
	Actions	• **Edit** — Changes the selected item. • **Duplicate** — Creates a copy of the selected item. (User-defined rules only)

Exclude items from Exploit Prevention protection

If Exploit Prevention blocks a trusted program, you can add an exclusion for the process name. For Buffer Overflow and Illegal API Use, you can also exclude by caller module, API or signature ID. For Network IPS, you can exclude by signature ID or IP address. For Services, you can exclude by service name. For Files- Processes – Registry, you can exclude by signature ID.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Perform one of the following:

To...	Do this...
Exclude items from all rules.	a. In the **Exclusions** section, click **Add** to add items to exclude from all rules. b. On the **Exclusion** page, configure the exclusion properties. c. Click **Save** twice to save the settings.
Specify processes for inclusion or exclusion in a user-defined Application Protection rule. (*Buffer overflow and illegal API violations only*)	a. Edit an existing user-defined rule or add an Application Protection rule. b. On the **Application Protection Rule** page, in the **Executables** section, click **Add**, then configure the executable properties. c. Click **Save** three times to save the settings.

Add Exclusion or Edit Exclusion

You can exclude a process, caller module, API, signature, IP address, Hostname, or service from Exploit Prevention.

When specifying exclusions, consider the following:

- Based on the type selected from the **Exclusion Type** drop-down list, you must specify at least one of **Files-Processes-Registry**, **Caller Module**, **API**, **Signatures**, **Service Name**, or **IP Addresses**.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match, the exclusion is invalid. For example, the file name and MD5 hash don't apply to the same file.
- Exclusions are case insensitive.
- Wildcards are allowed for all except User SID, Group SID, User name, Group name, MD5 hash, and Signature IDs.
- If you include signature IDs in an exclusion, the exclusion only applies to the process in the specified signatures. If no signature IDs are specified, the exclusion applies to the process in all signatures.
- For **Process** exclusions, you must specify at least one identifier: **File name or path**, **MD5 hash**, or **Signer**.
- Exclusions with **Caller Module** or **API** don't apply to DEP.
- When the **Process** section fields (**File name or path**, **MD5 hash**, **Signer**, **User SID**, **Group SID**, **User name**, **Group name**, or **Hostname**) are active, the **Target** section fields (**File name or path** or **Registry key or value**) is disabled by default and vice versa.
- **Target**, **User SID**, **Group SID**, **User name**, **Group name**, and **Hostname** only apply to **Files-Processes-Registry**.

Option definitions

Section	Option	Definition
Name		Specifies the exclusion name. This field is required with at least one other field whichever object field is applicable to the **Exclusion Type**. **Note:** This field is applicable only for **Files-Processes-Registry**.
Process (Initiator process) ***Files-Processes-Registry, Buffer Overflow,*** *or* ***Illegal API Use***	**Name**	Specifies the initiator process name to exclude. Exploit Prevention excludes the process wherever it is located.

Section	Option	Definition
		This field is required with at least one other field: **File name or path**, **MD5 hash**, or **Signer**. **Note:** This field is not applicable for **Files-Processes-Registry**.
	File name or path	Specifies (comma-separated) file name or path of the executable to add or edit. Click **Browse** to select the executable.
	MD5 hash	Indicates the MD5 hash (32-digit hexadecimal number) of the process.
	Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the log files. For example:

Section	Option	Definition
		`C=US, ST=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS` **Note:** You can enter `S` for the stateOrProvinceName object identifier, but the element automatically appears as `ST` in the log files. From Trellix ePO - On-prem **Event Log**, copy and paste the details from the **Source Signer Process** field from an Trellix ENS event.
Process ***Files-Processes-Registry*** *only*	**User SID**	Specifies User Security Identifier. **Note:** If this field is enabled, then **User name** will be disabled.
	Group SID	Specifies Group Security Identifier. **Note:** If this field is enabled, then **Group name** will be disabled.
	User name	Specifies the user name. **Note:** If this field is enabled, then **User SID** will be disabled.

Section	Option	Definition
	Group name	Specifies the group name. **Note:** If this field is enabled, then **Group SID** will be disabled.
	Hostname	Specifies exclusion by hostname. **Note:** This field is applicable only for **Files-Processes-Registry**.
Target ***Files-Processes-Registry*** *only*	**File name or path**	Specifies (comma-separated) target file, process, or section. **Note:** If this field is enabled, then **Registry key or value** will be disabled.
	Registry key or value	Specifies registry key or value. **Note:** If this field is enabled, then **File name or path** will be disabled.
Caller Module ***Buffer Overflow*** *or* ***Illegal API Use***	**Name**	Specifies the name of the module (a DLL) loaded by an executable that owns the writable memory that makes the call. This field is required with at least one other field: **File name or path**, **MD5 hash**, or **Signer**.
	File name or path	Specifies the file name or path of the executable to add or edit.

Section	Option	Definition
		Click **Browse** to select the executable.
	MD5 hash	Indicates the MD5 hash (32-digit hexadecimal number) of the process.
	Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the log files. For example: `C=US, ST=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS`

Section	Option	Definition
		Note: You can enter s for the stateOrProvinceName object identifier, but the element automatically appears as ST in the log files. From Trellix ePO - On-prem **Event Log**, copy and paste the details from the **Source Signer Process** field from an Trellix ENS event.
API ***Buffer Overflow*** *or* ***Illegal API Use***	**Name**	Specifies the name of the API (application programming interface) being called.
Signatures ***Files-Processes-Registry***, ***Buffer Overflow***, ***Illegal API Use***, *or* ***Network IPS***	**Signature IDs**	Specifies (comma-separated) Exploit Prevention signature identifiers. Invalid or non-existent signatures are not allowed. **Note:** Signature-based exclusion for Files-Processes-Registry is applicable to Trellix-Default rules and Expert rules (Custom rules).
IP Addresses ***Network IPS*** *only*	*IP addresses or ranges*	Specifies (comma-separated) IP addresses (in IPv4 format) or ranges. Enter the starting point and ending point of the range. For example: `203.0.113.0-203.0.113.255`

Section	Option	Definition
Services ***Services** only*	**Service Name**	Specifies the name of the service, such as AdobeARM, from the Services tab in Task Manager.
Notes		Provides more information about the item.

Get the signer distinguished name from Trellix ePO - On-prem to use to exclude executables

The signer distinguished name (SDN) is required when you enable a digital signature check and exclude only files signed by a specified process signer.

Task

1. Select **Menu** → **Reporting** → **Threat Event Log**.
2. Click the Trellix ENS event to display details.
3. Select and copy the **Source Process Signer** details.
4. When creating exclusions, paste the **Source Process Signer** details as a single line of text to the **Signed by** field.

   For example, the SDN required format is:

   ```
   C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION
   ```

Assigning multiple instances of Exploit Prevention policy

Assigning one or more instances of the policy to a group or system in the Trellix ePO - On-prem System Tree provides for single policy multi-purpose protection.

Exploit Prevention is a multiple-instance policy. This policy allows the application of more than one policy concurrently on a single client. When more than one instance is applied, what results is a union of all instances, called the effective policy.

A multiple-instance policy can be useful for an IIS Server, for example, where you might apply a general default policy, a server policy, and an IIS policy, the latter two configured to specifically target systems running as IIS servers. When assigning multiple instances, you are assigning a union of all elements in each instance of the policy.

To streamline your deployment, use multi-slot policy assignment. First, define groups of users for the deployment that have an essential property in common that dictates what resources need to be protected and what resources need exceptions to work properly. This property could be based on:

- **Department** — Each department should require protection of a unique set of resources and exceptions for a unique set of business activities.
- **Location** — Each location can have its own unique security standards or unique set of resources that need to be protected, and exceptions needed for business activity.

- **Computer type** — Each type of computer (laptops, workstations, servers) might have a unique set of applications that need to be protected but also allowed to perform essential business functions.

Without a multiple-instance IPS Rules policy, a combination of three departments, three locations, and three computer types would require 27 policies; with the multiple-instance approach, only nine are needed.

Note

When the policies are merged, the most restrictive policy settings are combined to become the effective policy.

Task

1. Click **Menu** → **System** → **System Tree** and select a group in the System Tree.
2. Under **Assigned Policies**, select **Endpoint Security Threat Prevention** in the **Product** list.
3. For **Exploit Prevention**, click **Edit Assignment** in the **Action** column.
4. On the **Policy Assignment** page, click **New Policy Instance**, and select a policy from the **Assigned Policies** list for the additional policy instance.
5. Click **Save** to save all changes.

Results

To view the effective or combined effect of multiple instance rule sets, click **View Effective Policy** under **Assigned Policies**.

Scanning for threats on client systems

Types of scans

Threat Prevention settings that apply to all on-access scans and on-demand scans include the quarantine location and potentially unwanted programs.

- **On-access scan** — Configure the on-access scanner in the **On-Access Scan** settings. When files, folders, and programs are accessed, the on-access scanner intercepts the operation and scans the item, based on criteria defined in the settings.
- **On-demand scan**

Manual	Run a predefined on-demand scan at any time from the Trellix Endpoint Security (ENS) Client by clicking **Scan System**, then selecting a scan type. ▫ **Quick Scan** runs a quick check of the areas of the system most susceptible to infection.	Configure the behavior of quick and full scans in the **On-Demand Scan** policy settings.

	▫ **Full Scan** performs a thorough check of all areas of the system. (Recommended if you suspect the computer is infected.)	
	Scan an individual file or folder at any time from Windows Explorer by right-clicking the file or folder and selecting **Scan for threats** from the pop-up menu.	Configure the behavior of the **Right-Click Scan** in the **On-Demand Scan** policy settings.
	Run a custom on-demand scan as administrator from the Trellix Endpoint Security (ENS) Client: ▫ Select **Settings** → **Common** → **Tasks**. ▫ Select the task to run. ▫ Click **Run Now**. **Tip: Best practice:** Use manual custom on-demand scans to associate a scan task with a reaction, such as a malware infection.	Configure custom scans in the **Custom On-Demand Scan** settings from the **Client Task Catalog**.
Scheduled	When a scheduled on-demand scan is about to start, Trellix ENS displays a scan prompt at the bottom of the screen. You can start the scan immediately or defer the scan, if configured.	
	Schedule the predefined on-demand scans using the **Policy-Based On-Demand Scan** client task settings.	Configure the behavior of quick and full scans in the **On-Demand Scan** policy settings.

	▫ **Quick Scan** — By default, the **Quick Scan** is enabled and scheduled to run every day at 7 p.m. ▫ **Full Scan** — By default, the **Full Scan** is enabled and scheduled to run every Wednesday at 12 midnight. **Tip: Best practice:** Use the weekly **Full Scan** to supplement the continuous protection of the on-access scan. The full scan includes fewer exclusions and actively checks all files for malicious code. Predefined on-demand scans provide details, such as scan duration, date of last full scan, and compliance status to Trellix ePO - On-prem in the **Systems Information Product properties** for Trellix ENS.	
	Schedule custom on-demand scans, using the **Custom On-Demand Scan** client task settings. **Tip: Best practice:** Use scheduled custom on-demand scans for targeted scans, such as daily memory scans.	Configure custom scans in the **Custom On-Demand Scan** settings from the **Client Task Catalog**.

Threat Prevention **Options** includes settings that apply to all scan types.

Configure settings for all scans

Threat Prevention settings that apply to all on-access scans and on-demand scans include the quarantine location and potentially unwanted programs.

These settings apply to all scans:

- Quarantine location and the number of days to keep quarantined items before automatically deleting them
- Detection names to exclude from scans, including buffer exclusions and command-line suppression for AMSI scanning
- Potentially unwanted programs to detect, such as spyware and adware
- Trellix GTI -based telemetry feedback

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Configure settings on the page, then click **Save**.

Exclude items from AMSI scanning

If AMSI is blocking scripts that you want to allow to run, you can exclude them from AMSI scanning. These exclusions apply to both Threat Prevention and Adaptive Threat Protection.

The process for excluding items from scanning depends on the type of exclusion.

Exclusion type	Action	Where specified?
File-based exclusion	Excludes the file from scanning.	In the **Exclusions** section of the **On-Access Scan** settings for **Standard** process types.
Buffer-hash exclusion	Excludes the buffer from scanning.	In the **Exclusion by Detection Name** section of the **Options** settings.
Command-line suppression	Scans the command line, but doesn't enforce the action specified in the **Actions** section of the **On-Access Scan** settings for **Standard** process types. If detections occur, Threat Prevention generates `Would Block`	In the **Exclusion by Detection Name** section of the **Options** settings.

Exclusion type	Action	Where specified?
	or `Would Clean` events.	

Task

1. Select **Menu** → **Reporting** → **Threat Event Log**.
2. Click an event name to display its details in the **Threat Event Log Details** page.
   AMSI scanning events include `AMSIScan` in the **Task Name** column.
3. From the **Actions** menu, select an option.
   - **Add Buffer Exclusion**
   - **Add Command-Line Suppression**
4. At the prompt, select the policy where you want to add the exclusion.
   Trellix ePO - On-prem displays a message indicating the exclusion was added to the selected policy.
5. Verify that the exclusion appears in the **Options** settings for the policy you selected.
   a. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
   b. From the **Category** list in the right pane, select **Options**.
   c. Click the **Edit** link for the policy that you added the exclusions to.
   d. Verify that the exclusions appear in the **Exclusion by Detection Name** list.
      - Buffer-hash exclusions include the prefix: `AMSI-B!`
      - Command-line suppressions include the prefix: `AMSI-CMD!`

Define which potentially unwanted programs to detect

You can specify programs that you want the on-access scanner and on-demand scanner to treat as unwanted programs.

Note

The scanners detect the programs you specify and programs specified in the AMCore content files.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. From **Potentially Unwanted Program Detections**:
   - Click **Add** to specify the name and optional description of a file or program to treat as a potentially unwanted program.

Note

The **Description** appears as the detection name when a detection occurs.

- Select an existing potentially unwanted program, then click **Edit** to change the name or description, or click **Delete** to remove it from the list.
- Click **Delete All** to remove all custom potentially unwanted programs from the list.

Enable detection and response for potentially unwanted programs

You can enable the on-access and on-demand scanners to detect potentially unwanted programs and specify responses when one is found.

Task

1. Configure **On-Access Scan** settings.
    a. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
    b. From the **Category** list in the right pane, select **On-Access Scan**.
    c. Click the **Edit** link for an editable policy.
    d. Under **Process Settings**, for each **On-Access Scan** type, select **Detect unwanted programs**.
    e. Under **Actions**, configure responses to unwanted programs.
2. Configure **On-Demand Scan** settings.
    a. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
    b. From the **Category** list in the right pane, select **On-Demand Scan**.
    c. Click the **Edit** link for an editable policy.
    d. For each scan type (**Full Scan**, **Quick Scan**, and **Right-Click Scan**):
        - Select **Detect unwanted programs**.
        - Under **Actions**, configure responses to unwanted programs.
3. Configure **Custom On-Demand Scan** client task settings.
    a. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
    b. Select **Endpoint Security Threat Prevention**.
    c. Click **New Task**.
    d. From **Task Types**, select **Custom On-Demand Scan**.
    e. Under **Scan Options**, select **Detect unwanted programs**.
    f. Under **Actions**, configure responses to unwanted programs.

Configure scans that run automatically when files are accessed

On-access scan configuration includes settings based on process type, and defining messages to send when a threat is detected.

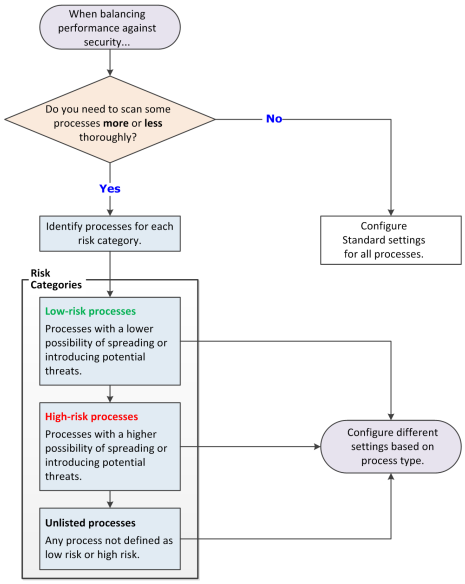
Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **On-Access Scan**.

3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Select **Enable On-Access Scan** to enable the on-access scanner and change options.
6. Specify whether to use Standard settings for all processes, or different settings for high-risk and low-risk processes.
    - **Use Standard settings for all processes** — Configure the scan settings on the **Standard** tab.
    - **Configure different settings for High Risk and Low Risk processes** — Select the tab (**Standard**, **High Risk**, or **Low Risk**) and configure the scan settings for each process type.
7. Configure settings on the page, then click **Save**.

Determining which scanning policies you need

Decide if you need more than one on-access scanning policy for your environment.



Choosing when to scan files with the on-access scanner

You can specify when the on-access scanner examines files: when writing to disk, when reading from disk, both, or let Trellix decide when to scan.

When writing to disk ("Write scan")

Caution

The Write scan option doesn't prevent access to files, either before or after scanning, and so can leave your system vulnerable to attack.

When you select Write scan, the scanner examines the file only after it has been written to disk and closed. A process can perform a Read, Open, or Execute operation on the file before the scanner can perform a Write scan, potentially resulting in infection. Applications might also encounter SHARING_VIOLATION errors if they access the file again after writing it, while a Write scan is in progress.

The on-access scanner examines when files are:

- Created or changed on the local hard drive.
- Copied or moved from a mapped drive to the local hard drive (if the **On network drives** option is also enabled).
- Copied or moved from the local hard drive to a mapped drive (if the **On network drives** option is also enabled).

When reading from disk ("Read scan")

Best practice: Enable the Read scan option to provide security against outbreaks.

When you select Read scan, the scanner prevents access to files unless they are determined to be clean.

The on-access scanner examines when files are:

- Read, opened, or executed from the local hard drive
- Read, opened, or executed from mapped network drives (if the **On network drives** option is also enabled)

Let Trellix decide

Best practice: Enable this option for the best protection and performance.

When you select this option, the on-access scanner uses trust logic to optimize scanning. Trust logic improves your security and boosts performance with scan avoidance — avoiding unnecessary scans. For example, Trellix analyzes and considers some programs to be trustworthy. If Trellix verifies that these programs haven't been tampered with, the scanner might perform reduced or optimized scanning.

Let me decide

When you select this option, you can choose whether the on-access scanner scans when writing to disk, when reading from disk, or both.

Best practices: Reducing the impact of on-access scans on users

To minimize the impact that on-access scans have on a system, select options to avoid impacting system performance and scan only what you need to.

Tip

Best practice: For information about troubleshooting high CPU usage with the on-access scanner, see KB89354. For suggestions on how to improve Trellix ENS performance, see KB88205.

Choose performance options

Some scan options can negatively affect system performance. For this reason, select these options only if you need to scan specific items. Select or deselect these options in the **On-Access Scan** settings.

- **Scan processes on service startup and content update** — Rescans all processes that are currently in memory each time:
    - You re-enable on-access scans.
    - Content files are updated.
    - The Threat Prevention service starts.
    - The system starts.

  Because some programs or executables start automatically when you start your system, deselect this option to improve system startup time.
- **Scan trusted installers** — Scans MSI files (installed by msiexec.exe and signed by Trellix or Microsoft) or Windows Trusted Installer service files. Deselect this option to improve the performance of large Microsoft application installers.

Scan only what you need to

Scanning some types of files can negatively affect system performance. For this reason, select these options only if you need to scan specific types of files. Select or deselect these options in the **What to Scan** section of the **On-Access Scan** settings.

- **On network drives** — Scans resources on mapped network drives. Deselect this option to improve performance. If you deselect this option, Adaptive Threat Protection won't scan files on network drives.
- **Opened for backups** — Scans files when accessed by backup software. For most environments, you don't need to select this setting.
- **Compressed archive files** — Examines the contents of archive (compressed) files, including .jar files. Even if an archive contains infected files, the files can't infect the system until the archive is extracted. Once the archive is extracted, the On-Access Scan examines the files and detects any malware.

Tip

Best practice: For information about solving slow performance with Java-based applications, see KB58727.

Configure Threat Prevention with no connection to Trellix GTI

For systems with no network connection to Adaptive Threat Protection, such as air-gapped systems, you can improve performance by manually disabling Adaptive Threat Protection.

Disable Adaptive Threat Protection to eliminate unnecessary attempts to connect to Adaptive Threat Protection when no network path exists and reduce the impact on Trellix ENS performance.

Caution

Disabling Adaptive Threat Protection might result in increased false positives.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **On-Access Scan**.
3. Click the **Edit** link for an editable policy.
4. In the **Trellix GTI** section, deselect **Enable Trellix GTI**, then click **Save**.

Verify ScriptScan exclusions

URLs excluded from ScriptScan appear in the On-Access Scan Debug log.

Task

1. Enable debug logging for Threat Prevention **On-Access Scan** in the Common **Options** settings.
2. Visit the excluded URL.
   For each excluded URL visited, ScriptScan includes an entry in the debug log, indicating the URL was excluded.
3. In the OnAccessScan_Debug.log file, search for "ExcludedURL".
   For example:

   ```
   ExcludedURLs: corp.mcafee.com
   ```

Configure predefined scans that can be run manually or scheduled

You can configure the behavior of three predefined on-demand scans: **Quick Scan**, **Full Scan**, and **Right-Click Scan**.

Best practice: For best practices for configuring on-demand scans, see KB74059.

Users can run these scans at any time on their system. To run the predefined **Quick Scan** or **Full Scan** on a client system from Trellix ePO - On-prem, schedule a **Policy-Based On-Demand Scan** client task.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **On-Demand Scan**.
3. Click the **Edit** link for an editable policy.
4. Click a tab to configure settings for the specified scan.
   - **Quick Scan**
   - **Full Scan**
   - **Right-Click Scan**
5. Configure settings on the page, then click **Save**.

Best practices: Reducing the impact of on-demand scans on users

To minimize the impact that on-demand scans have on a system, you can select options to avoid impacting system performance and scan only what you need to.

Best practice: For suggestions on how to improve Trellix ENS performance, see KB88205.

Scan only when the system is idle

The easiest way to make sure that the scan has no impact on users is to run the on-demand scan only when the computer is idle.

When this option is enabled, Threat Prevention pauses the scan when it detects disk or user activity, such as access using the keyboard or mouse. Threat Prevention resumes the scan when the user hasn't accessed the system for three minutes.

You can optionally:

- Allow users to resume scans that have been paused due to user activity.
- Return the scan to run only when the system is idle.

Disable this option only on server systems and systems that users access using Remote Desktop Connection (RDP). Threat Prevention depends on the Trellix notification area icon to determine if the system is idle. On systems accessed only by RDP, the notification area icon doesn't start and the on-demand scanner never runs. To work around this issue, add the UpdaterUI.exe to the logon script.

Select **Scan only when the system is idle** in the **Performance** section of the **Custom On-Demand Scan** client task settings.

Pause scans automatically

To improve performance, you can pause on-demand scans when the system is running on battery power. You can also pause the scan when an application, such as a browser, media player, or presentation, is running in full-screen mode. The scan resumes immediately when the system is connected to power or is no longer in full-screen mode.

- **Do not scan when the system is on battery power**
- **Do not scan when the system is in presentation mode** (available when **Scan anytime** is enabled)

Select these options in the **Performance** section of the **Custom On-Demand Scan** client task settings.

Allow users to defer scans

If you choose **Scan anytime**, you can allow users to defer scheduled scans in one-hour increments, up to 24 hours, or forever. Each user deferral can last one hour. For example, if the **Maximum number of hours user can defer** option is set to 2, the user can defer the scan twice (two hours). When the maximum specified number of hours elapses, the scan continues.

Select **User can defer scans** in the **Performance** section of the **Custom On-Demand Scan** client task settings.

Limit scan activity with incremental scans

Use incremental, or resumable, scans to limit when on-demand scan activity occurs, and still scan the whole system in multiple sessions. To use incremental scanning, add a time limit to the scheduled scan. The scan stops when the time limit is reached. The next time this task starts, it continues from the point in the file and folder structure where the previous scan stopped.

Select **Stop the task if it runs for** on the **Schedule** page for the **Custom On-Demand Scan** client task.

See Trellix ePO - On-prem Help for schedule information and the **Client Task Assignment Builder**.

In Trellix ePO - On-prem, check the **Systems Information Product properties** for Threat Prevention for scan statistics, such start time, end time, and time to complete the scan.

Configure system utilization

System utilization specifies the amount of CPU time that the scanner receives during the scan. For systems with end-user activity, set system utilization to **Low**.

You can use the Windows Task Manager to view CPU utilization consumed by the Trellix Scanner service process (mcshield.exe).

The scan process for **Full Scan** and **Quick Scan** on-demand scans runs at low priority. But, if no other processes are running during a scan, the mcshield.exe process might consume a higher amount of CPU resources. If any other processes make system requests, mcshield.exe releases the CPU resources.

Select **System utilization** in the **Performance** section of the **On-Demand Scan** client task settings.

Specify the maximum CPU percentage for scans

As an alternative to using system utilization to automatically determine the amount of CPU the scan uses, you can specify a maximum percentage. In this case, the CPU usage for **Full Scan**, **Quick Scan**, and custom scans is limited to the percentage you specify. For example, if you specify 60%, the full scan consumes 60% of the available CPU.

Note

Right-click scan is not supported.

In certain scenarios, such as in systems with a single core CPU, it has been observed that the CPU utilization exceeds the defined limit. For example, if the threshold value is set to 40%, there are chances that the CPU usage might exceed the defined threshold. But the additional usage does not exceed 5% and the scanning process is not affected because of the sudden spike.

Because the scan is single-threaded, if the system has multiple CPUs, the scan uses the percentage of 1 CPU. So, if you want to limit the scan to 25% of the total CPU processing power of a 4-CPU system, set the percentage to 25%.

This option only applies to scanning files. It doesn't limit CPU usage when scanning other items, such as memory, registry, and boot sectors.

Note

This option is available only when the **Scan anytime** option is selected.

Custom scans	In the **Custom On-Demand Scan** client task settings: 1. Select **Scan anytime** in the **Scheduled Scan Options** section.

	2. Select **Limit maximum CPU usage** in the **Performance** section.
Quick and full scans	In the **On-Demand Scan** policy on the appropriate tab (**Full Scan** or **Quick Scan**): 1. Select **Scan anytime** in the **Scheduled Scan Options** section. 2. Select **Limit maximum CPU usage** in the **Performance** section.

Scan only what you need to

Scanning some types of files can negatively affect system performance. For this reason, select these options only if you need to scan specific types of files.

Select or deselect these options in the **What to Scan** section of the **Custom On-Demand Scan** client task settings.

- **Files that have been migrated to storage** Some offline data storage solutions replace files with a stub file. When the scanner encounters a stub file, which indicates that the file has been migrated, the scanner restores the file to the local system before scanning. The restore process can negatively impact system performance. Deselect this option unless you have a specific need to scan files in storage.

  Note

  This option doesn't apply to files stored in Microsoft OneDrive. The on-demand scanner doesn't download OneDrive files or scan files that haven't been downloaded.

- **Compressed archive files** Even if an archive contains infected files, the files can't infect the system until the archive is extracted. Once the archive is extracted, the On-Access Scan examines the files and detects any malware. **Best practice:** Because scanning compressed archive files can negatively affect system performance, deselect this option to improve system performance.

Schedule quick scans and full scans from Trellix ePO - On-prem

Use a client task to run a predefined **Full Scan** or **Quick Scan** on computers in the **System Tree**.

Configure the behavior of quick and full scans in the **On-Demand Scan** policy settings.

Task

1. (Optional) Configure the behavior for the scan in the **On-Demand Scan** policy settings.
2. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
3. From **Client Task Types**, select **Endpoint Security Threat Prevention** → **Policy Based On-Demand Scan**.

4. Under **Actions** for the scan type, click the **Assign** link, specify the computers to assign the task to, then click **OK**.
5. Click **2 Schedule** to schedule the task, then click **Save**.

   See Trellix ePO - On-prem Help for schedule information and the **Client Task Assignment Builder**.

Configure and schedule custom scans from Trellix ePO - On-prem

You can create custom on-demand scan client tasks to scan targeted locations and run them on a schedule to avoid impacting users.

Tip

Best practice: For information on how to create a report for completed on-demand scans (event 1203), see KB69428.

Task

1. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
2. From **Client Task Types**, select **Endpoint Security Threat Prevention** → **Custom On-Demand Scan**.
3. Click the name of an existing client task or click **New Task**.
4. Make sure that **Custom On-Demand Scan** is selected, then click **OK**.
5. Configure the settings and click **Save**.
6. Under **Actions**, click the **Assign** link, specify the computers to assign the task to, then click **OK**.
7. Click **2 Schedule** to schedule the task, then click **Save**.

   See Trellix ePO - On-prem Help for schedule information and the **Client Task Assignment Builder**.

We recommend running a daily on-demand scan of memory and running processes.

The scan runs with virtually no impact to system users.

Note

Threat Prevention scans the process memory, the main module (.exe), and all loaded DLL files.

Rootkits and hidden processes function at the operating system level and allow an attacker hidden access to your system at the administrator level. Malware rootkits can inadvertently be installed on a target computer when users:

- Open rich-content files, such as PDF documents.
- Open malicious links that appear legitimate.
- Install a legitimate application with a rootkit added as part of the installation.

Important

If the memory scan detects any malware on a system, run a **Full Scan** immediately.

To scan memory and running processes, configure a **Custom On-Demand Scan**:

1. Select these locations to scan:
    - **Memory for rootkits**
    - **Running processes**
2. Schedule to run the scan once a day at a convenient time.

We recommend scheduling on-demand scans at regular intervals, with the interval based on the system type.

Scanning active user workstations

Because some locations on active user workstations are often targets of malware attacks, Trellix recommends that you scan these workstations more frequently than other systems. Because the locations are limited, the scans are less likely to affect users.

To scan active user workstations, configure a **Custom On-Demand Scan**:

1. Specify these locations to scan:
    - **User profile folder**
    - **Temp folder**
    - **Registered files** (Windows only)
    - **Windows folder** (Windows only)
2. Schedule to run the scan at least weekly, or even daily.

Regular server systems

To scan regular server workstations, configure a **Custom On-Demand Scan**:

1. Select the **Boot sectors** option (Windows only).
2. Specify these locations to scan:
    - **Scan subfolders**
    - **Memory for rootkits** (Windows only)
    - **Running processes** (Windows only)
    - **All local drives**
3. Schedule to run the scan at these intervals.

Daily	Only if you have had a major malware outbreak
Weekly	Recommended — Aggressive and provides good protection
Monthly	Acceptable — Provides decent protection with acceptable risk

Quarterly	Bare minimum scheduling interval

Note

To improve system performance during on-demand scans of **All local drives**, set **System utilization** to **Below Normal** or **Low**.

Pause the On-Demand Scan from Trellix ePO - On-prem

You can pause the custom On-Demand Scan and policy based On-Demand Scan running on the client system from Trellix ePO - On-prem.

Task

1. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
2. From **Client Task Types**, select **Endpoint Security Threat Prevention** → **Pause On-Demad Scan**.
3. Click **New Task**.
4. Make sure **Pause On-Demad Scan** is selected and click **OK**.
5. Provide the task name and click **Save**.
6. Click **Menu** → **System Tree** → **Systems** and select the client system.
7. Click **Actions** → **Agent** → **Run Client Task Now**.
8. In the **Run Client Task Now** page, do the following:
   a. In the **Product** list, select **Endpoint Security Threat Prevention**.
   b. In the **Task Type**, select **Pause On-Demand Scan**.
   c. In the **Task Name**, select the required task name.
   d. Click **Run Task Now**.
9. Click **Server Task Log** to check the status of the paused scan.
   The ongoing scans are paused and the paused scans are resumed during the next scheduled scan or when you reboot the system.

Note

You cannot pause the Full Scan or Quick Scan initiated from the Trellix ENS Client.

Cancel the On-Demand Scan from Trellix ePO - On-prem

You can cancel the custom On-Demand Scan and policy based On-Demand Scan running on the client system from Trellix ePO - On-prem.

Task

1. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
2. From **Client Task Types**, select **Endpoint Security Threat Prevention** → **Cancel On-Demad Scan**.
3. Click **New Task**.
4. Make sure **Cancel On-Demad Scan** is selected and click **OK**.

5. Provide the task name and click **Save**.
6. Click **Menu** → **System Tree** → **Systems** and select the client system.
7. Click **Actions** → **Agent** → **Run Client Task Now**.
8. In the **Run Client Task Now** page, do the following:
    a. In the **Product** list, select **Endpoint Security Threat Prevention**.
    b. In the **Task Type**, select **Cancel On-Demand Scan**.
    c. In the **Task Name**, select the required task name.
    d. Click **Run Task Now**.
9. Click **Server Task Log** to check the status of the cancelled scan.
   The ongoing scans are cancelled and you can reinitiate the scans if required.

Note

You cannot cancel the Full Scan or Quick Scan initiated from the Trellix ENS Client.

Configuring Firewall

Policies and Firewall

Policies let you configure, apply, and enforce settings for managed systems in your environment.

Policies are collections of settings that you create, configure, and apply, then enforce. Most policy settings correspond to settings that you configure in the Trellix Endpoint Security (ENS) Client. Other policy settings are the primary interface for configuring the software.

Your managed product adds these categories to the **Policy Catalog**. The available settings vary in each category.

Firewall categories

Category	Description
Options	Specifies options for the Firewall, including: • Turns on or off firewall protection. • Applies Adaptive mode for tuning. • Defines the domain name servers (DNS) to block. • Defines networks and trusted executables to use in rules and groups.
Rules	Specifies firewall rules, and groups of rules, that define what traffic is allowed and what is blocked. When DNS blocking is enabled in **Options**, this policy dynamically adds a rule near the top of the firewall

Category	Description
	rules list. This rule prevents resolving the IP address of the specified domain.

In addition, Firewall adds the **Firewall Catalog**. The **Firewall Catalog** simplifies firewall rule and group creation by enabling you to reference existing rules, groups, network options, applications, executables, and locations.

Customizing policies (Trellix ePO - On-prem)

Each policy category includes default policies.

You can use default policies as is, edit the **My Default** default policies, or create policies.

Firewall default policies

Policy	Description	Management platform
Trellix Default	Defines the default policy that takes effect if no other policy is applied. You can duplicate, but not delete or change, this policy.	All
Trellix Default Server	Defines the default server **Rules** policy, which allows all server default services, such as Windows AD Authentication, Web/FTP, and mail servers, to accept client service requests. You can duplicate, but not delete or change, this policy.	All
My Default	Defines default settings for the category.	Trellix ePO - On-prem

User-based policies (Trellix ePO - On-prem)

User-based policies (UBP) enable policies to be defined and enforced using Trellix ePO - On-prem policy assignment rules with an LDAP server. These assignment rules are enforced on the client system for the user at log-on, regardless of the Trellix ePO - On-prem group.

User-based policies are enforced when a user with a matching assignment rule logs on to the client system on the console. System-based policies (SBP) are enforced when two or more users are logged on to a system. Policy assignment rules take precedence over policies defined in the **System Tree**.

The user policy supersedes the system policy. All system policies apply and any user-based policy overrides the system policy.

Policy assignment rules are enforced only if the user logs on as the **interactive** user. The system policy, rather than the user policy, is enforced if the user logs on:

- With a **runas** command
- To a remote desktop or terminal service where the user's logon is not set to interactive

For more information about user-based policies and policy assignment rules, see the Trellix ePO - On-prem Help.

Comparing policies

You can compare all policy settings for the module using the **Policy Comparison** feature in Trellix ePO - On-prem. For information, see the Trellix ePO - On-prem Help.

For information about policies and the **Policy Catalog**, see the Trellix ePO - On-prem documentation.

Enable and configure Firewall

You can configure settings for Firewall to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Select **Enable Firewall** to make the firewall active and change its options.

Note

Host Intrusion Prevention 8.0 can be installed on the same system as Trellix ENS version 10.7. If McAfee Host IPS Firewall is installed and enabled, Trellix ENS Firewall is disabled even if enabled in the settings.

5. Click **Show Advanced**.
6. Configure settings on the page, then click **Save**.

Block DNS traffic

To refine firewall protection, you can create a list of FQDNs to block. Firewall blocks connections to the IP addresses resolving to the domain names.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Under **DNS Blocking**, click **Add**.
5. Enter the comma-separated FQDN of the domains to block, then click **Save**.

You can use the * and ? wildcards. For example, *domain.com.

Duplicate entries are removed automatically.

Note

If the firewall host has not initiated any DNS queries for the blocked domains or FQDN, the DNS blocking and FQDN-based rules do not work.

6. Click **Save**.

Define networks to use in rules and groups

You can define network addresses, subnets, or ranges to use in rules and groups, or define networks as trusted.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Click **Show Advanced**.
5. Under **Defined Networks**, click **Add Defined Network**.
6. Select the type from **Address type**, then enter a trusted IP address, subnet, or range in the **Address** field.
7. Select either **Trusted** or **Not trusted** from the drop-down menu.
    - **Trusted** — Firewall allows all traffic to and from trusted networks.
    - **Not trusted** — Defines networks for use in rules and groups. You can use networks defined as not trusted for the local or remote network criteria in a rule or group. Defining a network as not trusted adds those networks as exceptions to Trellix GTI rules in Firewall and excludes those networks from a Trellix GTI lookup.
8. Click **Save**.

Exclude network addresses from a Trellix GTI lookup

You can exclude certain network addresses from a Trellix GTI lookup to reduce traffic and improve performance.

Note

Trellix GTI automatically excludes certain IP addresses from a reputation check. For more information, see KB90837.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Click **Show Advanced**.
5. Under **Defined Networks**, click **Add Defined Network** or **+**.
6. From the **Address type** drop-down list, select the address type.

7. In the **Address** field, enter the address.
8. From the drop-down list, select **Not trusted**.
9. Click **Save**.

Configure trusted executables

Trusted executables are ones that are considered safe for your environment.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click **Show Advanced**.
4. Under **Trusted Executables**, click **Add**.
5. Configure the executable properties, then click **Save**.
6. Click **Save**.

Get the signer distinguished name from Trellix ePO - On-prem to use to specify trusted executables

The signer distinguished name (SDN) is required when you enable a digital signature check and add only files signed by a specified process signer.

Task

1. Select **Menu** → **Reporting** → **Threat Event Log**.
2. Click the Trellix ENS event to display details.
3. Select and copy the **Source Process Signer** details.
4. When specifying trusted executables, paste the **Source Process Signer** details to the **Signed by** field.

   For example, the SDN required format is:

   ```
   C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION
   ```

Manage firewall rules and groups

You can use firewall rule groups to group a set of rules with a single purpose.

For example, configure a group with rules to allow VPN connection. Groups appear in the rule list preceded by an arrow, which you can click to show or hide the rules in the group.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Rules**.
3. Click the name of an editable policy.
4. Do any of the following.

To...	Steps
Add a firewall rule	Click **Add Rule** or **Add Rule from Catalog**.
Add a firewall group	Click **Add Group** or **Add Group from Catalog**.
Change an existing rule or group	Select the rule or group and click **Edit** under **Actions**.
Make a copy of a rule or group	Select the rule or group and click **Duplicate**.
Delete a rule or group	Select the rule or group and click **Delete**.
Add an item to the **Firewall Catalog**	Click **Add to Catalog** under **Actions**.
Move an item up or down in the list	Select the rule or group and click **Move Up** or **Move Down**.
Export all rule and group information in the policy to an XML file	Click **Export**. You can then import this file into the **Firewall Catalog** or to another policy.

5. Click **Save**.

Wildcards in firewall rules

You can use wildcards to represent characters for some values in firewall rules. Wildcards match zero or more characters so that you don't have to specify an entire path or value, or set of values.

Firewall supports wildcards in blocked domains and executable paths only.

For paths of files, registry keys, executables, and URLs, use these wildcards.

Note

Registry key paths for firewall group locations don't recognize wildcard values.

?	Question mark	A single character. This wildcard applies only if the number of characters matches the length of the file or folder name. **For example:** The exclusion W?? excludes W**WW**, but doesn't exclude WW or WWWW.
*	Asterisk	Multiple characters, excluding slash (/) and backslash (\). Use this character to match the root-level contents of a folder with no subfolders. **Note:** *\ at the beginning of a file path is not valid. Use **\ instead. For example: **\ABC*.
**	Double asterisk	Multiple characters, including slash (/) and backslash (\). This wildcard matches zero or more characters. For example: C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ.
|	Pipe	Wildcard escape. **Note:** For the double asterisk (**), the escape is |*|*.

Note

Wildcards can appear in front of a backslash (\) in a path. For example, C:\ABC*\XYZ matches C:\ABC\DEF\XYZ.

For values that normally don't contain path information with slashes, use these wildcards.

?	Question mark	A single character.
*	Asterisk	Multiple characters, including slash (/) and backslash (\).
|	Pipe	Wildcard escape.

Wildcard examples

DNS Blocking feature- Use wildcards to match domain names and subdomains names.

*.domain.com
*domain.com
*subdomain.domain.com
*.subdomain.domain.com

Executable file path criteria- Trusted Executables, Firewall Rule Executables, and Firewall Group Executables.

When defining executables in the firewall configuration rules/groups, use executable file extensions such as .exe, .com, etc.

Note

Wildcards can’t be used in FQDN (fully qualified domain name) values, both in local and remote network. They are also restricted for usage in executable file descriptions, hash and signer details.

Example	Description
**\Temp\test.exe	Defines a specific executable file in a folder named Temp anywhere on the system.
**\test.exe	Defines a specific executable file anywhere on the system.

Example	Description
**\test.exe	Defines a specific executable file in any folder on a specific drive.
C:\Users*\Desktop\test.exe	Define a specific executable file on any user's profile Desktop directory.
C:\Program Files*\test.exe	Define a specific executable file to run from either the \Program Files or \Program Files (x86)\ directories.
**\test*.exe	Define a specific executable file to run if the filename starts with "test"
**\test?.exe	Define a specific executable file to run if the filename matches testX.com, where X is any valid character for a file name
C:\Program Files\Test*	Define an executable match for all executables in a specific directory.
C:\Program Files\Test**	Define an executable match for all executables in a specific directory and all sub-directories.

Create connection isolation groups

A connection isolation firewall rule group instructs Firewall to process only traffic that matches the defined connection type and group criteria.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Rules**.
3. Click the name of an editable policy.
4. On the **Rules** policy page, click **Add Group** or **Add Group from Catalog**.
5. Under **Description**, specify options for the group.
6. Under **Location**, select **Enable location awareness** and **Enable connection isolation**. Then, select the location criteria for matching.
7. Under **Networks**, for **Connection types**, select the type of connection (**Wired**, **Wireless**, or **Virtual**) to apply to the rules in this group.

Note

Settings for **Transport** and **Executables** aren't available for connection isolation groups.

8. Click **Save**.
9. Create new rules within this group, or move existing rules into it from the firewall rule list or the **Firewall Catalog**.
10. Click **Save**.

Create timed groups

You can create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Firewall** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Rules**.
3. Click the name of an editable policy.
4. Create a Firewall group with default settings that allow Internet connectivity.
   For example, allow port 80 HTTP traffic.
5. In the **Schedule** section, select how to enable the group.
   - **Enable schedule** — Specifies a start and end time for the group to be enabled.
   - **Disable schedule and enable the group from the Trellix system tray icon** — Allows users to enable the group from the Trellix system tray icon and keeps the group enabled for the specified number of minutes. If you allow users to manage the timed group, you can optionally require that they provide a justification before enabling the group.
6. Create a connection isolation group that matches the VPN network to allow needed traffic.

Tip

Best practice: To allow outbound traffic from only the connection isolation group on the client system, don't place any Firewall rules below this group.

7. Click **Save**.

Use the Firewall Catalog

The **Firewall Catalog** is a repository of items that you can use with Firewall. For example, you can define rule and groups to add to multiple policies or networks and applications to add to firewall rules.

Note

You can add an item to or from the catalog while creating a firewall rule or group. When you add an item, you create a link between the item and the catalog — items inherits properties from items in the catalog. To break the inheritance and create a new independent item, click **Break Catalog Inheritance**.

Best Practice:

- Firewall Catalog objects must be manually imported or exported between ePO Server.
- Firewall catalog object must be imported before importing Firewall Catalog rules and groups.
- While importing Firewall Catalog, ensure that you import in the following order:
    - Catalog RULES
    - Catalog GROUPS
    - Other Firewall Catalog objects
    - Policy Catalog Firewall RULES Policies
- Note that, during import, all duplicate entries will be skipped. Entries with the same GUIDs will be ignored and only unique entries are added to the database.
- Ensure that the firewall policy size doesn't cross 2 MB in size.
- Firewall Catalog cannot be actioned using any back-end web APIs.

Task

1. Select **Menu** → **Policy** → **Firewall Catalog**.
2. From the **Item type** drop-down list, select a catalog item.
3. Do any of the following on the **Firewall Catalog** page.

To...	Steps
Filter for an item.	Click **Show Filter Items**, enter filter criteria, then click **Set Filter**. Click **Clear** to return to the default view.
Change the view of items.	Select **Options** → **Choose Columns**, change the columns, then click **Save**.
Change an item.	Click the **Edit** link associated with the item.
Create and add an item to the catalog.	Click **New**.
Delete an existing item.	Click the **Delete** link associated with the item. **Note:** If you delete an item with a dependent link, a new, independent copy of that item is placed with the linking rule or group.
Export a single item.	Click the **Export** link associated with the item.

To...	Steps
Export all items of the catalog type.	Click **Export** in the upper-right corner of the page, then name and save the XML file.
Import items of the catalog type.	Click **Import** in the upper-right corner of the page, then locate and open the XML file with catalog data.

Tuning Firewall

Tuning involves balancing intrusion prevention protection with access to required information and applications per group type. Tuning involves finding the right balance between protecting your environment from intrusions and allowing access to required information and applications.

During Firewall deployment, identify a few distinct usage profiles and create policies for them. The best way to achieve this goal is to set up a test deployment, then begin reducing the number of false positives and generated events. This process is called tuning.

You can reduce the number of false positives by creating:

- **Exception rules** — Mechanisms for overriding a setting in specific circumstances.
- **Trusted executables** — Executable processes that ignore all firewall rules.
- **Firewall rules** — Determine whether traffic is permissible, and block packet reception or allow or block packet transmission.

Automatic tuning using Adaptive mode

Automatic tuning removes the need to constantly monitor all events and activities for all users.

To help tune protection settings, place clients in Adaptive mode. In Adaptive mode, client rules are created automatically to allow legitimate activity. After client rules are created, analyze them and decide which to convert to server-mandated policies.

Often in a large organization, avoiding disruption to business takes priority over security concerns. For example, you might need to install new applications on some computers, and you might not have the time or resources to immediately tune them. You can place specific computers in Adaptive mode to profile a newly installed application, and forward the resulting client rules to the management server. You can then promote these client rules to an existing or new policy and apply the policy to other computers to handle the new software.

Caution

Systems in Adaptive mode have virtually no protection. For this reason, use Adaptive mode only for tuning an environment, then turn it off to tighten the system's protection.

1. Apply Adaptive mode for Firewall policies.
2. Review the lists of client rules.
3. Promote appropriate client rules to administrative policy rules.
4. After at least a week, turn off Adaptive mode.
5. Monitor the test group for a few days to make sure that the policy settings are appropriate and offer the wanted protection.
6. Repeat this process with each group of similar computers.

Manual tuning

Manual tuning requires direct monitoring of events and client rules that are created.

1. Monitor events for false positives and create exceptions or trusted applications to prevent these events from reoccurring.
2. Monitor network traffic and define trusted networks to allow appropriate network traffic.
3. Monitor the effects of the new exceptions, trusted executables, and trusted networks.
4. If these rules prevent false positives, keep network traffic to a minimum, and allow legitimate activity, add them to the policy.
5. Apply the new policy to a set of computers and monitor the results.
6. Repeat this process with each group of similar computers.

Using Adaptive mode to create client rules automatically

Place systems in Adaptive mode so that Firewall can create client rules automatically without user interaction.

Tip

Best practice: Enable Adaptive mode temporarily on a few systems only while tuning Firewall. Enabling this mode might generate many client rules, which the Trellix ePO - On-prem server must process, negatively affecting performance.

Adaptive mode analyzes events first for the most malicious attacks. If the activity is considered regular and needed for business, Firewall creates client rules. By enabling Adaptive mode on representative clients, you can create a tuning configuration. You can then convert client rules to server-mandated policies. When tuning is complete, turn off Adaptive mode to tighten the system's protection.

Run client systems in Adaptive mode for at least a week. In this time, client systems encounter all normal activity, including scheduled activity, such as backups or script processing. As activity occurs, Firewall generates events and creates rules.

FAQ — Adaptive mode

Here are answers to frequently asked questions.

Adaptive mode is a setting that you can apply to Firewall when testing new rollouts. This mode enables the client system to automatically create rules that allow activity while preserving minimum protection against vulnerabilities. The following questions and answers can help you use this feature.

How do you turn on Adaptive mode?

Enable this option in the Firewall **Options** settings.
Enable this option in the Firewall **Options** settings and apply this policy to the client.

How does Adaptive mode work with Firewall?

Adaptive mode creates rules on the client system that allow network packets not covered by existing firewall rules. Firewall client rules are created on a per-process basis. The processes associated with firewall client rules are based on path, file description, digital signature, and MD5 hash.

When is a rule not created automatically with Adaptive mode?

- There is no application associated with the packet when examined in the client activity log. Some of the most common examples include:
    - Incoming requests for services that aren't running, such as FTP or telnet
    - Incoming ICMP, such as an echo request
    - Incoming or outgoing ICMP on Windows Vista
    - TCP packets to port 139 (NetBIOS SSN) or 445 (MSDS), which might be required for Windows file sharing
    - IPsec packets associated with VPN client solutions
- There is already a rule that blocks or allows the packet.
- The applied **Rules** policy has a location-aware group with connection isolation enabled and the following is true:
    - An active NIC matches the group.
    - The packet is sent or received on a NIC that doesn't match the group.
- The packet isn't TCP, UDP, or ICMP.
- More than one user is logged on to the system, or no user is logged on to the system.

Analyzing client data

To tune your deployment, analyze client rules created in Adaptive mode, and events triggered by activity on the clients.

- From client rules data, you can:
    - See which rules are being created.
    - Aggregate rules to find the most common rules.
    - Move the rules directly to a policy for application to other clients.
- From event data, you can see firewall intrusions and Trellix Global Threat Intelligence block events. Drill down to the details of an event to see:
    - Which process triggered the event
    - When the event was generated
    - Which client generated the event

  Use Trellix ePO - On-prem queries and reports to gather information about client rules. Use the **Threat Event Log** to view all threat events that Trellix ePO - On-prem receives from managed systems. Analyze the event and take the appropriate action to tune the Firewall deployment to provide better response to attacks.

Manage Firewall client rules

Tune and tighten security by reviewing Firewall client rules and moving them to a **Rules** policy.

Firewall client rules are created manually on a client or automatically in Adaptive mode.

For information about server tasks, see the Trellix ePO - On-prem documentation.

Task

1. From the **System Tree**, click **Wake Up Agents**.
   The agent wake-up call collects the Firewall client properties, including client rules, from the client.
2. Select **Menu** → **Automation** → **Server Tasks**, then run the **Endpoint Security Firewall Property Translator** server task.
   When enabled, the **Endpoint Security Firewall Property Translator** task runs automatically every 60 minutes, scans the client properties for Firewall client rules, and adds them to the **Firewall Client Rules** page.
3. Select **Menu** → **Reporting** → **Firewall Client Rules**.
4. In the **System Tree**, select a group to display its details.
5. Review the client rules to determine which rules to promote to a **Rules** policy.
6. Move rules to a policy by selecting rules, clicking **New Firewall Rule**, then indicating the policy to move the rules to.
7. In the Firewall **Options** policy, deselect these options:
   - **Enable Adaptive mode**
   - **Retain existing user-added rules and Adaptive mode rules when this policy is enforced**
8. Enforce the updated **Options** and **Rules** policies.

Results

The rules from the **Rules** policy replace the client rules that were created on the client system.

Configuring Web Control

Policies and Web Control

Policies let you configure, apply, and enforce settings for managed systems in your environment.

Policies are collections of settings that you create, configure, and apply, then enforce. Most policy settings correspond to settings that you configure in the Trellix Endpoint Security (ENS) Client. Other policy settings are the primary interface for configuring the software.

Your managed product adds these categories to the **Policy Catalog**. The available settings vary in each category.

Web Control policy categories

Category	Description
Block and Allow List (Multiple-instance)	Configures the **Block and Allow List**, including: • Sites that users are allowed to access • Sites that users are blocked from accessing

Category	Description
	• Access to individual resources, such as file downloads, on the sites • Whether the allowed sites have precedence over blocked sites You can apply several instances of this policy, resulting in one combined, effective policy.
Browser Control	Configures settings to prohibit specific supported and unsupported browsers.
Content Actions (Multiple-instance)	Configures rules for user access, based on the safety ratings assigned to: • Categories of web content • Websites • File downloads You can apply several instances of this policy, resulting in one combined, effective policy.
Enforcement Messaging	Specifies messages and explanations, which can include your own image, to display when users attempt to access: • Sites blocked and warned by **Rating Actions** • File downloads blocked and warned by **Rating Actions** • Phishing pages • Blocked sites on the **Block and Allow List** • Sites blocked when Trellix GTI is unreachable • Sites blocked and warned that Trellix GTI has not yet verified
Options	Configures general settings, including: • Disable and enable the client software. • Prevent users from uninstalling or disabling the browser plug-in. • Show and hide Web Control in the browser. • Configure action enforcement behavior. • Enable Observe mode to evaluate and tune policy settings before implementing them.

Category	Description
	• Specify Secure Search settings. • Configure logging. • Configure Web Reporter. • Set up Web Control behavior if your organization implements a web gateway.

Customizing policies (Trellix ePO - On-prem)

Each policy category includes default policies.

You can use default policies as is, edit the **My Default** default policies, or create policies.

Web Control default policies

Policy	Description	Management platform
Trellix Default	Defines the default policy that takes effect if no other policy is applied. You can duplicate, but not delete or modify, this policy.	All
My Default	Defines default settings for the category.	Trellix ePO - On-prem

Multiple-instance policies

The **Content Actions** and **Block and Allow List** policies are multiple instance policies. You can assign more than one policy instance to a client. For the policies that have multiple instances, an **Effective Policy** link provides a view of the details of the combined policy instances.

User-based policies (Trellix ePO - On-prem)

User-based policies (UBP) enable policies to be defined and enforced using Trellix ePO - On-prem policy assignment rules with an LDAP server. These assignment rules are enforced on the client system for the user at log-on, regardless of the Trellix ePO - On-prem group.

User-based policies are enforced when a user with a matching assignment rule logs on to the client system on the console. System-based policies (SBP) are enforced when two or more users are logged on to a system. Policy assignment rules take precedence over policies defined in the **System Tree**.

The user policy supersedes the system policy. All system policies apply and any user-based policy overrides the system policy.

Policy assignment rules are enforced only if the user logs on as the **interactive** user. The system policy, rather than the user policy, is enforced if the user logs on:

- With a **runas** command
- To a remote desktop or terminal service where the user's logon is not set to interactive

For more information about user-based policies and policy assignment rules, see the Trellix ePO - On-prem Help.

Comparing policies

You can compare all policy settings for the module using the **Policy Comparison** feature in Trellix ePO - On-prem. For information, see the Trellix ePO - On-prem Help.

For information about policies and the **Policy Catalog**, see the Trellix ePO - On-prem documentation.

How policies work

Web Control includes preconfigured default policies. You can't change the default policies, but you can create copies and modify them to meet your browsing protection needs.

You then assign the policy to managed systems running the client software. You can assign the same policy settings to all managed systems, or to groups of managed systems that require the same type of access and protection.

Multiple-instance policies

Multiple-instance policies, such as **Block and Allow List** and **Content Actions**, support combining multiple policies under a single effective policy.

Multiple-instance policies obey the Trellix ePO - On-prem laws of inheritance within a **System Tree**. See the Trellix ePO - On-prem Help.

You can use multiple-instance policies to apply a default list of sites, and add entries for a particular group or all groups. Instead of updating the entire list with the new entries, create a second policy instance for the new entries. Then, apply it and the default list together. The effective policy is then the combination of the two policies.

For example, you configure one **Block and Allow List** policy for Group A, another for Group B, and another for Group C. If Group A contains Group B, and Group B contains Group C, the **Block and Allow List** policy incorporates elements from the three policies. The allowed list for Group C might contain all sites listed for Group A and Group B, and extra sites specific to Group C. By using an effective policy, you don't have to re-enter all sites from Group A and Group B into the allowed list for Group C.

For more information about using policies, see the Trellix ePO - On-prem Help.

Assign multiple instances of a policy

Assign more than one instance of a policy to systems in the **System Tree** to combine multiple instances under one effective policy.

For policies that support multiple instances, an **Effective Policy** link provides details of the combined policies. **Block and Allow List** and **Content Actions** support multiple instances.

Task

1. Select **Menu** → **Systems** → **System Tree** and select a group in the **System Tree**.

   Note

   For one system, select a group in the **System Tree** that contains the system. Then, on the **Systems** tab, select the system and select **Actions** → **Agent** → **Modify Policies on a Single System**.

2. Under **Assigned Policies**, select **Endpoint Security Web Control** in the **Product** list.
3. Click **Edit Assignments** for one of the multiple-instance policies (**Block and Allow List** or **Content Actions**).
4. On the **Policy Assignment** page, click **New Policy Instance**, then select a policy from the **Assigned Policy** drop-down list for the additional policy instance.
   To view the combined effect of multiple policies, click **View Effective Policy**.

   Note

   You can view the effective policy at any time from the **Assigned Policies** tab of the **System Tree**.

5. Click **OK**.

Evaluating policy settings with Observe mode

Observe mode enables you to evaluate the effect of warn or block policy settings on network browsing activity before implementing them.

To enable Observe mode, see enforcement behavior settings in the **Options** policy.

Use Observe mode to track:

- Visits to red, yellow, or unrated sites
- Visits to sites that you configured to block or warn
- Visits to phishing pages if configured to block
- Downloads that you configured to block or warn

Information compiled in Observe mode is available by running queries, then viewing the results in reports or monitors.

If current settings adversely affect network browsing patterns, adjust settings before disabling Observe mode. When you disable Observe mode, Web Control enforces policy settings.

Enable and disable Web Control

Use settings to enable and disable Web Control on all systems managed by the Trellix ePO - On-prem server.

When the software is disabled:

- Policy settings are not enforced.
- The site report can't be displayed.
- The Web Control button is gray.

Tip

Best practice: Only disable Web Control to perform tests or troubleshoot network connection problems. Make sure to re-enable Web Control when you are done.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Configure settings in **Web Control** section.
5. Click **Save**.
6. Run an agent wake-up call to apply the setting immediately, or wait for the next automatic agent-server communication.

Configuring browsers to force-enable the Web Control plug-in

With Active Directory, you can configure Internet Explorer and Chrome to force-enable the Web Control browser plug-in so that users don't have to enable it manually on the client system.

- **Internet Explorer** For information, see Managing Browser Settings with Group Policy Tools.
  - The CLSID for the Web Control Browser Helper Object (BHO) is `{B164E929-A1B6-4A06-B104-2CD0E90A88FF}`.
  - The CLSID for the Web Control toolbar is `{0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064}`.
- **Chrome** For information, see Set Chrome policies for devices.
  - The APPID for Web Control is `jjkchpdmjjdmalgembblgafllbpcjlei`. The APPID is case sensitive.
  - The location where the extension is hosted is `https://clients2.google.com/service/update2/crx`.
- **Chromium Edge** For information, see Configure Microsoft Edge policy settings on Windows.
  - The extensionID for Web Control is `jjkchpdmjjdmalgembblgafllbpcjlei`.
  - The updateURL is the Chrome Web Store update URL, `https://clients2.google.com/service/update2/crx`.

Track browser events to use for reports

Use **Options** settings to configure Web Control events sent from client systems to the Trellix ePO - On-prem database to use for queries and reports.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.

4. Click **Show Advanced**.
5. Under **Event Logging**, configure settings on the page.
6. Click **Save**.

Specify enforcement behavior for specific actions

Configure how Web Control responds to certain situations by defining the behavior in the **Action Enforcement** section of the **Options** settings.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Configure settings in the **Action Enforcement** section.
5. Click **Save**.

Warn about or block unknown URLs and file downloads

Configure **Action Enforcement** settings in the **Options** settings to block, warn, or allow sites that Trellix GTI has not yet rated.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. In **Action Enforcement**, select the action (**Allow**, **Warn**, or **Block**) for sites not yet verified by Trellix GTI .
5. Click **Save**.

Scan files before downloading

Configure Web Control to scan all files before downloading and specify the sensitivity level to use when determining if a detected sample is malware.

Web Control performs a Trellix GTI lookup on the file. If Trellix GTI allows the file, Web Control sends the file to Threat Prevention for scanning. If a downloaded file is detected as a threat, Trellix ENS responds with the configured action and alerts the user.

Note

If users specify the complete URL to a file whose reputation is not malicious, Web Control allows the file download, even if the site is blocked.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Select **Enable file scanning for file downloads**, then select the sensitivity level.

Download files from not yet verified URLs

Configure **Action Enforcement** settings in the **Options** category to download clean files from the unverified URL.

Note

This feature is only available for Google Chrome.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane .
2. In the right pane, select **Options**.
3. Click the editable policy.
4. In **Action Enforcement**, select the action **Block** for sites not yet verified by Trellix GTI .
   Make sure **Enable file scanning for file downloads** option is selected.
5. Select **Allow Green-rated file downloads from not yet verified URL** to download files with clean reputation from the unverified URL.
6. Click **Save**.

Block all internal sites

By default Web Control doesn't block or report on IP addresses on the local private network. You can block all internal sites in the **Options** settings.

To allow specific sites in the local private network, add them to the **Block and Allow List**.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.
4. Deselect **Allow all local IP addresses in the local network**.
5. Click **Save**.

Configure Secure Search

Secure Search automatically filters the malicious sites in the search result based on their safety rating.

Note

Web Control uses Yahoo as the default search engine and supports **Secure Search** on Internet Explorer only.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the name of an editable policy.

4. Select **Enable Secure Search**, select the search engine, then specify whether to block links to risky sites.

   Note

   If you change the default search engine, restart the browser after enforcing the policy on the client system.

   The next time the user opens Internet Explorer, Web Control displays a pop-up prompting the user to change to Trellix Secure Search with the specified search engine. For Internet Explorer versions where the search engine is locked, the Secure Search pop-up doesn't appear.

5. Click **Save**.

Send Web Control logs from Trellix ePO - On-prem to Web Reporter

To send logs from Web Control to Web Reporter, configure **Options** settings and the **Send Web Reporter Logs** client task.

Web Control collects logs of page view and file downloads. The **Send Web Reporter Logs** client task sends the logs to the configured Web Reporter server.

Task

1. Configure Web Reporter settings.
   a. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
   b. From the **Category** list in the right pane, select **Options**.
   c. Click the name of an editable policy.
   d. Click **Show Advanced**.
   e. In **Event Logging**, select **Send browser page views and downloads to Web Reporter** and configure the Web Reporter server settings.
2. Configure the **Send Web Reporter Logs** client task.
   a. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
   b. From **Endpoint Security Web Control** , select **Send Web Reporter Logs**, and create and assign the new task.
   c. On the **Schedule** page, set the schedule for the task. Select **Enable Randomization** and set the randomization period.

      Tip

      Best practice: Because large amounts of data can be transferred when the logs are sent, set the client task to run on a randomized schedule.

      For information about client tasks and the **Client Task Catalog**, see the Trellix ePO - On-prem documentation.

Manage blocked and allowed sites

Define which websites are always allowed or always blocked based on their URL or domain in the **Block and Allow List** settings.

Note

Use the policy options for **Enforcement Messaging** to customize the message that is displayed to users for blocked and warned downloads.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Block and Allow List**.
3. Click the name of an editable policy.
4. Select one of these.

Action	Steps
Add allowed or blocked sites to the **Block and Allow List**.	On the **Block and Allow List** tab: a. Click **Add**. b. From the drop-down, select either **Allow** or **Block.** c. Enter URLs or partial URLs (site patterns) of at least 3 characters. For multiple sites, enter a comma-separated list or enter each site on a separate line. d. Enter a comment or note to associate with the site (optional). e. Click **OK**.
Delete sites from the **Block and Allow List**.	On the **Block and Allow List** tab, select the checkbox next to a site, then click **Delete**.
Change information (URL, site pattern, or comment) for a site.	On the **Block and Allow List** tab: a. Select the checkbox next to a site, then click **Edit**. b. Change the site pattern or comment as needed. c. Click **OK**.
Search the **Block and Allow List**. This feature is useful for finding sites in large lists.	On the **Block and Allow List** tab: a. Enter a URL, site pattern, or text in the **Search** field. b. Click **Search**. Web Control searches all site patterns and comments in the list and shows matches.

Action	Steps
	To remove the search criteria and redisplay the list, click **Clear**.
Test whether specific sites or site patterns are included in the **Block and Allow List**. For example, when a **Block and Allow List** is implemented as a multiple-instance policy, use these steps to test the resulting effective policy.	On the **Block and Allow List** tab: a. Enter a URL or partial URL in the **Search** field. b. Click **Test Pattern**. Web Control displays any site patterns that match your entry. If no site patterns are displayed, the list allows access to the specified URL. To remove the test criteria and results, click **Clear**.
Block or warn file downloads on allowed sites. An allowed site with an overall rating of green can contain individual download files that are rated yellow or red. To protect users, specify an action that is specific to the rating for an individual file.	a. Click **Show Advanced**. b. Select **Enforce actions for file downloads based on their rating**. c. Select an action (**Allow**, **Warn**, or **Block**) for **Red**, **Yellow**, and **Unrated** files.
Set action precedence. By default, when a site is set to both **Allow** and **Block**, the block action takes precedence and the site is blocked. Select this option to override the default behavior and make sure that users can access allowed sites, even if they are also blocked. ⚠ **Caution:** Use caution when selecting this option. Make sure that allowed sites are safe so that client systems remain protected from web-based threats.	a. Click **Show Advanced**. b. Select **Enable allowed sites to take precedence over blocked sites**.

5. Click **Save**.

Prohibit use of specific browsers

Use **Browser Control** settings to prohibit client systems from using supported or unsupported browsers.

Note

The **Browser Control** settings require that **Self Protection** is enabled in the Common settings.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Browser Control**.
3. Click the name of an editable policy.
4. Select the browsers to block from being started on the client systems.
5. Click **Save**.

Specify rating actions and block site access based on web category

You can specify actions, based on safety ratings, to apply to sites and file downloads. You can also block or allow sites in each web category.

Web Control applies the rating actions to sites in the unblocked categories specified in the **Web Category Blocking** section under **Advanced**.

Note

Use the settings in **Enforcement Messaging** to customize the message to display for blocked and warned sites and file downloads, and blocked phishing pages.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Content Actions**.
3. Click **Show Advanced**.
4. In the **Web Category Blocking** section, for each **Web Category**, enable or disable the **Block** option.

   Note

   For sites in the unblocked categories, Web Control also applies the rating actions.

5. In the **Rating Actions** section, specify the actions to apply to any sites and file downloads, based on safety ratings defined by Trellix.

   Note

   These actions also apply to sites that web category blocking doesn't block.

6. Click **Save**.

Customize user notifications for blocked content

Notifications appear when users access a site blocked by ratings or content, or sites in the **Block and Allow List**.

Customize notifications using **Enforcement Messaging** settings. Instead of navigating to the site, users are redirected to a page displaying the customized notification. You might use the notification to explain why a site is blocked.

The notification appears on client systems in the language configured for the client software, if you create the notification in that language.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Web Control** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Enforcement Messaging**.
3. Click the name of an editable policy.
4. Configure messages and explanations for sites and content.

   Don't type **Enter** when specifying enforcement messages. If a message in the policy includes **Enter**, the enforcement message appears blank in the browser.

5. Add an image, such as your company logo, to warn or block pages by specifying the URL link to the image.
6. Click **Save**.

Configuring Adaptive Threat Protection

Policies and Adaptive Threat Protection

Policies let you configure, apply, and enforce settings for managed systems in your environment.

Policies are collections of settings that you create, configure, and apply, then enforce. Most policy settings correspond to settings that you configure in the Trellix Endpoint Security (ENS) Client. Other policy settings are the primary interface for configuring the software.

Your managed product adds these categories to the **Policy Catalog**. The available settings vary in each category.

Adaptive Threat Protection categories

Category	Description
Dynamic Application Containment	Runs applications with specific reputations in a container, blocking actions based on containment rules. Uses the TIE server or Trellix GTI , depending on your configuration, for the application reputation.
Options	Specifies options for Adaptive Threat Protection, including: • Enabling and disabling Adaptive Threat Protection.

Category	Description
	• Selecting the rule group (**Productivity**, **Balanced**, or **Security**), which contains the rules Adaptive Threat Protection uses to calculate reputation. • Enabling and disabling Real Protect client-based and cloud-based scanning. • Enabling and disabling Credential Theft Protection. (It can also be set to run in **Observe Mode**) • Setting reputation thresholds. • Enabling and disabling enhanced remediation. • Configuring user messaging. • Specifying options for sending files to Sandbox server.

Customizing policies (Trellix ePO - On-prem)

Each policy category includes default policies.

You can use default policies as is, edit the **My Default** default policies, or create policies.

Adaptive Threat Protection default policies

Policy	Description	Management platform
Trellix Default	Defines the default policy that takes effect if no other policy is applied. The **Trellix Default** Dynamic Application Containment policy sets rules to **Report** only. Users experience no blocking or prompting. **Note:** To send Dynamic Application Containment Would Block events to Trellix ePO - On-prem, in the Common **Options** settings, set **Adaptive Threat Protection events to log** to **Warning, Critical, and Alert**.	• Trellix ePO - On-prem • Trellix ePO - SaaS

Policy	Description	Management platform
	You can duplicate, but not delete or change, this policy.	
My Default	Defines default settings for the category.	Trellix ePO - On-prem
Trellix Default Balanced	Defines a Dynamic Application Containment policy with **Block** rules set to provide a base level of protection while minimizing false positives for common unsigned installers and applications. Use this policy for typical business systems where new programs and changes are installed infrequently. Users experience some blocking and prompting.	• Trellix ePO - On-prem • Trellix ePO - SaaS
Trellix Default Security	Defines a Dynamic Application Containment policy with **Block** rules to provide aggressive protection. This policy might cause false positives more frequently on unsigned installers and applications.	• Trellix ePO - On-prem • Trellix ePO - SaaS

Note

The Dynamic Application Containment policies, **Trellix Default Balanced** and **Trellix Default Security**, specify rules settings for Dynamic Application Containment only. These policies are different from, and don't affect the **Productivity**, **Balanced**, or **Security** rule groups that Adaptive Threat Protection uses to calculate reputation.

Best practice

Evaluate the impact of Dynamic Application Containment rules by enforcing the **Trellix Default** policy. To determine whether to set rules to block, monitor the logs and reports for "Dynamic Application Containment violation allowed" (event ID 37280) events. Then, set Enterprise-Level Reputations or Dynamic Application Containment exclusions and enforce the **Trellix Default Balanced** policy.

Comparing policies

In Trellix ePO - On-prem 5.0 and later, you can compare policies within the same policy category using **Policy Comparison**.

For information about policies and the **Policy Catalog**, see the Trellix ePO - On-prem documentation.

Containing applications dynamically

Dynamic Application Containment enables you to specify that applications with specific reputations run in a container. Contained applications aren't allowed to perform certain actions, as specified by containment rules.

Based on the reputation threshold, ATP requests that Dynamic Application Containment run the application in a container.

This technology lets you evaluate unknown and potentially unsafe applications by allowing them to run in your environment, while limiting the actions they can take. Users can use the applications, but they might not work as expected if Dynamic Application Containment blocks certain actions. Once you determine that an application is safe, you can configure ATP or TIE server to allow it to run normally.

To use Dynamic Application Containment:

1. Enable ATP and specify the reputation threshold for triggering Dynamic Application Containment in the **Options** settings.
2. Configure Trellix-defined containment rules and exclusions in the **Dynamic Application Containment** settings.

Enable the trigger threshold for Dynamic Application Containment

With Dynamic Application Containment, you can specify that applications with specific reputations run in a container, limiting the actions they can perform. If the application reputation is at or below the containment reputation threshold, the application is contained.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Adaptive Threat Protection** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Verify that ATP is enabled.
5. Select **Trigger Dynamic Application Containment when reputation threshold reaches**.
6. Specify the reputation threshold at which to contain applications.
    - **Might Be Trusted**
    - **Unknown** (default for the **Security** rule group)
    - **Might Be Malicious** (default for the **Balanced** rule group)
    - **Most Likely Malicious** (default for the **Productivity** rule group)
    - **Known Malicious**

    The Dynamic Application Containment reputation threshold must be above the block and clean thresholds. For example, if the block threshold is set to **Known Malicious**, the Dynamic Application Containment threshold must be set to **Most Likely Malicious** or above.

7. Click **Save**.

Configure Trellix-defined containment rules

Trellix-defined containment rules block or log actions that contained applications perform. You can change the block and report settings, but you can't otherwise change or delete these rules.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Adaptive Threat Protection** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Dynamic Application Containment**.
3. Click the **Edit** link for an editable policy.
4. In the **Containment Rules** section, select **Block**, **Report**, or both for the rule.
    - To select or deselect all rules under **Block** or **Report**, click **Block All** or **Report All**.
    - To disable the rule, deselect both **Block** and **Report**.
5. In the **Exclusions** section, configure executables to exclude from Dynamic Application Containment.
   Processes in the **Exclusions** list run normally (not contained).
6. Click **Save**.

Trellix-defined Dynamic Application Containment rules

Trellix-defined containment rules control what changes contained applications can make to your system.

Note

You can change the block and report settings, but you can't otherwise change or delete these rules.

Dynamic Application Containment rules in the **Trellix Default** policy are set to report only to reduce false positives. Adaptive Threat Protection provides two additional predefined Dynamic Application Containment policies: **Trellix Default Balanced** and **Trellix Default Security**. These policies set recommended rules to block, based on the security profile.

Best practice: Evaluate the impact of the Dynamic Application Containment rules by using the **Trellix Default** policy with rules set to report. To determine whether to set rules to block, monitor the logs and reports. After collecting `Dynamic Application Containment violation allowed` (event ID 37280) events, set Enterprise Level Reputations or Dynamic Application Containment exclusions before enforcing the **Trellix Default Security** policy.

Dynamic Application Containment can exclude processes from containment based on name, MD5 hash, signature data, and path. If your organization signs tools that are deployed internally, add these signatures as exclusions to reduce false positives.

When Adaptive Threat Protection (ATP) is in Observe mode, Dynamic Application Containment reports `Would Contain`, `Would Block`, `Would Clean` and `Would Released` events (an application must meet containment requirements before ATP determines whether it would clean or block). Would Contain events on their own do not indicate a potential block. All Dynamic Application Contain rules are evaluated when in Observe mode and the rules are set to report only. Actions are not blocked in Observe

mode. To properly tune Dynamic Application Containment, after you disable Observe mode, modify containment rules to report but not block, and then set the rules to block as needed to match the default configuration.

Dynamic Application Containment rules have flood control, which limits the number of events generated to once per hour, per rule, and per process. Dynamic Application Containment flood control tracks processes by process ID (PID). When a process restarts, the operating system assigns it a new PID, which resets the flood control, even though the process name is the same. For example, if Process A violates rule A 100 times per hour, you receive 1 event per hour. If Process A restarts during that hour, flood control resets for Process A and you receive another event if it continues to violate rule A. If Process B violates the same rule A, you receive a second event (with Process B details).

Best practice: Run the Trellix GetClean tool on the deployment base images for your production systems to ensure that clean files are sent to Trellix GTI to be categorized. This tool helps to ensure that Trellix GTI doesn't provide an incorrect reputation value for your files.

Trellix-defined containment rule	**Description**	**Trellix Default Balanced recommended set to block**	**Trellix Default Security recommended set to block**
Accessing insecure password LM hashes	Protects the SAM file in %WINDIR%\system32\config. Windows stores passwords in this file. Programs generally don't access this file. **Best practice:** Set this rule to report only (default) to monitor for potentially malicious programs or unauthorized access attempts.		
Accessing user cookie locations	Protects the Internet Explorer cookies folder in %AppData%\Roaming and %AppData%\Local from change. **Best practice:** Set this rule to report only		

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	(default) to monitor access to Internet Explorer cookies by contained programs.		
Allocating memory in another process	Prevents contained processes from changing the memory in other processes on the system.	✓	✓
Changing users' data folders	Prevents contained processes from changing or executing files in the user's common data folders. Common data folders include the Desktop, Downloads, Documents, Pictures, and other locations in the AppData folder, which malware targets in ransomware attacks. This rule can result in false positives depending on whether the contained program is truly malicious or not. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Creating a thread in another process	Prevents contained processes from creating	✓	✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	or changing a thread in other processes on the system.		
Creating files on any network location	Prevents contained processes from creating files on network locations. Malware can use these locations to spread the infected files. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Creating files on CD, floppy, and removable drives	Prevents contained processes from creating files on removable devices. Malware can use these devices to propagate. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Creating files with the .bat extension	Prevents contained applications from creating any files with the .bat extension. If batch files are used for administrative purposes, this rule might produce false		✔

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	positives and impact business operations. **Best practice:** If batch files aren't used to administer the system, set this rule to block and report to prevent malware from creating scripts that scripting engines execute later.		
Creating files with the .exe extension	Prevents contained processes from creating any file with the .exe extension. This rule stops malware from creating executables on the system. The typical "false blocks" that can occur with this rule might include WinZip (if users update WinZip regularly) and some installers and uninstallers. **Best practice:** Run GetClean before setting this rule to block. You can further tune this rule by using Dynamic Application Containment global exclusions.		✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
Creating files with the .html, .jpg, or .bmp extension	Prevents contained processes from creating files with the .html, .jpg, or .bmp extension. Malware sometimes hijacks these extensions to trick the user into executing the payload. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Creating files with the .job extension	Prevents contained processes from scheduling tasks on the system. Malware actively exploits scheduled tasks to avoid behavioral scanners.	✓	✓
Creating files with the .vbs extension	Prevents contained processes from creating files with the .vbs (Visual Basic Script) extension. If .vbs files are used for administrative purposes, this rule might produce false positives and impact business operations. **Best practice:** If .vbsfiles aren't used		

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	to administer the system, set this rule to block and report to prevent malware from creating scripts that scripting engines execute later.		
Creating new CLSIDs, APPIDs, and TYPELIBs	Prevents contained processes from creating Class IDs, App IDs, or TypeLIBs. These registry locations can be used to register new file types and allow malware an entry point on the system. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Deleting files commonly targeted by ransomware-class malware	Prevents contained processes from deleting files that ransomware-class malware commonly targets. Ransomware sometimes tries to read the files into memory, write the file contents to a new file, encrypt it, and then delete the original. Ransomware-class malware does not	✓	✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	typically try to directly change the files it is targeting for encryption. Instead, it uses a process already on the system, such as explorer.exe or powershell.exe, to proxy the attack. If enough attempts are blocked, the malware might fall back to trying to encrypt the file directly.		
Disabling critical operating system executables	Prevents contained processes from disabling regedit or Task Manager and thus restricting administrator rights to these tools.	✓	✓
Executing any child process	Prevents contained processes from executing any child process on the system. **Best practice:** Run GetClean before setting this rule to block.		✓
Modifying appinit DLL registry entries	Prevents contained processes from adding entries to the appinit registry location. User-mode processes on the system can	✓	✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	load any entry in the appinit registry location. For this reason, malware can use these processes as an attack vector to insert its payload.		
Modifying application compatibility shims	Prevents contained processes from creating application compatibility shims. Malware can use this technique to gain the same rights of the target process and inject shellcode.	✓	✓
Modifying critical Windows files and registry locations	Prevents contained processes from changing critical files and registry locations such as the hosts file, WINLOGON registry location, session manager registry location, and others. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Modifying desktop background settings	Prevents contained processes from changing the settings for the		

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	desktop wallpaper or background. Malware can use this technique to trick the user, hide files, or make the user think that they are clicking something else. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Modifying file extension associations	Prevents contained processes hijacking file extension associations. Malware can use this technique to trick the user into executing unknown file types or using unknown programs to execute files.		✔
Modifying files with the .bat extension	Prevents contained processes from changing files with the .bat extension. Use this rule to help stop malware from infecting script files on the operating system. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
Modifying files with the .vbs extension	Prevents contained processes from changing files with the .vbs extension. Use this rule to help stop malware from infecting script files on the operating system. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Modifying Image File Execution Options registry entries	Prevents contained processes from changing Image File Execution Options in the registry. Malware can use this technique to hijack process execution and stop processes from executing altogether.	✓	✓
Modifying portable executable files	Prevents contained processes from changing any portable executable (PE) file on the system. PE files are files that Windows can execute natively, such as .exe, .dll, and .sys.		✓
Modifying screen saver settings	Prevents contained processes from changing screensaver	✓	✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	settings. Malware can use this technique to drop malicious payloads onto the system.		
Modifying startup registry locations	Prevents contained processes from creating or changing the Windows registry startup locations. Malware frequently hides payloads or proxies to payloads in the Windows registry startup locations.	✓	✓
Modifying the automatic debugger	Prevents contained processes from changing or adding the automatic debugger, which malware can use to hijack process execution and steal sensitive information.		
Modifying the hidden attribute bit	Prevents contained processes from changing the hidden bit in files on the system.	✓	✓
Modifying the read-only attribute bit	Prevents contained processes from changing the read-only bit in files on the system.	✓	✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
Modifying the Services registry location	Prevents contained processes from changing service behavior on the system.		✔
Modifying the Windows Firewall policy	Prevents contained processes from changing the Windows Firewall policies stored in the registry. Malware can use the Windows Firewall to open security holes on the system. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Modifying the Windows Tasks folder	Prevents contained processes from creating or changing tasks stored in the Tasks folders. Malware can use tasks to place its payload on the system. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Modifying user policies	Prevents contained processes from changing group policy settings directly.		✔

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	Malware can use this technique to change the security posture and open vulnerabilities in the system.		
Reading files commonly targeted by ransomware-class malware	Prevents contained processes from reading files that ransomware-class malware commonly targets. Ransomware sometimes tries to read the files into memory, write the file contents to a new file, encrypt it, and then delete the original. Ransomware-class malware does not typically try to directly change the files it is targeting for encryption. Instead, it uses a process already on the system, such as explorer.exe or powershell.exe, to proxy the attack. If enough attempts are blocked, the malware might fall back to trying to encrypt the file directly.		✓
Reading from another process's memory	Prevents contained processes from reading		✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	the memory from another process on the system. This rule can help thwart attempts to steal information contained in targeted processes.		
Reading or modifying files on any network location	Prevents contained processes from reading or changing files on network locations. Malware can use these locations to spread the infected files. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Reading or modifying files on CD, floppy, and removable drives	Prevents contained processes from reading or changing the contents of removable devices. Malware can use these devices to propagate. **Best practice:** During an outbreak, set this rule to block and report to help stop or slow the infection.		
Suspending a process	Prevents contained processes from suspending other	✓	✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	processes on the system. Some malware tries to suspend a process to hijack it or hollow it out for malicious purposes, also known as process hollowing.		
Terminating another process	Prevents contained processes from stopping processes on the system.	✓	✓
Writing to another process's memory	Prevents contained processes from writing to the memory space of another process on the system.	✓	✓
Writing to files commonly targeted by ransomware-class malware	Prevents contained processes from changing files that ransomware-class malware commonly targets. Ransomware sometimes tries to read the files into memory, write the file contents to a new file, encrypt it, and then delete the original. Ransomware-class malware does not typically try to directly change the files it is targeting for		✓

Trellix-defined containment rule	Description	Trellix Default Balanced recommended set to block	Trellix Default Security recommended set to block
	encryption. Instead, it uses a process already on the system, such as explorer.exe or powershell.exe, to proxy the attack. If enough attempts are blocked, the malware might fall back to trying to encrypt the file directly.		

Best practice: Tune Dynamic Application Containment

When you first enable Dynamic Application Containment in your environment, set the rules to **Report** only and evaluate the effects before enforcing them. Users experience no blocking or prompting.

Task

1. In the Common **Options** settings, **Event Logging** section, select **Warning, Critical, and Alert** from the **Adaptive Threat Protection events to log** drop-down list.
   This step is required to send Dynamic Application Containment Would Block events to Trellix ePO - On-prem.
2. Enforce the **Trellix Default** Dynamic Application Containment policy.
   This policy sets rules to **Report** only and generates "Dynamic Application Containment violation allowed" (event ID 37280) events.
3. Monitor the logs and reports and determine whether to set rules to block.
4. After collecting "Dynamic Application Containment violation allowed" (event ID 37280) events, set Enterprise Level Reputations or Dynamic Application Containment exclusions.
5. Enforce the **Trellix Default Balanced** Dynamic Application Containment policy.

View contained applications from Trellix ePO - On-prem

Trellix Agent sends the list of contained applications to Trellix ePO - On-prem in the client properties. You can use this list to exclude applications from Dynamic Application Containment.

Task

1. From the **System Tree**, select the system, then click **Wake Up Agents**.

   The agent wake-up call collects the client properties, including contained applications, from the client.

For information about the **Wake Up Agents** page, see the Trellix ePO - On-prem Help.

2. From the **System Tree**, click the system name.
3. Click **Products**, then click **Endpoint Security Adaptive Threat Protection**.
4. Scroll down to the **Dynamic Application Containment** section to view the applications contained on the client system.
5. Review the list for any trusted applications to exclude.

Prevent Dynamic Application Containment from containing trusted programs

If a trusted program is contained, you can allow it to run normally by creating a Dynamic Application Containment exclusion.

Exclusions created using the Trellix Endpoint Security (ENS) Client apply to the client system only. These exclusions aren't sent to Trellix ePO - On-prem and don't appear in the **Exclusions** section in the **Dynamic Application Containment** settings.

Create global exclusions in the **Dynamic Application Containment** settings in Trellix ePO - On-prem.

Trellix ENS treats all file and folder exclusions as case insensitive — all case variations of the specified locations are excluded. For example, if you exclude C:\Temp\ABC, Trellix ENS also excludes C:\temp\abc and C:\TEMP\Abc.

Task

1. Identify trusted applications to exclude: View the list of contained applications sent from managed systems to Trellix ePO - On-prem.
2. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Adaptive Threat Protection** from the **Products** list in the left pane.
3. From the **Category** list in the right pane, select **Dynamic Application Containment**.
4. Click the **Edit** link for an editable policy.
5. Click **Show Advanced**.
6. In the **Exclusions** section, click **Add** to add processes to exclude from all rules.
7. On the **Exclusion** page, configure the executable properties.
8. Click **Save** twice to save the policy settings.

Get the signer distinguished name from Trellix ePO - On-prem to use to exclude executables

The signer distinguished name (SDN) is required when you enable a digital signature check and exclude only files signed by a specified process signer.

Task

1. Select **Menu** → **Reporting** → **Threat Event Log**.
2. Click the Adaptive Threat Protection event (**Adaptive Threat Protection** prefix in the **Action Taken** field) to display details.
3. Select and copy the **Source Process Signer** details.
4. When creating exclusions, paste the **Source Process Signer** details as a single line of text to the **Signed by** field.

   For example, the SDN required format is:

   ```
   C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION
   ```

Allowing contained applications to run normally

Once you determine that a contained application is safe, you can allow it to run normally in your environment.

- Add the application to the global **Exclusions** list in the Dynamic Application Containment settings. In this case, the application is released from containment and runs normally, regardless of how many technologies have requested containment.
- Configure Adaptive Threat Protection to raise the reputation threshold and release it from containment. In this case, the application is released from containment and runs normally unless another technology has requested to contain the application.
- If TIE server is available, change the reputation of the file to a level that allows it to run, like **Known Trusted**. In this case, the application is released from containment and runs normally unless another technology has requested to contain the application. See the *Trellix Threat Intelligence Exchange (TIE) Product Guide.*

Configure Adaptive Threat Protection

Adaptive Threat Protection settings determine when a file or process is allowed to run, and if it is contained, cleaned, blocked, or the user is prompted. You can also use these settings to enable Real Protect, enhanced remediation, and enhanced script scanning with AMSI.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Adaptive Threat Protection** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. Configure settings on the page, then click **Save**.

Exclude processes from Adaptive Threat Protection scanning

ATP scanning uses exclusions defined in the Threat Prevention **On-Access Scan** settings for **Standard** process types.

If the TIE server is available, you can change the reputation of the file to a level that allows it to run, like **Known Trusted**, instead of creating exclusions.

Best practice: For suggestions on how to improve Trellix ENS performance, see KB88205.

On-access scan **Standard** process exclusions specified by file name or file path apply to all ATP scanners, including Dynamic Application Containment and Real Protect. On-access scan exclusions specified by file type or age don't apply to ATP. ATP supports the same wildcards in path-based exclusions as Threat Prevention does.

Trellix ENS treats all file and folder exclusions as case insensitive — all case variations of the specified locations are excluded. For example, if you exclude C:\Temp\ABC, Trellix ENS also excludes C:\temp\abc and C:\TEMP\Abc.

Best practice: For information about troubleshooting blocked third-party applications, see KB88482.

For a list of executables that ATP scanned, check the Adaptive Threat Protection debug log (AdaptiveThreatProtection_Debug.log) on the client system.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **On-Access Scan**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the **Process Types** section, select the **Standard** tab.

Note

Exclusions specified in the **High Risk** and **Low Risk** tabs don't apply to ATP.

6. In the **Exclusions** section, click **Add** to enter the process to exclude from ATP scanning.

   In the **When to exclude** section, select **On read**.

Tip

If you want to exclude items from ATP scanning only, select this option. Threat Prevention still scans those items when they are being written to or changed on the disk.

Wildcards in exclusions

You can use the ? and * wildcards to represent 1 or more characters when excluding files, folders, detection names, and potentially unwanted programs.You can use the ? and * wildcards to represent 1 or more characters when excluding files and folders from scanning.

Valid wildcards

Wildcard character	Name	Represents	Example
?	Question mark	Single character in the exact location in the file, folder, or path name. You can use a single ? character as the root of a file path. For example, ?:\ABC matches the root-level	W?? excludes WWW, but doesn't exclude WW or WWWW.

Wildcard character	Name	Represents	Example
		ABC folder for all drives.	
*	Asterisk	Multiple characters, except backslash (\). Doesn't cross folder boundaries. **Note:** *\ at the beginning of a file path is not valid. Use **\ instead. For example: **\ABC*.	C:\Users\Will* matches path names, such as C:\Users\William, C:\Users\Willamina, and C:\Users\WillAnderson, but not subfolders of those names.
**	Double asterisk	One or more of any characters, including backslash (\). Crosses folder boundaries.	C:\Users\Will** matches path names, such as C:\Users\William, C:\Users\Willamina, and C:\Users\WillAnderson and all their subfolders. C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ.
**\		One or more complete path components (including a single backslash), delimited by backslashes.	C:**\Favorites\ matches any folder named Favorites on drive C.

Wildcards can appear in front of a backslash (\) in a path. For example, C:\ABC*\XYZ matches C:\ABC\DEF\XYZ.

Wildcard examples

Example	Description
**\Temp\test.docx	Excludes a specific file in a folder named Temp anywhere on the system.
**\test.docx	Excludes a specific file anywhere on the system.
**\test.docx	Excludes a specific file in any folder on a specific drive.
Users**\Documents\Microsoft User Data\	Excludes any folder under Users and any folder under User Data, if you select **Also exclude subfolders**.
C:\Documents and Settings**\Favorites\	Excludes the Favorites folder for all users.
C:**\Favorites\	Excludes any folder named Favorites on the C: drive.
\Temp	Excludes the Temp folder in any location, on any drive, including: • C:\Temp • D:\Windows\temp • C:\Documents and Settings\Administrator\Local Settings\temp
**\Temp*.tmp	Excludes any file with a .tmp extension in a folder named Temp anywhere on the system.
***.html	Excludes any file with an .html extension anywhere on the system.
C:\Windows\Temp*\inifile?.*	Excludes all files named inifileX, where X is any valid character for a file name, in any folder name beginning with Temp under C:\Windows.

Example	Description
***.tmp	Excludes all files with the .tmp extension (*.tmp) in any folder on a specific drive.
D:***.tmp	Excludes any *.tmp files on the D: drive.

Environment variables in exclusions

In addition to wildcards, you can use system environment variables, such as %SystemRoot% in exclusions. Exclusions don't support user environment variables, such as %UserProfile%. The reason for this is that the on-access scanner runs under the Windows LocalSystem account and can only access the system environment variables.

Best practices: Improve performance during program compilation

Systems that are used by developers to compile programs can experience significant performance impact during compilation when Adaptive Threat Protection is running. You can mitigate this impact using exclusions and signed certificates.

Reasons for the impact on performance include:

- Compilers, such as Cygwin, git, and CMake, create many short-lived processes and execute them multiple times. Adaptive Threat Protection requests reputation data for the processes from the TIE server or Trellix GTI (depending on your configured reputation source), resulting in time spent waiting for the response to come back.
- Compilers might also create unsigned image files. The unsigned files trigger Adaptive Threat Protection scanning, which slows down the compilation.

We recommend using one of the following workarounds to improve performance during compilation.

Note

We don't recommend disabling Adaptive Threat Protection to improve performance.

Add exclusions for compilers

Exclusions are the most common solution used by organizations. Depending on the compiler being used, we recommend adding the following exclusions.

Note

The exclusion paths show compilers installed in the default location. Verify the actual compiler locations with the developers.

- **Exclusions for Cygwin**

```
C:\cygwin\bin\as.exe
C:\cygwin\bin\make.exe
C:\cygwin\bin\sh.exe
C:\cygwin\bin\gcc.exe
C:\cygwin\bin\gcc-4.exe
C:\cygwin\lib\gcc\i686-pc-cygwin\5.4.0\CC1.exe
```

- **Exclusions for git**

```
C:\PROGRAM FILES\GIT\USR\BIN\BASH.EXE
C:\PROGRAM FILES\GIT\USR\BIN\UNAME.EXE
C:\PROGRAM FILES\GIT\USR\BIN\SH.EXEC
C:\PROGRAM FILES\GIT\MINGW64\LIBEXEC\GIT-CORE\GIT.EXEC
C:\PROGRAM FILES\GIT\USR\BIN\SED.EXEC
C:\PROGRAM FILES\GIT\USR\BIN\BASENAME.EXE
```

- **Exclusion for CMake**

```
C:\PROGRAM FILES\CMAKE\BIN\CMAKE.EXE
```

Sign executables with a code-signing certificate

When an executable is ready to be released, you can sign it with a trusted code-signing certificate that is configured to be trusted throughout your organization. The code-signing certificate must be marked as trusted by the TIE server; all executables signed by this certificate are fully trusted.

Submit executables to Trellix GTI

When application is ready to be released, you can submit the unknown files to Trellix using GetClean. Once confirmed, Trellix GTI trusts the files.

Trellix sends an email to confirm the files were received and notifies when the executables are added to Trellix GTI . The normal turnaround time is between 2 and 48 hours.

For information on GetClean, see KB73044.

Exclude items from enhanced script scanning

If enhanced script scanning is blocking scripts that you want to allow to run, you can exclude them from scanning. These exclusions apply to both Threat Prevention and Adaptive Threat Protection.

The process for excluding items from scanning depends on the type of exclusion.

Exclusion type	Action	Where specified?
File-based exclusion	Excludes the file from scanning.	In the **Exclusions** section of the Threat Prevention **On-Access**

Exclusion type	Action	Where specified?
		Scan settings for **Standard** process types.
Buffer-hash exclusion	Excludes the buffer from scanning.	In the **Exclusion by Detection Name** section of the Threat Prevention **Options** settings.
Command-line suppression	Scans the command line, but doesn't enforce the action specified in the **Action Enforcement** section of the Adaptive Threat Protection **Options** settings. If detections occur, ATP generates `Would Block` or `Would Clean` events.	In the **Exclusion by Detection Name** section of the Threat Prevention **Options** settings.

Task

1. Select **Menu** → **Reporting** → **Threat Event Log**.
2. Click an event name to display its details in the **Threat Event Log Details** page.
   AMSI scanning events include `AMSIScan` in the **Task Name** column.
3. From the **Actions** menu, select an option.
   - **Add Buffer Exclusion**
   - **Add Command-Line Suppression**
4. At the prompt, select the policy where you want to add the exclusion.
   Trellix ePO - On-prem displays a message indicating the exclusion was added to the selected policy.
5. Verify that the exclusion appears in the Threat Prevention **Options** settings for the policy you selected.
   a. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
   b. From the **Category** list in the right pane, select **Options**.
   c. Click the **Edit** link for the policy that you added the exclusions to.
   d. Verify that the exclusions appear in the **Exclusion by Detection Name** list.
      - Buffer-hash exclusions include the prefix: `AMSI-B!`
      - Command-line suppressions include the prefix: `AMSI-CMD!`

Configure Adaptive Threat Protection with no connection to Trellix GTI

For systems with no network connection to Adaptive Threat Protection, such as air-gapped systems, you can improve performance by manually disabling Adaptive Threat Protection.

Disable Adaptive Threat Protection to eliminate unnecessary attempts to connect to Adaptive Threat Protection when no network path exists and reduce the impact on Trellix ENS performance.

⚠ Caution

Disabling Adaptive Threat Protection might result in increased false positives.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **On-Access Scan**.
3. Click the **Edit** link for an editable policy.
4. In the **Trellix GTI** section, deselect **Enable Trellix GTI**, then click **Save**.
5. In the **Policy Catalog**, select **Endpoint Security Adaptive Threat Protection** from the **Products** list in the left pane.
6. Click **Options**.
7. Click the **Edit** link for an editable policy.
8. Click **Show Advanced**.
9. In the **Reputation Source** section, click the drop-down list and select **Use only the TIE server**, then click **Save**.

Managing with Trellix ePO - On-prem

Managing common features

Keeping your protection up to date

You can get updated security files manually or automatically.

For example, you might want to update manually to apply an emergency fix to a new threat or include the latest content after a new installation.

Automatic updates

Automatic update methods include:

Default Client Update task

The task updates content only. By default, the **Default Client Update** task runs every day at 1:00 a.m. and repeats every four hours until 11:59 p.m.

Trellix Agent Product Update task

From Trellix ePO - On-prem, schedule when you want updates to occur at an interval, for example, every Saturday at 1 a.m.

Manual updates

Manual update methods include:

Update button

From the Trellix Endpoint Security (ENS) Client, immediately download the latest content or software, or both according to settings. You can configure the visibility and behavior of the **Update** button in the Common settings.

Update Security option

From the Trellix system tray icon, update content and software.

Command line

From the client system, run a command to update the AMCore content.

Check the content date and version

To provide the best protection, Trellix ENS needs the latest content files to be installed on the system.

Task

1. Select **Menu** → **Software** → **Main Repository**.

2. From the **Preset** drop-down list, select **DAT**.
3. Verify that the **Check-In Date** for **AMCore Content Package** matches today or yesterday's date.
4. Verify that the **Endpoint Security Exploit Prevention Content** date matches the latest content listed on the Trellix Exploit Prevention Security Content Releases page.
5. Select **Reporting** → **Dashboards** to check the content status for systems in your enterprise.

Dashboard	Reports
Endpoint Security: Content Status	Reports the versions of the content files and engine for AMCore Content and Exploit Prevention Content. Reports the versions of the content files and engine for AMCore Content.
Endpoint Security Compliance Status	Number of systems with AMCore content compliant — AMCore content creation date is less than 7 days old.

6. Check the content date and version for an individual system.
   a. Select **Menu** → **Systems** → **System Tree**, then select a system to display its details.
   b. Click a module and verify that the content date matches the content in the **Main Repository**.

Module	Field
Adaptive Threat Protection	**Real Protect content date**
Threat Prevention	**AMCore content date**
Threat Prevention	**Exploit Prevention content date**

Update content files with Trellix ePO - On-prem

To keep your protection up to date, you can configure Trellix ePO - On-prem to pull updates from the Trellix source site as they are available.

To make sure that client systems always have the latest content files, follow this process:

Task

1. Configure your management platform to pull the latest content files from Trellix.

   For information, see the Trellix ePO - On-prem or Trellix Agent documentation.

2. Replicate repository content to mirror sites in your network.

   For information, see the Trellix ePO - On-prem documentation.

3. Schedule automatic downloads of the latest content files and scan engine to the client systems.
   In the **Package types** section, select **AMCore Content Package** and **Exploit Prevention Content**.

   For information, see the Trellix ePO - On-prem documentation.

4. Deploy Extra.DAT files, when required. (Trellix ePO - On-prem)

Using repository lists for update sites

The repository list specifies information about repositories (update sites) that Trellix Agent uses to update Trellix products, including Engine and DAT files.

The repository list includes:

- Repository information and location
- Repository order preference
- Proxy server settings, where required
- Encrypted credentials required to access each repository

The Trellix Agent **Product Update** client task connects to the first enabled update site in the repository list. If this repository is unavailable, the task contacts the next site in the list until it connects successfully or reaches the end of the list.

If your network uses a proxy server, you can specify which proxy settings to use, the address of the proxy server, and whether to use authentication. Proxy information is stored in the repository list. The proxy settings that you configure apply to all repositories in the repository list.

The location of the repository list depends on your operating system:

Operating system	Repository list location
Microsoft Windows 10	C:\ProgramData\McAfee\Common Framework\SiteList.xml
Microsoft Windows 8.1	
Microsoft Windows 7	
Earlier versions	C:\Documents and Settings\All Users\Application Data\McAfee\Common Framework\SiteList.xml

How mirror tasks work

The mirror task replicates the update files from the first accessible repository, defined in the repository list, to a mirror site on your network.

The most common use of this task is to mirror the contents of the Trellix download site to a local server.

After you replicate the Trellix site that contains the update files, computers on your network can download the files from the mirror site. This approach enables you to update any computer on your network, whether or not it has Internet access. Using a replicated site is more efficient because your systems communicate with a server that is closer than a Trellix Internet site, economizing access and download time.

The software relies on a directory to update itself. Therefore, when mirroring a site, make sure to replicate the entire directory structure.

Submitting threat samples for analysis

If you find a potential threat that the scanner doesn't detect or a false positive, you can submit a sample of the threat to Trellix Labs.

Trellix Labs analyze the sample and considers it for inclusion, or exclusion, in the next content file update.

Access the Submit a Virus or Malware Sample website for information about submitting a sample to Trellix Labs.

You can also use the Trellix GetClean tool, which uses Trellix GTI to report on files that are unknown to Trellix Labs, or falsely classified. Using GetClean, you can submit samples or metadata to Trellix Labs for whitelisting by Trellix GTI .

Common additions to Trellix ePO - On-prem

The Common module extends your ability to secure your network with these features and enhancements.

Important

You must have appropriate permissions to access most features.

Trellix ePO - On-prem feature	Addition	Management platform
Client tasks	Client tasks that you can use to automate management and maintenance on client systems.	All

Trellix ePO - On-prem feature	Addition	Management platform
Dashboards	• Dashboards and monitors that you can use to keep watch on your environment.	• All
	• Custom dashboards	• Trellix ePO - On-prem
Events and responses	• Events for which you can configure automatic responses. • Event groups and event types that you can use to customize automatic responses.	All
Managed system properties	Properties that you can review in the **System Tree** or use to customize queries.	All
Permissions sets	**Endpoint Security Common** and **Endpoint Security Platform Query** permission category, available in all existing permission set.	Trellix ePO - On-prem
Policies	• **Options** policy category in the **Endpoint Security Common** product group.	• All
	• Custom policies	• Trellix ePO - On-prem
Queries and reports	• Default queries that you can use to run reports.	• All
	• Custom property groups based on managed system properties	• Trellix ePO - On-prem

Trellix ePO - On-prem feature	Addition	Management platform
	that you can use to build your own queries and reports.	

Permission sets and Common (Trellix ePO - On-prem)

Permission sets define rights for managed product functionality in Trellix ePO - On-prem.

Your managed product adds these permission controls to Trellix ePO - On-prem.

Permissions sets	Default permissions
Executive Reviewer **Endpoint Security Common** and **Endpoint Security Platform Query**	No permissions
Global Reviewer **Endpoint Security Common**	Views policy and task settings.
Global Reviewer **Endpoint Security Platform Query**	No permissions
Group Admin **Endpoint Security Common** and **Endpoint Security Platform Query**	No permissions
Group Reviewer **Endpoint Security Common** and **Endpoint Security Platform Query**	No permissions

This managed product grants **No Permissions** by default.

Permissions must be granted for users to access or use permission-controlled features.

Client tasks and Common

Automate management or maintenance on managed systems using client tasks.

Your managed product adds these client tasks to the **Client Task Catalog**. You can use client tasks as is, edit them, or create new ones.

Common default client tasks

Client task	Description
Unlock Client Interface	The Unlock Client Interface client task is created automatically when you use the **Endpoint Security: Locked Client Systems Due to Failed Password Attempts** query on the **Queries & Reports** page.

Common leverages the following default Trellix Agent client tasks.

Trellix Agent default client tasks

Client task	Description	Management platform
Product Deployment	Deploys Trellix products to client systems.	Trellix ePO - On-prem
Product Update	Updates content files, engines, and all Trellix products automatically.	All
Mirror Repositories	Replicates the updated content and engine files from the first accessible repository to a mirror site on your network. For information about using distributed repositories to keep your security software up to date, see the Trellix ePO - On-prem *Best Practices Guide*.	Trellix ePO - On-prem

For information about client tasks and the **Client Task Catalog**, see the Trellix ePO - On-prem documentation.

Managing Threat Prevention

Check the content date and version

To provide the best protection, Trellix ENS needs the latest content files to be installed on the system.

Task

1. Select **Menu** → **Software** → **Main Repository**.
2. From the **Preset** drop-down list, select **DAT**.
3. Verify that the **Check-In Date** for **AMCore Content Package** matches today or yesterday's date.
4. Verify that the **Endpoint Security Exploit Prevention Content** date matches the latest content listed on the Trellix Exploit Prevention Security Content Releases page.
5. Select **Reporting** → **Dashboards** to check the content status for systems in your enterprise.

Dashboard	Reports
Endpoint Security: Content Status	Reports the versions of the content files and engine for AMCore Content and Exploit Prevention Content. Reports the versions of the content files and engine for AMCore Content.
Endpoint Security Compliance Status	Number of systems with AMCore content compliant — AMCore content creation date is less than 7 days old.

6. Check the content date and version for an individual system.
   a. Select **Menu** → **Systems** → **System Tree**, then select a system to display its details.
   b. Click a module and verify that the content date matches the content in the **Main Repository**.

Module	Field
Adaptive Threat Protection	**Real Protect content date**
Threat Prevention	**AMCore content date**
Threat Prevention	**Exploit Prevention content date**

Update content files with Trellix ePO - On-prem

To keep your protection up to date, you can configure Trellix ePO - On-prem to pull updates from the Trellix source site as they are available.

To make sure that client systems always have the latest content files, follow this process:

Task

1. Configure your management platform to pull the latest content files from Trellix.

   For information, see the Trellix ePO - On-prem or Trellix Agent documentation.

2. Replicate repository content to mirror sites in your network.

   For information, see the Trellix ePO - On-prem documentation.

3. Schedule automatic downloads of the latest content files and scan engine to the client systems.
   In the **Package types** section, select **AMCore Content Package** and **Exploit Prevention Content**.

   For information, see the Trellix ePO - On-prem documentation.

4. Deploy Extra.DAT files, when required. (Trellix ePO - On-prem)

Content file update strategies

You can use distributed repositories to update the engine and content files efficiently on systems in your organization. Distributed repositories enable you to host security content locally throughout your network so that client systems can receive updates more quickly.

When planning a content file update strategy, consider the following:

- Number of clients
- Number of sites
- Number of systems at each remote site
- How remote sites access the Internet

Designate at least one system in your organization to retrieve updates from the Trellix download site. Once downloaded to your organization, replicate the updated files to distributed repositories throughout your organization. Then, use Trellix Agent **Product Update** client tasks to update client systems from the distributed repositories.

Product Update tasks enable you to:

- **Schedule network-wide content file rollouts.** Use a schedule to stagger content file updates or phase in updates to different parts of the network at convenient times and with minimal intervention.
- **Split duties for rollout administration.** Keep update traffic primarily internal and increase network bandwidth efficiency by using different servers or domain controllers, in different network regions or divisions. This strategy also reduces the potential for network security breaches.
- **Reduce updated content or engine file download waiting time.** Traffic on computers protected by Trellix increases dramatically on regular content file publishing dates and whenever new product versions are available. Avoiding the competition for network bandwidth enables you to deploy your new software with minimal interruptions.

Submitting threat samples for analysis

If you find a potential threat that the scanner doesn't detect or a false positive, you can submit a sample of the threat to Trellix Labs.

Trellix Labs analyze the sample and considers it for inclusion, or exclusion, in the next content file update.

Access the Submit a Virus or Malware Sample website for information about submitting a sample to Trellix Labs.

You can also use the Trellix GetClean tool, which uses Trellix GTI to report on files that are unknown to Trellix Labs, or falsely classified. Using GetClean, you can submit samples or metadata to Trellix Labs for whitelisting by Trellix GTI .

Handling new malware with Extra.DAT files

When new malware is discovered and extra detection is required, Trellix Labs releases an Extra.DAT file. Extra.DAT files contain information that Threat Prevention uses to handle the new malware.

Threat Prevention supports using only one Extra.DAT file at a time. In a situation where you need both a positive Extra.DAT file for Threat Prevention and a negative Extra.DAT for Adaptive Threat Protection, you can request a combined file from Trellix Labs.

Each Extra.DAT file has an expiration date built in. When the Extra.DAT file is loaded, this expiration date is compared against the build date of the AMCore content installed on the system. If the build date of the AMCore content is newer than the Extra.DAT expiration date, the Extra.DAT is considered expired. It is no longer loaded and used by the engine. During the next update, the Extra.DAT is removed from the system.

If the next update of AMCore content includes information in the Extra.DAT, the Extra.DAT is removed.

Trellix ENS stores Extra.DAT files in the c:\Program Files\Common Files\McAfee\Engine\content\avengine\extradat folder.

Download and deploy an Extra.DAT file to client systems from Trellix ePO - On-prem

In a major malware outbreak, you must load an Extra.DAT file to protect client systems until the next scheduled content update. You might need to load an Extra.DAT file on client systems to suppress detections that are considered false positives until the next scheduled content update.

Best practice: For information on how to create a report of which computers have an Extra.DAT file installed, see KB59410.

Task

1. Download the Extra.DAT file.
    a. Click the download link supplied by Trellix Labs, specify a location to save the Extra.DAT file, then click **Save**.
    b. If needed, unzip the EXTRA.ZIP file.
2. Select **Menu** → **Software** → **Main Repository**.
3. Select **Actions** → **Check in Packages**.
4. Select **Extra DAT (.DAT)**, browse to the location where you downloaded the file, then click **Open**.
5. Confirm your selection, then click **Next**.
   The **Main Repository** page displays the new content package in the **Name** column.

6. Replicate the Extra.DAT file to mirror sites, if applicable. Run a Trellix Agent **Mirror Repositories** client task.

   Best practice: When you finish using the Extra.DAT file, remove it from the **Main Repository** and run a **Mirror Repositories** client task to remove it from distributed repositories. Removing the Extra.DAT file prevents clients from downloading it during an update. By default, detection for the new threat in the Extra.DAT file is ignored once the new detection definition is added to the daily content files.

7. Deploy the Extra.DAT file to client systems using a Trellix Agent **Product Update** client task.
8. Send an agent wake-up call to update the client systems with the Extra.DAT file.

Remove AMCore content on the client system from Trellix ePO - On-prem

Configure **Roll Back AMCore Content** client tasks from the **Client Task Catalog**, then assign them to systems in the **System Tree**.

Trellix ENS stores the currently loaded content file and the previous two versions in the Program Files\Common Files\McAfee\Engine\content folder. If needed, you can revert to a previous version.

Note

Exploit Prevention content updates cannot be rolled back.

Task

1. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
2. From **Client Task Types**, select **Endpoint Security Threat Prevention** → **Remove AMCore Content**.
3. Click the name of an existing client task or click **New Task**.
4. Make sure that **Roll Back AMCore Content** is selected, then click **OK**.
5. Configure the settings and click **Save**.
6. Under **Actions**, click the **Assign** link, specify the computers to assign the task to, then click **OK**.
7. Click **2 Schedule** to schedule the task, then click **Save**.

   See Trellix ePO - On-prem Help for schedule information and the **Client Task Assignment Builder**.

Responding to detections

Responding to access point violations

When a system access point is violated, the action depends on how the rule is configured.

If the rule was configured to:

- **Report** — Information is recorded in the log file.
- **Block** — Access is denied.

Take these steps:

1. Review the log file to determine which system access points were violated and which rules detected the violations.

2. Configure the **Access Protection** rules to allow users access to legitimate items and prevent users from accessing protected items.

Use these scenarios to decide which action to take as a response.

Detection type	Scenarios
Unwanted processes	• If the rule reported the violation in the log file, but didn't block the violation, select **Block** for the rule. • If the rule blocked the violation, but didn't report the violation in the log file, select **Report** for the rule. • If the rule blocked the violation and reported it in the log file, no action is necessary. • If you find an unwanted process that wasn't detected, edit the rule to include it as blocked.
Legitimate processes	• If the rule reported the violation in the log file, but didn't block the violation, deselect **Report** for the rule. • If the rule blocked the violation and reported it in the log file, edit the rule to exclude the legitimate process from being blocked.

Responding to Exploit Prevention detections

When Exploit Prevention detects security violations, as defined by signatures or rules, it triggers events and sends them to the Trellix ePO - On-prem server.

Exploit Prevention Events page

Trellix ePO - On-prem displays buffer overflow and illegal API use events in the **Exploit Prevention Events** page under **Reporting**.

Review the list of events to determine which events are allowable and which indicate suspicious behavior. Under certain circumstances, behavior that is interpreted as an attack can be a normal part of a user's work routine. When this occurs, you can create an exclusion for that behavior. Creating exclusions allows you to reduce false positive alerts, and helps ensure that the notifications you receive are meaningful.

In the **Exploit Prevention Events** page, you can:

- Use filters to reduce the list to only those events that satisfy the filter criteria.
- Aggregate events to generate a list of events grouped by the value associated with selected criteria.

- Create exclusions from events.

Threat Event Log page

All Exploit Prevention events, including Network IPS events, appear in the **Threat Event Log** under **Reporting** with the events for all products managed by Trellix ePO - On-prem.

Filter the Exploit Prevention Events list

Use filters to reduce the list of Exploit Prevention events to only those events that satisfy the filter criteria.

Task

1. Select **Menu** → **Reporting** → **Exploit Prevention Events**.
2. Specify the systems to view events for.
    a. In the **System Tree**, select the group to show events for.
    All Exploit Prevention events associated with the group appear.
    b. From the **Preset** drop-down list, select to show events for the selected group only or for the selected group and all subgroups.
3. Filter the list.

To...	Follow these steps
Apply a previously defined custom filter.	From the **Custom** drop-down list, select an existing custom filter. To remove the filter, select **None** from the drop-down list.
Create a filter.	From the **Custom** drop-down list, click **Add**, then select properties and values.
Filter the list by text.	Enter the text in the **Quick find** field, then click **Apply** to show only events that match. To remove the filter, click **Clear**.
Show only rows that you have selected.	Click **Show selected rows**.

Aggregate Exploit Prevention events

Aggregating events generates a list of events grouped and consolidated by the selected criteria. You can then create exclusions using the information from specific events.

Task

1. Select **Menu** → **Reporting** → **Exploit Prevention Events**.

2. In the **System Tree**, select the groups to show events for.
3. If needed, select **Actions** → **Choose Columns**, then add or remove columns from the display.
   The displayed columns determine the criteria that you can aggregate events on. By default, the **Exploit Prevention Events** page displays these columns from the **Exploit Prevention Events** queries and reports data:

API Name	**Action Taken**
Analyzer Rule ID (also known as the Signature ID)	**Detecting Product Host Name**
Target Hash	**Target Signer**
Threat Name	**Threat Target File Path**

   The columns that you select are associated with your user ID and persist when you log off from Trellix ePO - On-prem. To remove custom columns, click **Use Default** on the **Select Columns to Display** page.

4. Click **Aggregate**, select the columns to aggregate events on, then click **OK**.
   The aggregated view consolidates the events by the selected criteria (columns) and lists the number of events for each.

   For example, to aggregate events by signer, select the **Target Signer** column. The aggregation shows the number of events associated with each signer. You can then use this information to create exclusions for files from a specific trusted signer.

   Note

   Exploit Prevention aggregates on the full list of rows, even if you filtered the events before aggregating.

5. Click a row to display the events that match the criteria.
   From this page, you can select events to create exclusions for.

   Click **Close** to return to the aggregated events view.

6. Click **Clear** to remove aggregation settings.
   The previous list of Exploit Prevention events appears.

Create exclusions from Exploit Prevention events

From the **Exploit Prevention Events** page, you can create exclusions to allow particular actions and prevent events from being generated.

Note

Exclusions created in this way don't include the **Caller Module** information. If you need that information for creating more granular exclusions, add **Caller Module** information manually to the exclusion.

Task

1. Select **Menu** → **Reporting** → **Exploit Prevention Events**.
2. If needed, filter the list or aggregate events.
   If you aggregate events, click a row to display the events that match the criteria. Otherwise, select the events to create an exclusion for.

   You can select multiple events to create exclusions from. Exploit Prevention skips any repeated events.

3. Select **Actions** → **Add Exclusion**.
4. In the dialog box, select a destination **Exploit Prevention** policy and click **OK**.
   Exclusions are created and added automatically to the **Exclusions** list in the destination **Exploit Prevention** policy. Exploit Prevention creates only unique exclusions in the policy.

Responding to unwanted program detections

When the on-access or on-demand scanner detects an unwanted program, it responds with the action that you configured for that scanner.

The on-access and on-demand scanners use potentially unwanted programs settings and AMCore content files to detect unwanted programs.

Review the information in the log file, then decide whether to take any of these additional actions:

- Fine-tune scanning items to make your scans more efficient.
- Exclude the program from detection. If a legitimate program was detected (false positive), configure it as an exclusion.
- Add the unwanted program to the user-defined detection list. If an unwanted program wasn't detected (false negative), add it to the user-defined detection list in the **Options** settings.
- Submit a sample to Trellix Labs for analysis. If you find a false positive or a false negative, submit a sample of the threat to Trellix Labs.

Responding to on-access scan detections

When the on-access or on-demand scanner detects an unwanted program, it responds with the action that you configured for that scanner.

Review the information in the activity log to decide whether to take more actions:

- Fine-tune scan items. To make scanning more efficient, exclude legitimate files and delete known threats from the quarantine.
- Configure the scanner to perform actions on files.
  - **Deny access to files** — Prevents the user from accessing files with detected threats.
  - **Clean files** — Removes the threat from the detected file, if possible.

    - **Delete files** — Deletes the item that contains the threat.

  If an action isn't available for the current detection, the corresponding option isn't available. For example, **Clean** isn't available if the file has already been deleted, or **Delete** isn't available if the settings don't allow it.
- Configure the scanner to display a message to users when a threat is detected.
- Submit a sample to Trellix Labs for analysis. If you find a false positive or a false negative, submit a sample of the threat to Trellix Labs.

Responding to on-demand scan detections

When the on-demand scanner detects a threat, it responds based on the type of on-demand scan. For custom on-demand scans, the scanner uses **Custom On-Demand Scan** client task settings. For policy-based on-demand scans, the scanner uses **On-Demand Scan** policy settings.

Review the information in the log file to decide whether to take more actions:

- Fine-tune items to scan. To make scanning more efficient, exclude legitimate files and delete known threats from the quarantine.
- Configure the scanner to prompt for action.
- Configure the scanner to perform actions on files.
    - **Continue scanning** — Continues scanning when a threat is detected.
    - **Clean files** — Removes the threat from the detected file, if possible.
    - **Delete** — Deletes the item that contains the threat.

  If an action isn't available for the current detection, the corresponding option isn't available. For example, **Clean** isn't available if the file has already been deleted, or **Delete** isn't available if the settings don't allow it.
- Submit a sample to Trellix Labs for analysis. If you find a false positive or a false negative, submit a sample of the threat to Trellix Labs.

Quarantined items

Specify quarantine location and retention time

You can configure the location of the quarantine folder and how long to keep quarantined items.

Quarantined items can include various types of scanned objects, such as files, registries, or anything that Trellix ENS scans for malware. Threat Prevention cleans or deletes items that are detected as threats and saves copies in a non-executable format to the Quarantine folder. You can delete quarantined items, restore or rescan them, or get more information about the threat. For example, you might be able to restore an item after downloading a later version of the content that contains information that cleans the threat.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Options**.
3. Click the **Edit** link for an editable policy.

4. Configure settings on the page, then click **Save**.

Restore quarantined items from Trellix ePO - On-prem

If Threat Prevention quarantines a trusted file on a client system, you can restore it from Trellix ePO - On-prem.

Task

1. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
2. From **Client Task Types**, select **Endpoint Security Threat Prevention** → **Restore from Quarantine**.
3. Click the name of an existing client task or click **New Task**.
4. Configure the settings and click **Save**.
5. Under **Actions**, click the **Assign** link, specify the computers to assign the task to, then click **OK**.
6. Click **Schedule** to schedule the task, then click **Save**.

   See Trellix ePO - On-prem Help for schedule information and the **Client Task Assignment Builder**.

Enabling activity logging for on-demand scan

Enable activity logging for on-demand scan to track all the files scanned by the on-demand scan task.

When activity logging for on-demand scan is enabled, you can track the list of scanned files, timed-out files, and files having errors. If the on-demand scan task is interrupted or stopped before completion, the log file will contain all file details till the on-demand scan is stopped. The log files are available in .zip format at `/var/McAfee/ens/log/tp/odsreport/archive/`

For managed systems, you can configure this feature using the **Endpoint security common** policy extension.

For standalone systems, configure activity logging using the command line.

Configure on-demand scanning activity logging for managed systems

Follow these steps to enable activity logging for on-demand scan in a managed systems.

Task

1. Log on to Trellix ePO - On-prem as an administrator.
2. Go to **Menu** > **Policy Catalog** > **Endpoint Security Common**.
3. In the **Endpoint Security Common** page, click **Policy Category** > **Options** > **My Default**.
   Click **Show Advanced** on the top left corner of the page.
4. In the **Client Logging** section, enable these options:
   - **Enable activity logging**.
   - Enable log for all scanned files during on-demand scans.
   - **Enable Limit size** (MB) of each of the activity log files and set the log size as 20MB.
5. Navigate to **System Tree**, and click on the **Assigned Policies** tab and in the **Product** section, select **Endpoint Security Common**.
6. Select **Endpoint Security Common** from the Product list, then click **Edit Assignment**.

   In the next page, click **Break inheritance and assign the policy** > **My Default** > **Assigned Policy** and select the **Save** option.

7. In the **System Tree** page, select the system to assign the policy. Click **Wake Up Agents**, and select **Force complete policy and task update** and select **OK**.
   Endpoint Security Common Policy by default gets enforced on the selected system.

View on-demand scan activity logging status on managed systems

Follow these steps to verify on-demand scan for activity logging on managed systems.

Task

1. Log on to managed systems as an administrator.
2. Navigate to the directory:
   `/opt/McAfee/ens/tp/bin/`
3. Verify the Activity logging for on-demand scan is enabled:
   `/opt/McAfee/ens/tp/bin/mfetpcli`
4. Execute on-demand scan task from Linux client:
   `/mfetpcli --runtask --name quick scan`
5. Verify the completion of on-demand scan task:
   `/mfetpcli --listtasks`
6. Verify on-demand scan activity report:
   `/var/McAfee/ens/log/tp/odsreport/quick\ scan-<timestamp>.zip`

Configure on-demand scanning activity logging for standalone systems

Follow these steps to enable on-demand scan for activity logging for standalone systems.

Task

1. Log on to the system as a user with administrative rights.
2. Navigate to the directory:
   `/opt/McAfee/ens/tp/bin/`
3. Run the command:
   - To enable on-demand scanning task for activity logging:

   `/opt/McAfee/ens/tp/bin/mfetpcli --odsactivitylog enable`

   - To confirm the enabled settings:

   `/opt/McAfee/ens/tp/bin/mfetpcli -showlogsettings`

Disable on-demand scan activity logging

Follow these steps to disable on-demand scan activity logging for standalone systems.

Task

1. Log on to the system as a user with administrative rights.
2. Navigate to the directory:
   `/opt/McAfee/ens/tp/bin/`
3. To disable the on-demand scan activity logging:

```
/opt/McAfee/ens/tp/bin/mfetpcli --odsactivitylog disable
```

Set the required product log size

Use this command to set the product log size.

Task

1. Log on to the system as a user with administrative rights.
2. Navigate to the directory:
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run these commands to set the product log size to 20 MB:
   ```
   /opt/McAfee/ens/tp/bin/mfetpcli --setmaxproductlogsize 20
   ```

Analyzing your protection

Analyzing your system protection is an ongoing process to improve protection and performance of your system.

Analyzing your protection enables you to determine:

- Which threats you are facing
- What malware was used in the attack
- Where the threats are coming from
- Where and when the attacks occurred
- How often threats are found
- Which systems are being targeted For example, if one system is being continuously attacked, you might move that system to a more secure part of your network and enable increased security.
- How the attack affected the system

Protection analysis is also helpful to:

- Create reports for IT and managers.
- Capture information used to create scripts and queries.
- Monitor network access time and Threat Prevention update network usage.

Dashboards and queries

Use dashboards to view information about your environment, including names and number of threats and how infection spreads through the environment. Use queries to determine where and when the attacks occurred.

For information, see the Trellix ePO - On-prem Help.

Threat Event Log

Use the **Threat Event Log** to determine which malware was used in the attack.

- **Threat Name** and **Threat Type** describe what malware was used in the attack.
- **Event Description** describes how the attack affected the system and which actions were taken on the threat.
- **Threat Source IP Address** and **Threat Target IP Address** can help you determine which actions to take.

For information, see the Trellix ePO - On-prem Help.

Managing Adaptive Threat Protection

Check the content date and version

To provide the best protection, Trellix ENS needs the latest content files to be installed on the system.

Task

1. Select **Menu** → **Software** → **Main Repository**.
2. From the **Preset** drop-down list, select **DAT**.
3. Verify that the **Check-In Date** for **AMCore Content Package** matches today or yesterday's date.
4. Verify that the **Endpoint Security Exploit Prevention Content** date matches the latest content listed on the Trellix Exploit Prevention Security Content Releases page.
5. Select **Reporting** → **Dashboards** to check the content status for systems in your enterprise.

Dashboard	Reports
Endpoint Security: Content Status	Reports the versions of the content files and engine for AMCore Content and Exploit Prevention Content. Reports the versions of the content files and engine for AMCore Content.
Endpoint Security Compliance Status	Number of systems with AMCore content compliant — AMCore content creation date is less than 7 days old.

6. Check the content date and version for an individual system.
   a. Select **Menu** → **Systems** → **System Tree**, then select a system to display its details.
   b. Click a module and verify that the content date matches the content in the **Main Repository**.

Module	Field
Adaptive Threat Protection	**Real Protect content date**
Threat Prevention	**AMCore content date**
Threat Prevention	**Exploit Prevention content date**

Update content files with Trellix ePO - On-prem

To keep your protection up to date, you can configure Trellix ePO - On-prem to pull updates from the Trellix source site as they are available.

To make sure that client systems always have the latest content files, follow this process:

Task

1. Configure your management platform to pull the latest content files from Trellix.

   For information, see the Trellix ePO - On-prem or Trellix Agent documentation.

2. Replicate repository content to mirror sites in your network.

   For information, see the Trellix ePO - On-prem documentation.

3. Schedule automatic downloads of the latest content files and scan engine to the client systems.
   In the **Package types** section, select **AMCore Content Package** and **Exploit Prevention Content**.

   For information, see the Trellix ePO - On-prem documentation.

4. Deploy Extra.DAT files, when required. (Trellix ePO - On-prem)

Content file update strategies

You can use distributed repositories to update the engine and content files efficiently on systems in your organization. Distributed repositories enable you to host security content locally throughout your network so that client systems can receive updates more quickly.

When planning a content file update strategy, consider the following:

- Number of clients
- Number of sites
- Number of systems at each remote site
- How remote sites access the Internet

Designate at least one system in your organization to retrieve updates from the Trellix download site. Once downloaded to your organization, replicate the updated files to distributed repositories throughout your organization. Then, use Trellix Agent **Product Update** client tasks to update client systems from the distributed repositories.

Product Update tasks enable you to:

- **Schedule network-wide content file rollouts.** Use a schedule to stagger content file updates or phase in updates to different parts of the network at convenient times and with minimal intervention.
- **Split duties for rollout administration.** Keep update traffic primarily internal and increase network bandwidth efficiency by using different servers or domain controllers, in different network regions or divisions. This strategy also reduces the potential for network security breaches.

- **Reduce updated content or engine file download waiting time.** Traffic on computers protected by Trellix increases dramatically on regular content file publishing dates and whenever new product versions are available. Avoiding the competition for network bandwidth enables you to deploy your new software with minimal interruptions.

Submitting threat samples for analysis

If you find a potential threat that the scanner doesn't detect or a false positive, you can submit a sample of the threat to Trellix Labs.

Trellix Labs analyze the sample and considers it for inclusion, or exclusion, in the next content file update.

Access the Submit a Virus or Malware Sample website for information about submitting a sample to Trellix Labs.

You can also use the Trellix GetClean tool, which uses Trellix GTI to report on files that are unknown to Trellix Labs, or falsely classified. Using GetClean, you can submit samples or metadata to Trellix Labs for whitelisting by Trellix GTI .

Handling new false positives with Extra.DAT files

If Adaptive Threat Protection determines that a detection is a false positive, Trellix Labs might release a negative Extra.DAT file to suppress the detection until the next content update.

Deploying a negative Extra.DAT is optional. If the TIE server is present, you can change the reputation score to eliminate the false positive. For information, see KB82922.

ATP supports using only one Extra.DAT file at a time. In a situation where you need both a negative Extra.DAT file and a positive Extra.DAT file for Threat Prevention, you can request a combined file from Trellix Labs.

Each Extra.DAT file has an expiration date built in. When the Extra.DAT file is loaded, this expiration date is compared against the build date of the AMCore content installed on the system. If the build date of the AMCore content is newer than the Extra.DAT expiration date, the Extra.DAT is considered expired. It is no longer loaded and used by the engine. During the next update, the Extra.DAT is removed from the system.

If the next update of AMCore content includes information in the Extra.DAT, the Extra.DAT is removed.

Trellix ENS stores Extra.DAT files in the c:\Program Files\Common Files\McAfee\Engine\content\avengine\extradat folder.

Download and deploy an Extra.DAT file to client systems from Trellix ePO - On-prem

In a major malware outbreak, you must load an Extra.DAT file to protect client systems until the next scheduled content update. You might need to load an Extra.DAT file on client systems to suppress detections that are considered false positives until the next scheduled content update.

Best practice: For information on how to create a report of which computers have an Extra.DAT file installed, see KB59410.

Task

1. Download the Extra.DAT file.
    a. Click the download link supplied by Trellix Labs, specify a location to save the Extra.DAT file, then click **Save**.

b. If needed, unzip the EXTRA.ZIP file.

2. Select **Menu** → **Software** → **Main Repository**.
3. Select **Actions** → **Check in Packages**.
4. Select **Extra DAT (.DAT)**, browse to the location where you downloaded the file, then click **Open**.
5. Confirm your selection, then click **Next**.
   The **Main Repository** page displays the new content package in the **Name** column.
6. Replicate the Extra.DAT file to mirror sites, if applicable. Run a Trellix Agent **Mirror Repositories** client task.

   Best practice: When you finish using the Extra.DAT file, remove it from the **Main Repository** and run a **Mirror Repositories** client task to remove it from distributed repositories. Removing the Extra.DAT file prevents clients from downloading it during an update. By default, detection for the new threat in the Extra.DAT file is ignored once the new detection definition is added to the daily content files.

7. Deploy the Extra.DAT file to client systems using a Trellix Agent **Product Update** client task.
8. Send an agent wake-up call to update the client systems with the Extra.DAT file.

Restore quarantined objects from Trellix ePO - On-prem

Restoring objects from the quarantine replaces all objects that the convicted processes created, changed, or deleted, and the files associated with those processes, on the system where they were before the **Clean** action occurred.

Task

1. Select **Menu** → **Client Tasks** → **Client Task Catalog**.
2. From **Client Task Types**, select **Endpoint Security Threat Prevention** → **Restore from Quarantine**.
3. Click the name of an existing client task or click **New Task**.
4. Configure the settings and click **Save**.
5. Under **Actions**, click the **Assign** link, specify the computers to assign the task to, then click **OK**.
6. Click **Schedule** to schedule the task, then click **Save**.

   See Trellix ePO - On-prem Help for schedule information and the **Client Task Assignment Builder**.

7. After restoring a Windows service, reboot the client system to complete the restore.

Monitoring activity in your environment

Monitoring your protection

Dashboards, monitors, and Common

Keep watch on the status of your managed systems and any threats in your environment using your customizable dashboard.

Dashboards are collections of monitors that track activity in your Trellix ePO - On-prem environment.

Default dashboards and monitors

The Common module provides several dashboards that include monitors from other modules.

Common dashboards

Dashboard	Monitor	Description	Installed by module
Endpoint Security: Compliance Status		Whether the enabled state in the policy matches the enabled state on the client system. If the technology is enabled in policy and disabled on the client, the system is noncompliant.	Common
	Endpoint Security: Policy Compliance by Policy Name	Policies that are up to date, including the number of systems.	Common
	Endpoint Security Common: Self Protection Compliance Status	Number of systems with Self Protection compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy	Common

Dashboard	Monitor	Description	Installed by module
		doesn't match the enabled state on client system	
	Endpoint Security: Policy Compliance by Computer Name	Systems where the policies are up to date, including the number of policies.	Common
	Endpoint Security Threat Prevention: Access Protection Compliance Status	Number of systems with Access Protection compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system	Threat Prevention
	Endpoint Security Threat Prevention: AMCore Content Compliance Status	Number of systems with AMCore content compliant or noncompliant: • **Compliant** — The AMCore content creation date is less than 7 days old. • **Non-Compliant** — The AMCore content creation date is more than 7 days old.	Threat Prevention
	Endpoint Security Threat Prevention:	Number of systems with Exploit Prevention	Threat Prevention

Dashboard	Monitor	Description	Installed by module
	Exploit Prevention Compliance Status	compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system	
	Endpoint Security Threat Prevention: On-Access Scan Compliance Status	Number of systems with on-access scanner protection compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system	Threat Prevention
	Endpoint Security Firewall: Compliance Status	Number of systems with Firewall compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system	Firewall

Dashboard	Monitor	Description	Installed by module
	Endpoint Security Web Control: Compliance Status	Number of systems with Web Control compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system	Web Control
Endpoint Security: Detection Status		Threats detected for the previous 24 hours and 7 days.	Common
	Endpoint Security: Threats Detected in the Last 24 Hours	Number of threat events in the last 24 hours, including the time of detection.	Common
	Endpoint Security: Threats Detected in the Last 7 Days	Number of threat events in the last 7 days, including the time of detection.	Common
	Endpoint Security: Summary of Threats Detected in the Last 24 Hours	Names of threats detected in the last 24 hours, including the number of threat events.	Common
	Endpoint Security: Summary of Threats Detected in the Last 7 Days	Names of threats detected in the last 7 days, including the	Common

Dashboard	Monitor	Description	Installed by module
		number of threat events.	
Endpoint Security: Environmental Health		Protection status of deployed Trellix ENS modules.	Common
	Endpoint Security: Currently Enabled Technology	Number of systems that have a module or feature enabled, including the number of systems and percentage. For each technology, this monitor shows: • System name • Last communicated time	Common
Endpoint Security: Installation Status		Whether a module is installed.	Common
	Endpoint Security: Installation Status Report	Number of systems with Trellix ENS deployed, by module, including version details.	Common
	Endpoint Security Platform: Hotfixes Installed	Number of systems with hotfixes installed, by module, including hotfix version numbers.	Common
	Endpoint Security Threat Prevention: Hotfixes Installed	Number of systems with Threat Prevention hotfixes installed, including hotfix version numbers.	Threat Prevention

Dashboard	Monitor	Description	Installed by module
	Endpoint Security Firewall: Hotfixes Installed	Number of systems with Firewall hotfixes installed, including hotfix version numbers.	Firewall
	Endpoint Security Web Control: Hotfixes Installed	Number of systems with Web Control hotfixes installed, including hotfix version numbers.	Web Control
Endpoint Security: Threat Behavior		Threat activity and the spread of infection in the environment.	Common
	Endpoint Security: Top Threats in the Last 48 Hours	Top 5 virus threats by number of events detected in the last 48 hours, including the total number of events and total number of infected users and systems. For each threat incident, this monitor shows: • Event generated time • Duration before detection • Event description • Threat type • Threat target user name • System name • Technology Name • Action taken	Common
	Endpoint Security: Duration before	How long a particular threat was on the	Common

Dashboard	Monitor	Description	Installed by module
	Detection on Endpoints in the Last 2 Weeks	system before being detected, including: • Number of events • Number of infected users • Number of infected systems For each duration, this monitor shows: • Date and time • Time duration before detection • Threat name, severity, and impact • Infected system name, user name, technology name, and product name	
	Endpoint Security: Top 10 Attacking Systems in the Last 7 Days	Top 10 systems that are infecting other systems (system name, IP address, and MAC address) and number of threat events per system.	Common
Endpoint Security: Threat Event Origins		How threats are entering the environment.	Common
	Endpoint Security: Primary Vectors of Attack in the Last 7 Days	Primary vectors of attack, such as web or instant message, and includes: • Number of events • Vector percent	Common

Dashboard	Monitor	Description	Installed by module
		• Total number of infected users For each vector, this monitor shows: • Date and time • Event description and category • Threat type and name • Infected user name	
	Endpoint Security: Top Infected Users in the Last 7 Days	Top 10 infected users, including the number and percentage of threat events per user.	Common
	Endpoint Security Threat Prevention: Applications with the Most Exploits in the Last 7 Days	Applications with the most buffer overflow exploits, including the number of detections.	Threat Prevention
	Endpoint Security Web Control: Web Content Categories that Caused the Most Infections in the Last 7 Days	Top 10 categories of websites that cause the most infections in the environment.	Web Control

Custom dashboards (Trellix ePO - On-prem)

Depending on your permissions, you can create custom dashboards and add monitors using default Trellix ENS queries.

For information about dashboards, see the Trellix ePO - On-prem documentation.

Queries, reports, and Common

Use queries to retrieve detailed information about the status of your managed systems and any threats in your environment. You can export, download, or combine queries into reports, and use queries as dashboard monitors.

Queries are questions that you ask Trellix ePO - On-prem, which returns answers as charts and tables. Reports enable you to package one or more queries into a single PDF document, for access outside of Trellix ePO - On-prem.

Similar information is available by accessing activity logs from the Trellix Endpoint Security (ENS) Client on individual systems.

You can view query data only for resources where you have permissions. For example, if your permissions grant access to a specific **System Tree** location, your queries return data only for that location.

Default queries

The module adds default queries to **McAfee Groups**. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the Trellix ePO - On-prem database.

- **Endpoint Security: Client Interface Logon Audit Log**
- **Endpoint Security: Currently Enabled Technology**
- **Endpoint Security: Duration before Detection on Endpoints in the Last 2 Weeks**
- **Endpoint Security: Installation Status Report**
- **Endpoint Security: Locked Client Systems Due to Failed Password Attempts**
- **Endpoint Security Platform: Hotfixes installed**
- **Endpoint Security: Policy Compliance by Computer Name**
- **Endpoint Security: Policy Compliance by Policy Name**
- **Endpoint Security: Primary Vectors of Attack in the last 7 Days**
- **Endpoint Security: Self Protection Compliance Status**
- **Endpoint Security: Summary of Threats Detected in the last 7 Days**
- **Endpoint Security: Threats Detected in the last 24 Hours**
- **Endpoint Security: Threats Detected in the last 7 Days**
- **Endpoint Security: Top 10 Attacking Systems in the Last 7 Days**
- **Endpoint Security: Top Infected Users in the last 7 Days**
- **Endpoint Security: Top Threats in the Last 48 Hours**

Custom queries (Trellix ePO - On-prem)

The module adds default properties to the **Endpoint Security** feature group. You can use these properties to create custom queries.

Feature Group	Result Type	Property (Column)	Property (Column)
Endpoint Security	Endpoint Security Platform Systems	Access Protection Debug Logging Enabled	License Status
		Access Protection Events Filter Level	Trellix GTI Proxy Type
		Adaptive Threat Protection Debug Logging Enabled	On Access Scan Debug Logging Enabled

Feature Group	Result Type	Property (Column)	Property (Column)
		Adaptive Threat Protection Events Filter Level	On Access Scan Events Filter Level
		Client Activity Logging Enabled	On Demand Scan Debug Logging Enabled
		Client Activity Log Size in MB	On Demand Scan Events Filter Level
		Client Debug Log Size in MB	Self Protection Additional Reasons
		Client Log Files Location	Self Protection Compliance Status
		Client User Interface Access Level	Self Protection Enabled
		ESP Hotfix	Self Protection Reason
		ESP Patch Version	Send Events to McAfee ePO Enabled
		Exploit Prevention Debug Logging Enabled	SystemCore Version
		Exploit Prevention Events Filter Level	Time-Based Password Enabled
		Firewall Debug Logging Enabled	User Interface Password Changed
		Firewall Events Filter Level	Web Control Debug Logging Enabled

Feature Group	Result Type	Property (Column)	Property (Column)
		Global Exclusions Status	Web Control Events Filter Level
		Language	Windows Application Logging Enabled
	Endpoint Security Platform Properties	Language (Endpoint Security Platform)	Product Version (Endpoint Security Platform)
Events	Endpoint Security Threat Events	Access Requested	Source Parent Process Signer
		AMCore Content Version	Source Port
		Analyzer Content Creation Date	Source Process Hash
		Analyzer Content Version	Source Process Signed
		Analyzer Trellix GTI Query	Source Process Signer
		Analyzer Reg Info	Source Share Name
		Analyzer Rule ID	Source Signed
		Analyzer Rule Name	Source Signer
		Analyzer Technology Version	Source URL Rating Code
		API Name	Source URL Web Category

Feature Group	Result Type	Property (Column)	Property (Column)
		Attack Vector Type	Target Access Time
		Cleanable	Target Create Time
		Description	Target Description
		Direction	Target Device Display Name
		Duration Before Detection (Days)	Target Device PID
		First Action Status	Target Device Serial Number
		First Attempted Action	Target Device VID
		Location	Target File Size (Bytes)
		Module Name	Target Hash
		Second Action Status	Target Modify Time
		Second Attempted action	Target Name
		Source Access Time	Target Parent Process Hash
		Source Create Time	Target Parent Process Name
		Source Description	Target Parent Process Signed

Feature Group	Result Type	Property (Column)	Property (Column)
		Source Device Display Name	Target Parent Process Signer
		Source Device PID	Target Path
		Source Device Serial Number	Target Share Name
		Source Device VID	Target Signed
		Source File Hash	Target Signer
		Source File Path	Target URL
		Source File Size (Bytes)	Task Name
		Source Modify Time	Threat Detected On Creation
		Source Parent Process Hash	Threat Impact
		Source Parent Process Name	Topic
		Source Parent Process Signed	

For information about queries and reports, see the Trellix ePO - On-prem documentation.

Server tasks and Common

Automate server management or maintenance using server tasks.

Server tasks are scheduled management or maintenance tasks that you run on your Trellix ePO - On-prem server. Server tasks enable you to schedule and automate repetitive tasks. Use server tasks to monitor your server and software.

Depending on your permissions, you can use default server tasks as is, edit them, or create server tasks using Trellix ePO - On-prem.

Default server tasks

Common does not provide predefined server tasks. You can use predefined Trellix ePO - On-prem server tasks to manage Common.

Custom server tasks

To create a custom server task, run the **Server Task Builder** and select from the **Actions** drop-down list.

Server tasks	Description	Management platform
Export Policies	Downloads an XML file that contains the associated policy.	Trellix ePO - On-prem
Export Queries or **Export Reports**	Generates a query or report output file that can be saved or emailed to a recipient.	Trellix ePO - On-prem
Purge Client Events	Deletes client events based on a time unit or using a query	Trellix ePO - On-prem
Purge Rolled-up Data	Deletes selected Data Types from other registered Trellix ePO - On-prem servers.	Trellix ePO - On-prem
Purge Threat Event Log	Deletes threat event logs based on a time unit or using a query.	Trellix ePO - On-prem
Repository Pull	Retrieves packages from the source site and place them in the **Main Repository**. Select **AMCore Content** or **Endpoint Security Exploit Prevention Content** as a package type to retrieve content updates automatically.	Trellix ePO - On-prem
Roll Up Data	Rolls up system or event data from multiple servers at the same time.	Trellix ePO - On-prem

Server tasks	Description	Management platform
	Select **Endpoint Security Platform Systems** for the **Data Type**.	
Run Query	Runs default queries at a specified time and schedule.	All
Run Report	Generates a query report file that can be exported or emailed to a recipient.	All

For information about server tasks, see the Trellix ePO - On-prem documentation.

Roll up system or event data for Trellix ENS (Trellix ePO - On-prem)

You can compile Trellix ENS system data and event data from multiple servers managed Trellix ePO - On-prem.

Trellix ePO - On-prem roll up server task does not enforce any version limitation. However, the database schema or table structure needs to be compatible between the source table and target table. Hence, it is recommended to run roll up task between same product versions to avoid any conflicts.

Task

1. Select **Menu** → **Automation** → **Server Tasks**, then click **New Task**.
2. On the **Description** page, type a name and description for the task, and select whether to enable it, then click **Next**.
3. Click **Actions**, then select **Roll Up Data**.
4. From the **Roll up data from:** drop-down list, select one:
    - **All registered servers**
    - **Selected registered servers** — Select the servers you want, then click **OK**.
5. To roll up system data:
    a. For the **Data Type**, select **Managed Systems**.
    b. Select the **Additional Types: Configure** link, and select the Trellix ENS types you want to include.
6. To roll up event data:
    a. Click the **+** button at the end of the table heading to add another data type, then select **Threat Events.**
    b. Click **Additional Types: Configure**, and select the Trellix ENS types you want to include.
7. Schedule the task, then click **Next**.
8. Review the settings, then click **Save**.

Events, responses, and Common

Configure **Automatic Responses** to react to threat events.

The **Threat Event Log** is a log file of all threat events that Trellix ePO - On-prem receives from managed systems.

In Trellix ePO - On-prem, you can define which events are forwarded to the Trellix ePO - On-prem server. To display the complete list of events in Trellix ePO - On-prem, select **Menu** → **Configuration** → **Server Settings**, select **Event Filtering**, then click **Edit**.

Set up a **Purge Threat Event Log** server task to purge the **Threat Event Log** periodically.

For information about **Automatic Responses** and working with the **Threat Event Log**, see the Trellix ePO - On-prem Help.

Monitoring Threat Prevention activity

Dashboards, monitors, and Threat Prevention

Keep watch on the status of your managed systems and any threats in your environment using your customizable dashboard.

Dashboards are collections of monitors that track activity in your Trellix ePO - On-prem environment.

Default dashboards and monitors

Threat Prevention contributes monitors to several Common dashboards.

Common dashboards and Threat Prevention monitors

Dashboard	Monitor	Description
Endpoint Security: Compliance Status		Whether the enabled state in the policy matches the enabled state on the client system. If the technology is enabled in policy and disabled on the client, the system is noncompliant.
	Endpoint Security Threat Prevention: Access Protection Compliance Status	Number of systems with Access Protection compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system

Dashboard	Monitor	Description
	Endpoint Security Threat Prevention: AMCore Content Compliance Status	Number of systems with AMCore content compliant or noncompliant: • **Compliant** — The AMCore content creation date is less than 7 days old. • **Non-Compliant** — The AMCore content creation date is more than 7 days old.
	Endpoint Security Threat Prevention: Exploit Prevention Compliance Status	Number of systems with Exploit Prevention compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system
	Endpoint Security Threat Prevention: On-Access Scan Compliance Status	Number of systems with on-access scanner protection compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system
Endpoint Security: Content Status		Versions of the content files and engine.

Dashboard	Monitor	Description
	Endpoint Security Threat Prevention: Content Status	Version of the AMCore Content and the number of systems with that version installed.
	Endpoint Security Threat Prevention: Exploit Prevention Content Status	Version of the Exploit Prevention Content and the number of systems with that version installed.
Endpoint Security: Installation Status		Whether a module is installed.
	Endpoint Security Threat Prevention: Hotfixes Installed	Number of systems with Threat Prevention hotfixes installed, including hotfix version numbers.
Endpoint Security: Scan Duration		Average time for system scans.
	Endpoint Security Threat Prevention: Duration of Completed Full Scans in the Last 7 Days	Number of completed **Full Scan** system scans by time in hours (from less than 1 hour to greater than 12 hours) and the number of systems per duration. For each duration, this monitor shows: • Scan start and end time • System name • Last communicated time
	Endpoint Security Threat Prevention: Duration of Completed Quick Scans in the Last 7 Days	Number of completed **Quick Scan** system scans by time in hours (from less than 10 minutes to greater than an hour) and the number of systems per duration. For each duration, this monitor shows: • Scan start and end time • System name

Dashboard	Monitor	Description
		• Last communicated time
Endpoint Security: Threat Event Origins		How threats are entering the environment.
	Endpoint Security Threat Prevention: Applications with the Most Exploits in the Last 7 Days	Applications with the most buffer overflow exploits, including the number of detections.
Endpoint Security: Protection Summary (Only in Trellix ePO - SaaS)		Displays information on the number of nodes installed, protected, and whether the content is up to date (i.e., less than a week old).
	Protection Status	There is also an option to start the Install Protection workflow from this monitor. In this monitor, the criteria for **Installed**, **Protected**, and **Up-to-date** count is as follows: • **Installed**: The customer must have all licensed Endpoint modules installed on all end-nodes to get a perfect score. • **Protected**: The customer must have all licensed Endpoint module technologies enabled on all end-nodes to get a perfect score. • **Up-to-date**: The customer must have AMCore content that is less than a week old installed on all end-nodes to get a perfect score.

Custom dashboards (Trellix ePO - On-prem)

Depending on your permissions, you can create custom dashboards and add monitors using default Trellix ENS queries.

For information about dashboards, see the Trellix ePO - On-prem documentation.

Queries, reports, and Threat Prevention

Use queries to retrieve detailed information about the status of your managed systems and any threats in your environment. You can export, download, or combine queries into reports, and use queries as dashboard monitors.

Queries are questions that you ask Trellix ePO - On-prem, which returns answers as charts and tables. Reports enable you to package one or more queries into a single PDF document, for access outside of Trellix ePO - On-prem.

Similar information is available by accessing activity logs from the Trellix Endpoint Security (ENS) Client on individual systems.

You can view query data only for resources where you have permissions. For example, if your permissions grant access to a specific **System Tree** location, your queries return data only for that location.

Best practice: For information on how to create a report of which computers have an Extra.DAT file installed, see KB59410. For information on how to create a report for completed on-demand scans (event 1203), see KB69428.

Default queries

The module adds default queries to **McAfee Groups**. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the Trellix ePO - On-prem database.

- **Endpoint Security Threat Prevention: Access Protection Compliance Status**
- **Endpoint Security Threat Prevention: AMCore Content Compliance Status**
- **Endpoint Security Threat Prevention: Applications with the Most Exploits in the Last 7 Days**
- **Endpoint Security Threat Prevention: Content Status**
- **Endpoint Security Threat Prevention: Detection Response Summary**
- **Endpoint Security Threat Prevention: Duration of Completed Full Scans in the Last 7 Days**
- **Endpoint Security Threat Prevention: Duration of Completed Quick Scans in the Last 7 Days**
- **Endpoint Security Threat Prevention: Exploit Prevention Compliance Status**
- **Endpoint Security Threat Prevention: Exploit Prevention Content Status**
- **Endpoint Security Threat Prevention: False Positive Mitigation Events**
- **Endpoint Security Threat Prevention: Hotfixes Installed**
- **Endpoint Security Threat Prevention: On-Access Scan Compliance Status**
- **Endpoint Security Threat Prevention: On-Access Scan McAfee GTI Sensitivity Level**
- **Endpoint Security Threat Prevention: On-Demand Full Scan McAfee GTI Sensitivity Level**
- **Endpoint Security Threat Prevention: On-Demand Quick Scan McAfee GTI Sensitivity Level**
- **Endpoint Security Threat Prevention: Right-Click Scan McAfee GTI Sensitivity Level**
- **Endpoint Security Threat Prevention: Systems Not Completed a Full Scan in the Last 7 Days**
- **Endpoint Security Threat Prevention: Systems Not Completed a Full Scan in the Last Month**
- **Endpoint Security Threat Prevention: Threat Count by Severity**

- **Endpoint Security Threat Prevention: Threats Detected Over the Previous 2 Quarters**
- **Endpoint Security Threat Prevention: Top 10 Access Protection Rules Broken**
- **Endpoint Security Threat Prevention: Top 10 Computers with the Most Detections**
- **Endpoint Security Threat Prevention: Top 10 Detected Threats**
- **Endpoint Security Threat Prevention: Top 10 Exploits Prevented**
- **Endpoint Security Threat Prevention: Top 10 Threat Sources**
- **Endpoint Security Threat Prevention: Top 10 Threats per Threat Category**
- **Endpoint Security Threat Prevention: Top 10 Users with the Most Detections**

Custom queries (Trellix ePO - On-prem)

The module adds default properties to the **Endpoint Security** feature group. You can use these properties to create custom queries.

Feature Group	Result Type	Property (Column)	Property (Column)
Endpoint Security	Endpoint Security Threat Prevention Systems	Access Protection Additional Reasons	License Status
		Access Protection Compliance Status	Names of threats that Extra.DAT can detect
		Access Protection Enabled	On-Access Scan Additional Reason
		Access Protection Reason	On-Access Scan Compliance Status
		AMCore Content Additional Reasons	On-Access Scan Enabled
		AMCore Content Compliance Days	On-Access Scan Trellix Sensitivity
		AMCore Content Compliance Status	On-Access Scan Reason
		AMCore Content Date	On-Demand Full Scan Date
		AMCore Content Reason	On-Demand Full Scan Duration (hours)

Feature Group	Result Type	Property (Column)	Property (Column)
		AMCore Content Version	**On-Demand Full Scan Trellix Sensitivity**
		AMCore Engine Version	**On-Demand Quick Scan Date**
		AMSI Enabled (Windows 10 and Windows Server 2016 systems only)	**On-Demand Quick Scan Duration (minutes)**
		AMSI Observe Mode Enabled (Windows 10 and Windows Server 2016 systems only)	**On-Demand Quick Scan Trellix Sensitivity**
		AMSI supported by system	**On-Demand Scan Additional Reasons**
		AMSI supported by system reason	**On-Demand Scan Compliance Status** (*)
		DAT Version (Non-Windows)	**On-Demand Scan Reason**
		Exploit Prevention Additional Reasons	**Right-Click Scan Trellix Sensitivity**
		Exploit Prevention Compliance Status	**ScriptScan Additional Reasons**
		Exploit Prevention Content Created	**ScriptScan Compliance Status**
		Exploit Prevention Content Version	**ScriptScan Enabled**

Feature Group	Result Type	Property (Column)	Property (Column)
		Exploit Prevention Enabled	ScriptScan Reason
		Exploit Prevention Reason	Threat Prevention Hotfix
		Language	Threat Prevention Patch Version
	Endpoint Security Platform Systems	Access Protection Debug Logging Enabled	On Access Scan Debug Logging Enabled
		Access Protection Events Filter Level	On Access Scan Events Filter Level
		Exploit Prevention Debug Logging Enabled	On Demand Scan Debug Logging Enabled
		Exploit Prevention Events Filter Level	On Demand Scan Events Filter Level
Events	Exploit Prevention Events	Access Requested	Source Port
		Action Taken	Source Process Hash
		Agent GUID	Source Process Signed
		AMCore Content Version	Source Process Signer
		Analyzer Content Creation Date	Source Share Name
		Analyzer Content Creation Version	Source Signed

Feature Group	Result Type	Property (Column)	Property (Column)
		Analyzer Detection Method	Source Signer
		Analyzer Trellix Query	Source URL Rating Code
		Analyzer Reg Info	Source URL Web Category
		Analyzer Rule ID	Target Access Time
		Analyzer Rule Name	Target Create Time
		Analyzer Technology Version	Target Description
		API Name	Target Device Display Name
		Attack Vector Type	Target Device PID
		Cleanable	Target Device Serial Number
		DAT Version	Target Device VID
		Description	Target File Size (Bytes)
		Detecting Prod ID (deprecated)	Target Hash
		Detecting Product Host Name	Target Modify Time
		Detecting Product IP Address	Target Name

Feature Group	Result Type	Property (Column)	Property (Column)
		Detecting Product IPv4 Address	Target Parent Process Hash
		Detecting Product MAC Address	Target Parent Process Name
		Detecting Product Name	Target Parent Process Signed
		Detecting Product Version	Target Parent Process Signer
		Direction	Target Path
		Duration Before Detection (Days)	Target Share Name
		Engine Version	Target Signed
		Event Category	Target Signer
		Event Generated Time	Target URL
		Event ID	Task Name
		Event Received Time	Threat Detected On Creation
		First Action Status	Threat Handled
		First Attempted Action	Threat Impact
		Location	Threat Name
		Module Name	Threat Severity

Feature Group	Result Type	Property (Column)	Property (Column)
		Second Action Status	Threat Source Host Name
		Second Attempted Action	Threat Source IP Address
		Server ID	Threat Source IPv4 Address
		Source Access Time	Threat Source MAC Address
		Source Create Time	Threat Source Process Name
		Source Description	Threat Source URL
		Source Device Display Name	Threat Source User Name
		Source Device PID	Threat Target File Path
		Source Device Serial Number	Threat Target Host Name
		Source Device VID	Threat Target IP Address
		Source File Hash	Threat Target IPv4 Address
		Source File Path	Threat Target MAC Address
		Source File Size (Bytes)	Threat Target Network Protocol

Feature Group	Result Type	Property (Column)	Property (Column)
		Source Modify Time	Threat Target Port Number
		Source Parent Process Hash	Threat Target Process Name
		Source Parent Process Name	Threat Target User Name
		Source Parent Process Signed	Threat Type
		Source Parent Process Signer	Topic

For information about queries and reports, see the Trellix ePO - On-prem documentation.

* * A system is considered compliant for on-demand scans based on any of the following criteria:

- Threat Prevention was installed less than 7 days ago.
- The on-demand scan Full Scan task completed less than 7 days ago.
- An on-demand scan task that at least contains all same scan locations as the Full Scan task, completed less than 7 days ago.

Server tasks and Threat Prevention

Automate server management or maintenance using server tasks.

Server tasks are scheduled management or maintenance tasks that you run on your Trellix ePO - On-prem server. Server tasks enable you to schedule and automate repetitive tasks. Use server tasks to monitor your server and software.

Depending on your permissions, you can use default server tasks as is, edit them, or create server tasks using Trellix ePO - On-prem.

Default server tasks

Threat Prevention does not provide predefined server tasks. You can use predefined Trellix ePO - On-prem server tasks to manage Threat Prevention.

Custom server tasks

To create a custom server task, run the **Server Task Builder** and select from the **Actions** drop-down list.

Server tasks	Description	Management platform
Export Policies	Downloads an XML file that contains the associated policy.	Trellix ePO - On-prem
Export Queries or **Export Reports**	Generates a query or report output file that can be saved or emailed to a recipient.	Trellix ePO - On-prem
Purge Client Events	Deletes client events based on a time unit or using a query	Trellix ePO - On-prem
Purge Rolled-up Data	Deletes selected Data Types from other registered Trellix ePO - On-prem servers.	Trellix ePO - On-prem
Purge Threat Event Log	Deletes threat event logs based on a time unit or using a query.	Trellix ePO - On-prem
Repository Pull	Retrieves packages from the source site and place them in the **Main Repository**. Select **AMCore Content** or **Endpoint Security Exploit Prevention Content** as a package type to retrieve content updates automatically.	Trellix ePO - On-prem
Roll Up Data	Rolls up system or event data from multiple servers at the same time. Select **Endpoint Security Threat Prevention Rolled-Up Systems** or **Endpoint Security Threat Events** for the **Data type**.	Trellix ePO - On-prem
Run Query	Runs default queries at a specified time and schedule.	All

Server tasks	Description	Management platform
Run Report	Generates a query report file that can be exported or emailed to a recipient.	All

For information about server tasks, see the Trellix ePO - On-prem documentation.

Roll up system or event data for Trellix ENS (Trellix ePO - On-prem)

You can compile Trellix ENS system data and event data from multiple servers managed Trellix ePO - On-prem.

Trellix ePO - On-prem roll up server task does not enforce any version limitation. However, the database schema or table structure needs to be compatible between the source table and target table. Hence, it is recommended to run roll up task between same product versions to avoid any conflicts.

Task

1. Select **Menu** → **Automation** → **Server Tasks**, then click **New Task**.
2. On the **Description** page, type a name and description for the task, and select whether to enable it, then click **Next**.
3. Click **Actions**, then select **Roll Up Data**.
4. From the **Roll up data from:** drop-down list, select one:
    - **All registered servers**
    - **Selected registered servers** — Select the servers you want, then click **OK**.
5. To roll up system data:
    a. For the **Data Type**, select **Managed Systems**.
    b. Select the **Additional Types: Configure** link, and select the Trellix ENS types you want to include.
6. To roll up event data:
    a. Click the **+** button at the end of the table heading to add another data type, then select **Threat Events.**
    b. Click **Additional Types: Configure**, and select the Trellix ENS types you want to include.
7. Schedule the task, then click **Next**.
8. Review the settings, then click **Save**.

Events, responses, and Threat Prevention

Configure **Automatic Responses** to react to threat events.

The **Threat Event Log** is a log file of all threat events that Trellix ePO - On-prem receives from managed systems.

In Trellix ePO - On-prem, you can define which events are forwarded to the Trellix ePO - On-prem server. To display the complete list of events in Trellix ePO - On-prem, select **Menu** → **Configuration** → **Server Settings**, select **Event Filtering**, then click **Edit**.

Set up a **Purge Threat Event Log** server task to purge the **Threat Event Log** periodically.

You can also view and manage Exploit Prevention events in Trellix ePO - On-prem in the **Exploit Prevention Events** page under **Reporting**.

You can use events to customize **Automatic Responses**.

For information about **Automatic Responses** and working with the **Threat Event Log**, see the Trellix ePO - On-prem Help.

Monitoring Firewall activity

Dashboards, monitors, and Firewall

Keep watch on the status of your managed systems and any threats in your environment using your customizable dashboard.

Dashboards are collections of monitors that track activity in your Trellix ePO - On-prem environment.

Default dashboards and monitors

The module provides default dashboards and monitors. Depending on your permissions, you can use them as is, modify them to add or remove monitors, or create custom dashboards using Trellix ePO - On-prem.

Firewall includes the following default dashboard.

Firewall dashboards and monitors

Dashboard	Monitor	Description
Endpoint Security: Firewall Dashboard		Status of Trellix Endpoint Security (ENS) Firewall.
	Endpoint Security Firewall: Events from McAfee GTI	Number of Firewall intrusion or detection events from Trellix GTI .
	Endpoint Security Firewall: Events in the last 24 hours	Number of intrusion or detection events from Firewall in the last 24 hours.

In addition to the default Firewall dashboard, Firewall contributes monitors to several Common dashboards.

Common dashboards and Firewall monitors

Dashboard	Monitor	Description
Endpoint Security: Compliance Status		Whether the enabled state in the policy matches the enabled state on the client system. If the technology is enabled in policy

Dashboard	Monitor	Description
		and disabled on the client, the system is noncompliant.
	Endpoint Security Firewall: Compliance Status	Number of systems with Firewall compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system
Endpoint Security: Installation Status		Whether a module is installed.
	Endpoint Security Firewall: Hotfixes Installed	Number of systems with Firewall hotfixes installed, including hotfix version numbers.

Custom dashboards (Trellix ePO - On-prem)

Depending on your permissions, you can create custom dashboards and add monitors using default Trellix ENS queries.

For information about dashboards, see the Trellix ePO - On-prem documentation.

Queries, reports, and Firewall

Use queries to retrieve detailed information about the status of your managed systems and any threats in your environment. You can export, download, or combine queries into reports, and use queries as dashboard monitors.

Queries are questions that you ask Trellix ePO - On-prem, which returns answers as charts and tables. Reports enable you to package one or more queries into a single PDF document, for access outside of Trellix ePO - On-prem.

Similar information is available by accessing activity logs from the Trellix Endpoint Security (ENS) Client on individual systems.

You can view query data only for resources where you have permissions. For example, if your permissions grant access to a specific **System Tree** location, your queries return data only for that location.

Default queries

The module adds default queries to **McAfee Groups**. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the Trellix ePO - On-prem database.

- Endpoint Security Firewall: Firewall Client Rules By Process
- Endpoint Security Firewall: Firewall Client Rules By Process/Port Range
- Endpoint Security Firewall: Firewall Client Rules By Process/User
- Endpoint Security Firewall: Firewall Client Rules By Protocol/System Name
- Endpoint Security Firewall: Compliance Status
- Endpoint Security Firewall: Count of Firewall Client Rules
- Endpoint Security Firewall: Errors
- Endpoint Security Firewall: Events from McAfee GTI in the last 6 months
- Endpoint Security Firewall: Events in the last 24 hours
- Endpoint Security Firewall: Hotfixes Installed
- Endpoint Security Firewall: Intrusion events in the last 24 hours
- Endpoint Security Firewall: Status
- Endpoint Security Firewall: Traffic block events in the last 24 hours

Custom queries (Trellix ePO - On-prem)

The module adds default properties to the **Endpoint Security** feature group. You can use these properties to create custom queries.

Feature Group	Result Type	Property (Column)	Property (Column)
Endpoint Security	Endpoint Security Firewall Systems	Additional Compliance Status Reason	Firewall Patch Version
		Compliance Status Reason	Firewall Rules Policy
		Endpoint Security Firewall client version	Firewall Service Running
		Endpoint Security Firewall Compliance Status	Firewall Status
		Firewall Adaptive Mode Status	Firewall Trusted Applications Policy
		Firewall Fault	Firewall Trusted Networks Policy
		Firewall Hotfixes	Install Directory (32 bit version)

Feature Group	Result Type	Property (Column)	Property (Column)
		Firewall Last Policy Enforcement	Install Directory (64 bit version)
		Firewall License Status	Language
		Firewall Mode	Product Version
		Firewall Name Client UI Policy	Reboot Required
		Firewall Options Policy	
	Endpoint Security Firewall Properties	Language (Endpoint Security Firewall)	Product Version (Endpoint Security Firewall)
	Endpoint Security Platform Systems	Firewall Debug Logging Enabled	Firewall Event Filter Level

For information about queries and reports, see the Trellix ePO - On-prem documentation.

Server tasks and Firewall

Automate server management or maintenance using server tasks.

Server tasks are scheduled management or maintenance tasks that you run on your Trellix ePO - On-prem server. Server tasks enable you to schedule and automate repetitive tasks. Use server tasks to monitor your server and software.

Depending on your permissions, you can use default server tasks as is, edit them, or create server tasks using Trellix ePO - On-prem.

Default server tasks

Your managed product provides these server tasks. You can use server tasks as is, edit them, or create new ones.

Server task	Description	Management platform
Endpoint Security Firewall Property Translator	Translates Firewall client rules in the client properties stored in the Trellix ePO - On-prem database,	Trellix ePO - On-prem

Server task	Description	Management platform
	and adds them to the **Firewall Client Rules** page. When enabled, the **Endpoint Security Firewall Property Translator** task runs automatically every 60 minutes and requires no user interaction. To see immediate feedback from actions on the client, run an agent wake-up call, then run this server task manually.	

Custom server tasks

To create a custom server task, run the **Server Task Builder** and select from the **Actions** drop-down list.

Server tasks	Description	Management platform
Export Policies	Downloads an XML file that contains the associated policy.	Trellix ePO - On-prem
Export Queries or **Export Reports**	Generates a query or report output file that can be saved or emailed to a recipient.	Trellix ePO - On-prem
Purge Client Events	Deletes client events based on a time unit or using a query	Trellix ePO - On-prem
Purge Rolled-up Data	Deletes selected Data Types from other registered Trellix ePO - On-prem servers.	Trellix ePO - On-prem
Purge Server Task Log	Deletes entries from the Server Task Log based on user-configured age.	All
Purge Threat Event Log	Deletes threat event logs based on a time unit or using a query.	Trellix ePO - On-prem

Server tasks	Description	Management platform
Roll Up Data	Rolls up system or event data from multiple servers at the same time. Select **Endpoint Security Firewall Systems** or **Endpoint Security Threat Events** for the **Data type**.	Trellix ePO - On-prem
Run Query	Runs default queries at a specified time and schedule.	All
Run Report	Generates a query report file that can be exported or emailed to a recipient.	All

For information about server tasks, see the Trellix ePO - On-prem documentation.

Roll up system or event data for Trellix ENS (Trellix ePO - On-prem)

You can compile Trellix ENS system data and event data from multiple servers managed Trellix ePO - On-prem.

Trellix ePO - On-prem roll up server task does not enforce any version limitation. However, the database schema or table structure needs to be compatible between the source table and target table. Hence, it is recommended to run roll up task between same product versions to avoid any conflicts.

Task

1. Select **Menu** → **Automation** → **Server Tasks**, then click **New Task**.
2. On the **Description** page, type a name and description for the task, and select whether to enable it, then click **Next**.
3. Click **Actions**, then select **Roll Up Data**.
4. From the **Roll up data from:** drop-down list, select one:
    - **All registered servers**
    - **Selected registered servers** — Select the servers you want, then click **OK**.
5. To roll up system data:
    a. For the **Data Type**, select **Managed Systems**.
    b. Select the **Additional Types: Configure** link, and select the Trellix ENS types you want to include.
6. To roll up event data:
    a. Click the **+** button at the end of the table heading to add another data type, then select **Threat Events.**
    b. Click **Additional Types: Configure**, and select the Trellix ENS types you want to include.
7. Schedule the task, then click **Next**.
8. Review the settings, then click **Save**.

Events, responses, and Firewall

Configure **Automatic Responses** to react to threat events.

The **Threat Event Log** is a log file of all threat events that Trellix ePO - On-prem receives from managed systems.

In Trellix ePO - On-prem, you can define which events are forwarded to the Trellix ePO - On-prem server. To display the complete list of events in Trellix ePO - On-prem, select **Menu** → **Configuration** → **Server Settings**, select **Event Filtering**, then click **Edit**.

Set up a **Purge Threat Event Log** server task to purge the **Threat Event Log** periodically.

For information about **Automatic Responses** and working with the **Threat Event Log**, see the Trellix ePO - On-prem Help.

Monitoring Web Control activity

Dashboards, monitors, and Web Control

Keep watch on the status of your managed systems and any threats in your environment using your customizable dashboard.

Dashboards are collections of monitors that track activity in your Trellix ePO - On-prem environment.

Default dashboards and monitors

The module provides default dashboards and monitors. Depending on your permissions, you can use them as is, modify them to add or remove monitors, or create custom dashboards using Trellix ePO - On-prem.

Web Control includes the following default dashboards.

Web Control dashboards and monitors

Dashboard	Monitor	Description
Endpoint Security Web Control: Activity		Activity reported by Web Control.
	Endpoint Security Web Control: Top 100 Visited Red Sites	Top 100 visited sites for each rating.
	Endpoint Security Web Control: Top 100 Visited Yellow Sites	
	Endpoint Security Web Control: Top 100 Visited Unrated Sites	

Dashboard	Monitor	Description
	Endpoint Security Web Control: Top 100 Red Downloads	Top 100 download sites for each rating.
	Endpoint Security Web Control: Top 100 Yellow Downloads	
	Endpoint Security Web Control: Top 100 Unrated Downloads	
Endpoint Security Web Control: Block and Allow Lists	**Endpoint Security Web Control: Top 100 Sites on Block List**	Top 100 sites set to allow in the **Block and Allow List**.
	Endpoint Security Web Control: Top 100 Sites on Allow List	Top 100 sites set to block in the **Block and Allow List**.
	Endpoint Security Web Control: Top 100 Red Sites on Allow List	Top 100 sites rated as red allowed in the **Block and Allow List**.
Endpoint Security Web Control: Content Summary	**Endpoint Security Web Control: Visits by Content**	Activity based on content type.
	Endpoint Security Web Control: Top Sites Grouped by Content	Top site visits organized by content.
	Endpoint Security Web Control: Visits by Action Grouped by Content	Site visits organized by action taken based on content.
Endpoint Security Web Control: Security Summary	**Endpoint Security Web Control: Visits by Rating**	Site visits organized by content rating.
	Endpoint Security Web Control: Visits by Action	Site visits organized by action taken.
	Endpoint Security Web Control: Downloads by Rating	Downloads organized by content rating.

Dashboard	Monitor	Description
	Endpoint Security Web Control: Downloads by Action	Downloads organized by action taken.
Endpoint Security Web Control: Warned/Blocked	**Endpoint Security Web Control: Top 100 Blocked Sites**	Top 100 sites, which Web Control blocked.
	Endpoint Security Web Control: Top 100 Blocked Red Sites	Top 100 sites rated as red, which Web Control blocked.
	Endpoint Security Web Control: Top 100 Warned-Cancelled Sites	Top 100 sites where Web Control warned the user and the user canceled the operation.
	Endpoint Security Web Control: Top 100 Warned-Continued Sites	Top 100 sites where Web Control warned the user and the user continued to the site.

In addition to the default Web Control dashboards, Web Control contributes monitors to several Common dashboards.

Common dashboards and Web Control monitors

Dashboard	Monitor	Description
Endpoint Security: Compliance Status		Whether the enabled state in the policy matches the enabled state on the client system. If the technology is enabled in policy and disabled on the client, the system is noncompliant.
	Endpoint Security Web Control: Compliance Status	Number of systems with Web Control compliant or noncompliant: • **Compliant** — Enabled state in policy matches the enabled state on client system • **Non-Compliant** — Enabled state in policy doesn't match

Dashboard	Monitor	Description
		the enabled state on client system
Endpoint Security: Installation Status		Whether a module is installed.
	Endpoint Security Web Control: Hotfixes Installed	Number of systems with Web Control hotfixes installed, including hotfix version numbers.
Endpoint Security: Threat Event Origins		How threats are entering the environment.
	Endpoint Security Web Control: Web Content Categories that Caused the Most Infections in the Last 7 Days	Top 10 categories of websites that cause the most infections in the environment.

Custom dashboards (Trellix ePO - On-prem)

Depending on your permissions, you can create custom dashboards and add monitors using default Trellix ENS queries.

For information about dashboards, see the Trellix ePO - On-prem documentation.

Queries, reports, and Web Control

Use queries to retrieve detailed information about the status of your managed systems and any threats in your environment. You can export, download, or combine queries into reports, and use queries as dashboard monitors.

Queries are questions that you ask Trellix ePO - On-prem, which returns answers as charts and tables. Reports enable you to package one or more queries into a single PDF document, for access outside of Trellix ePO - On-prem.

Similar information is available by accessing activity logs from the Trellix Endpoint Security (ENS) Client on individual systems.

You can view query data only for resources where you have permissions. For example, if your permissions grant access to a specific **System Tree** location, your queries return data only for that location.

Default queries

The module adds default queries to **McAfee Groups**. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the Trellix ePO - On-prem database.

- Endpoint Security Web Control: Compliance Status
- Endpoint Security Web Control: Download Log
- Endpoint Security Web Control: Downloads by Action
- Endpoint Security Web Control: Downloads by Rating
- Endpoint Security Web Control: Hotfixes Installed
- Endpoint Security Web Control: Top 100 Blocked Red Sites
- Endpoint Security Web Control: Top 100 Blocked Sites
- Endpoint Security Web Control: Top 100 Red Downloads
- Endpoint Security Web Control: Top 100 Red Sites on Allow List
- Endpoint Security Web Control: Top 100 Sites on Allow List
- Endpoint Security Web Control: Top 100 Sites on Block List
- Endpoint Security Web Control: Top 100 Unrated Downloads
- Endpoint Security Web Control: Top 100 Visited Red Sites
- Endpoint Security Web Control: Top 100 Visited Unrated Sites
- Endpoint Security Web Control: Top 100 Visited Yellow Sites
- Endpoint Security Web Control: Top 100 Warned-Cancelled Sites
- Endpoint Security Web Control: Top 100 Warned-Continued Sites
- Endpoint Security Web Control: Top 100 Yellow Downloads
- Endpoint Security Web Control: Top Sites Grouped by Content
- Endpoint Security Web Control: Visit Log
- Endpoint Security Web Control: Visits by Action
- Endpoint Security Web Control: Visits by Action Grouped by Content
- Endpoint Security Web Control: Visits by Content
- Endpoint Security Web Control: Visits by Rating
- Endpoint Security Web Control: Web Content Categories that Caused the Most Infections in the Last 7 Days

Custom queries (Trellix ePO - On-prem)

The module adds default properties to the **Endpoint Security** feature group. You can use these properties to create custom queries.

Feature Group	Result Type	Property (Column)	Property (Column)
Endpoint Security	Endpoint Security Web Control Systems	Compliance Status	Language
		Compliance Status Additional Reasons	License Status
		Compliance Status Reason	Web Control Enabled
		Functional in Chrome	Web Control Functional Status

Feature Group	Result Type	Property (Column)	Property (Column)
		Functional in Firefox	Web Control Hotfixes
		Functional in Internet Explorer	Web Control Patch Version
		Functional in Safari (macOS only)	
	Endpoint Security Web Control Properties	Language (Endpoint Security Web Control)	Product Version (Endpoint Security Web Control)
Events	Web Control Events	Action	email
		Affiliations	Exploits
		Annoyances	List Type
		Content	Observe Mode
		Count	Rating
		Domain	Reason
		Download	URL
		e-Commerce	
	Endpoint Security Platform Systems	Web Control Debug Logging Enabled	Web Control Event Filter Level

For information about queries and reports, see the Trellix ePO - On-prem documentation.

Server tasks and Web Control

Automate server management or maintenance using server tasks.

Server tasks are scheduled management or maintenance tasks that you run on your Trellix ePO - On-prem server. Server tasks enable you to schedule and automate repetitive tasks. Use server tasks to monitor your server and software.

Depending on your permissions, you can use default server tasks as is, edit them, or create server tasks using Trellix ePO - On-prem.

Default server tasks

Web Control does not provide predefined server tasks. You can use predefined Trellix ePO - On-prem server tasks to manage Web Control.

Custom server tasks

To create a custom server task, run the **Server Task Builder** and select from the **Actions** drop-down list.

Server tasks	Description	Management platform
Export Policies	Downloads an XML file that contains the associated policy.	Trellix ePO - On-prem
Export Queries or **Export Reports**	Generates a query or report output file that can be saved or emailed to a recipient.	Trellix ePO - On-prem
Purge Client Events	Deletes client events based on a time unit or using a query	Trellix ePO - On-prem
Purge Rolled-up Data	Deletes selected Data Types from other registered Trellix ePO - On-prem servers.	Trellix ePO - On-prem
Purge Threat Event Log	Deletes threat event logs based on a time unit or using a query. Select a **Endpoint Security Web Control: Download Log** or **Endpoint Security Web Control: Visit Log** query to purge from the log.	Trellix ePO - On-prem
Roll Up Data	Rolls up system or event data from multiple servers at the same time. Select **Endpoint Security Web Control Rolled-Up Events**,	Trellix ePO - On-prem

Server tasks	Description	Management platform
	Endpoint Security Web Control Systems, or **Endpoint Security Threat Events** for the **Data type**.	
Run Query	Runs default queries at a specified time and schedule.	All
Run Report	Generates a query report file that can be exported or emailed to a recipient.	All

For information about server tasks, see the Trellix ePO - On-prem documentation.

Roll up system or event data for Trellix ENS (Trellix ePO - On-prem)

You can compile Trellix ENS system data and event data from multiple servers managed Trellix ePO - On-prem.

Trellix ePO - On-prem roll up server task does not enforce any version limitation. However, the database schema or table structure needs to be compatible between the source table and target table. Hence, it is recommended to run roll up task between same product versions to avoid any conflicts.

Task

1. Select **Menu** → **Automation** → **Server Tasks**, then click **New Task**.
2. On the **Description** page, type a name and description for the task, and select whether to enable it, then click **Next**.
3. Click **Actions**, then select **Roll Up Data**.
4. From the **Roll up data from:** drop-down list, select one:
    - **All registered servers**
    - **Selected registered servers** — Select the servers you want, then click **OK**.
5. To roll up system data:
    a. For the **Data Type**, select **Managed Systems**.
    b. Select the **Additional Types: Configure** link, and select the Trellix ENS types you want to include.
6. To roll up event data:
    a. Click the **+** button at the end of the table heading to add another data type, then select **Threat Events.**
    b. Click **Additional Types: Configure**, and select the Trellix ENS types you want to include.
7. Schedule the task, then click **Next**.
8. Review the settings, then click **Save**.

Events, responses, and Web Control

Configure **Automatic Responses** to react to threat events.

The **Threat Event Log** is a log file of all threat events that Trellix ePO - On-prem receives from managed systems.

In Trellix ePO - On-prem, you can define which events are forwarded to the Trellix ePO - On-prem server. To display the complete list of events in Trellix ePO - On-prem, select **Menu** → **Configuration** → **Server Settings**, select **Event Filtering**, then click **Edit**.

Set up a **Purge Threat Event Log** server task to purge the **Threat Event Log** periodically.

For information about **Automatic Responses** and working with the **Threat Event Log**, see the Trellix ePO - On-prem Help.

Monitoring Adaptive Threat Protection activity

Dashboards, monitors, and Adaptive Threat Protection

Keep watch on the status of your managed systems and any threats in your environment using your customizable dashboard.

Dashboards are collections of monitors that track activity in your Trellix ePO - On-prem environment.

Default dashboards and monitors

The module provides default dashboards and monitors. Depending on your permissions, you can use them as is, modify them to add or remove monitors, or create custom dashboards using Trellix ePO - On-prem.

Adaptive Threat Protection includes the following predefined dashboards.

Dashboard	Monitor	Description
Endpoint Security: Adaptive Threat Protection Enforced Events	**Endpoint Security Adaptive Threat Protection: Clean Events for Last 30 Days**	Events for actions that were detected and enforced based on the Adaptive Threat Protection policy.
	Endpoint Security Adaptive Threat Protection: Block Events for Last 30 Days	
	Endpoint Security Adaptive Threat Protection: Allow Events for Last 30 Days	
	Endpoint Security Adaptive Threat Protection: Clean Events by Event Type	

Dashboard	Monitor	Description
	Endpoint Security Adaptive Threat Protection: Block Events by Event Type	
	Endpoint Security Adaptive Threat Protection: Allow Events by Event Type	
Endpoint Security: Adaptive Threat Protection Observed Events	**Endpoint Security Adaptive Threat Protection: Observation Clean Events for Last 30 Days**	Events, such as `Would Block`, for actions that would have been taken if the Adaptive Threat Protection actions were enforced.
	Endpoint Security Adaptive Threat Protection: Observation Block Events for Last 30 Days	
	Endpoint Security Adaptive Threat Protection: Observation Allow Events for Last 30 Days	
	Endpoint Security Adaptive Threat Protection: Observation Clean Events by Event Type	
	Endpoint Security Adaptive Threat Protection: Observation Block Events by Event Type	
	Endpoint Security Adaptive Threat Protection: Observation Allow Events by Event Type	
Endpoint Security: Adaptive Threat Protection Real Protect Detection Events	**Endpoint Security Adaptive Threat Protection: Real Protect Detection Events for Last 24 Hours**	Events for threat detections and actions taken by the Real Protect scanner.

Dashboard	Monitor	Description
	Endpoint Security Adaptive Threat Protection: Real Protect Detection Events For Last 7 Days	
	Endpoint Security Adaptive Threat Protection: Real Protect Detection Events For Last 30 Days	
	Endpoint Security Adaptive Threat Protection: Real Protect Detection Events For Last Quarter	

Custom dashboards (Trellix ePO - On-prem)

Depending on your permissions, you can create custom dashboards and add monitors using default Trellix ENS queries.

For information about dashboards, see the Trellix ePO - On-prem documentation.

Queries, reports, and Adaptive Threat Protection

Use queries to retrieve detailed information about the status of your managed systems and any threats in your environment. You can export, download, or combine queries into reports, and use queries as dashboard monitors.

Queries are questions that you ask Trellix ePO - On-prem, which returns answers as charts and tables. Reports enable you to package one or more queries into a single PDF document, for access outside of Trellix ePO - On-prem.

Similar information is available by accessing activity logs from the Trellix Endpoint Security (ENS) Client on individual systems.

You can view query data only for resources where you have permissions. For example, if your permissions grant access to a specific **System Tree** location, your queries return data only for that location.

Best practice: For information on how to create a report of which computers have an Extra.DAT file installed, see KB59410.

Default queries

The module adds default queries to **McAfee Groups**. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the Trellix ePO - On-prem database.

- **Endpoint Security Adaptive Threat Protection: Allow Events by Event Type**
- **Endpoint Security Adaptive Threat Protection: Allow Events by Rule (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Allow Events for Last 30 Days**

- **Endpoint Security Adaptive Threat Protection: Block Events by Event Type**
- **Endpoint Security Adaptive Threat Protection: Block Events by Rule (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Block Events for Last 30 Days**
- **Endpoint Security Adaptive Threat Protection: Clean Events by Event Type**
- **Endpoint Security Adaptive Threat Protection: Clean Events by Rule (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Clean Events for Last 30 Days**
- **Endpoint Security Adaptive Threat Protection: Content Status**
- **Endpoint Security Adaptive Threat Protection: Enhanced Script Scanning Support by System**
- **Endpoint Security Adaptive Threat Protection: Events by File (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Events by System (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Extra.DAT Signatures**
- **Endpoint Security Adaptive Threat Protection: Observation Allow Events by Event Type**
- **Endpoint Security Adaptive Threat Protection: Observation Allow Events by Rule (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Observation Allow Events for Last 30 Days**
- **Endpoint Security Adaptive Threat Protection: Observation Block Events by Event Type**
- **Endpoint Security Adaptive Threat Protection: Observation Block Events by Rule (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Observation Block Events for Last 30 Days**
- **Endpoint Security Adaptive Threat Protection: Observation Clean Events by Event Type**
- **Endpoint Security Adaptive Threat Protection: Observation Clean Events by Rule (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Observation Clean Events for Last 30 Days**
- **Endpoint Security Adaptive Threat Protection: Observation Events by File (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Observation Events by System (Top 10)**
- **Endpoint Security Adaptive Threat Protection: Real Protect Detection Events for Last 30 Days**
- **Endpoint Security Adaptive Threat Protection: Real Protect Detection Events for Last 7 Days**
- **Endpoint Security Adaptive Threat Protection: Real Protect Detection Events for Last Quarter**
- **Endpoint Security Adaptive Threat Protection: Real Protect Detection Events in Last 24 Hours**

Custom queries (Trellix ePO - On-prem)

The module adds default properties to the **Endpoint Security** feature group. You can use these properties to create custom queries.

Feature Group	Result Type	Property (Column)	Property (Column)
Endpoint Security	Endpoint Security Adaptive Threat Protection Systems	Adaptive Threat Protection content version	Enable offline scanning
		ATP Hotfix	Enhanced script scanning supported by system

Feature Group	Result Type	Property (Column)	Property (Column)
		ATP Patch Version	Enhanced script scanning supported by system reason
		Connection status	Is Supported OS
		Contained Applications	License Status
		Enable Adaptive Threat Protection	Monitor and remediate deleted and changed files
		Enable Adaptive Threat Protection Observe mode	Real Protect content date
		Enable client-based scanning	Real Protect content version
		Enable cloud-based scanning	Real Protect engine date
		Enable enhanced remediation	Real Protect engine version
		Enable enhanced script scanning (includes AMSI integration)	Reputation Source
		Enable enhanced script scanning Observe mode	Signatures in Extra.DAT
		Credential Theft Protection Version	Enable Credential Theft Protection Scanning

Feature Group	Result Type	Property (Column)	Property (Column)
		Enable Credential Theft Protection Observe Mode	
	Endpoint Security Platform Systems	Adaptive Threat Protection Debug Logging Enabled	Adaptive Threat Protection Events Filter Level
	Adaptive Threat Protection Events	Balance Security For	File MD5 Hash
		Certificate Company Creator	File Reputation
		Certificate Hash	File SHA1 Hash
		Certificate Name	Object Type
		Certificate Public Key Hash	Real Protect Scanning Sensitivity Level
		Content Version	Rule ID
		Detection Type	User Prompt Comments
		File Company Creator	
Others	Story Graph Properties → Adaptive Threat Protection Rules	Description	Rule Name
		Long Description	

For information about queries and reports, see the Trellix ePO - On-prem documentation.

Server tasks and Adaptive Threat Protection

Automate server management or maintenance using server tasks.

Server tasks are scheduled management or maintenance tasks that you run on your Trellix ePO - On-prem server. Server tasks enable you to schedule and automate repetitive tasks. Use server tasks to monitor your server and software.

Depending on your permissions, you can use default server tasks as is, edit them, or create server tasks using Trellix ePO - On-prem.

Default server tasks

Adaptive Threat Protection does not provide default server tasks. You can use default Trellix ePO - On-prem server tasks to manage Threat Prevention.

Custom server tasks

To create a custom server task, run the **Server Task Builder** and select from the **Actions** drop-down list.

Server tasks	Description	Management platform
Export Policies	Downloads an XML file that contains the associated policy.	Trellix ePO - On-prem
Export Queries or **Export Reports**	Generates a query or report output file that can be saved or emailed to a recipient.	Trellix ePO - On-prem
Purge Client Events	Deletes client events based on a time unit or using a query	Trellix ePO - On-prem
Purge Rolled-up Data	Deletes selected Data Types from other registered Trellix ePO - On-prem servers.	Trellix ePO - On-prem
Purge Threat Event Log	Deletes threat event logs based on a time unit or using a query.	Trellix ePO - On-prem
Repository Pull	Retrieves packages from the source site and place them in the **Main Repository**. Select **AMCore Content** as a package type to retrieve content updates automatically.	• Trellix ePO - On-prem • Trellix ePO - SaaS
Roll Up Data	Rolls up system or event data from multiple servers at the same time.	Trellix ePO - On-prem

Server tasks	Description	Management platform
	Select **Endpoint Security Threat Events** for the **Data type**.	
Run Query	Runs default queries at a specified time and schedule.	• Trellix ePO - On-prem • Trellix ePO - SaaS
Run Report	Generates a query report file that can be exported or emailed to a recipient.	• Trellix ePO - On-prem • Trellix ePO - SaaS

For information about server tasks, see the Trellix ePO - On-prem documentation.

Roll up system or event data for Trellix ENS (Trellix ePO - On-prem)

You can compile Trellix ENS system data and event data from multiple servers managed Trellix ePO - On-prem.

Trellix ePO - On-prem roll up server task does not enforce any version limitation. However, the database schema or table structure needs to be compatible between the source table and target table. Hence, it is recommended to run roll up task between same product versions to avoid any conflicts.

Task

1. Select **Menu** → **Automation** → **Server Tasks**, then click **New Task**.
2. On the **Description** page, type a name and description for the task, and select whether to enable it, then click **Next**.
3. Click **Actions**, then select **Roll Up Data**.
4. From the **Roll up data from:** drop-down list, select one:
    - **All registered servers**
    - **Selected registered servers** — Select the servers you want, then click **OK**.
5. To roll up system data:
    a. For the **Data Type**, select **Managed Systems**.
    b. Select the **Additional Types: Configure** link, and select the Trellix ENS types you want to include.
6. To roll up event data:
    a. Click the **+** button at the end of the table heading to add another data type, then select **Threat Events.**
    b. Click **Additional Types: Configure**, and select the Trellix ENS types you want to include.
7. Schedule the task, then click **Next**.
8. Review the settings, then click **Save**.

Events, responses, and Adaptive Threat Protection

Configure **Automatic Responses** to react to threat events.

The **Threat Event Log** is a log file of all threat events that Trellix ePO - On-prem receives from managed systems.

In Trellix ePO - On-prem, you can define which events are forwarded to the Trellix ePO - On-prem server. To display the complete list of events in Trellix ePO - On-prem, select **Menu** → **Configuration** → **Server Settings**, select **Event Filtering**, then click **Edit**.

Set up a **Purge Threat Event Log** server task to purge the **Threat Event Log** periodically.

For information about **Automatic Responses** and working with the **Threat Event Log**, see the Trellix ePO - On-prem Help.

Navigating the Story Graph

The Story Graph in the **Threat Event Log** provides a visual representation of file-based and fileless-based ATP threat detections. You can examine the context of threats by reviewing the details of events leading up to a detection.

For ATP to generate a Story Graph, you must enable these options in the Adaptive Threat Protection **Options** policy:

- **Adaptive Threat Protection**
- One of these options:
    - **Trigger Dynamic Application Containment when reputation threshold reaches**
    - **Block when reputation threshold reaches**
    - **Clean when reputation threshold reaches**

  The reputation threshold specified must also match the reputation of the detected event.

The Story Graph helps you answer these questions:

- **What** was executed?
- **Why** does ATP think it's malicious?
- **Where** did the threat come from?
- **When** in the attack chain did ATP stop the threat?

To view the graph for a particular threat event, open the **Threat Event Log**, select an event, and scroll down to the **Story Graph (Trace Summary)** section.

Identifying events

Icons on the Story Graph represent the type of event being traced.

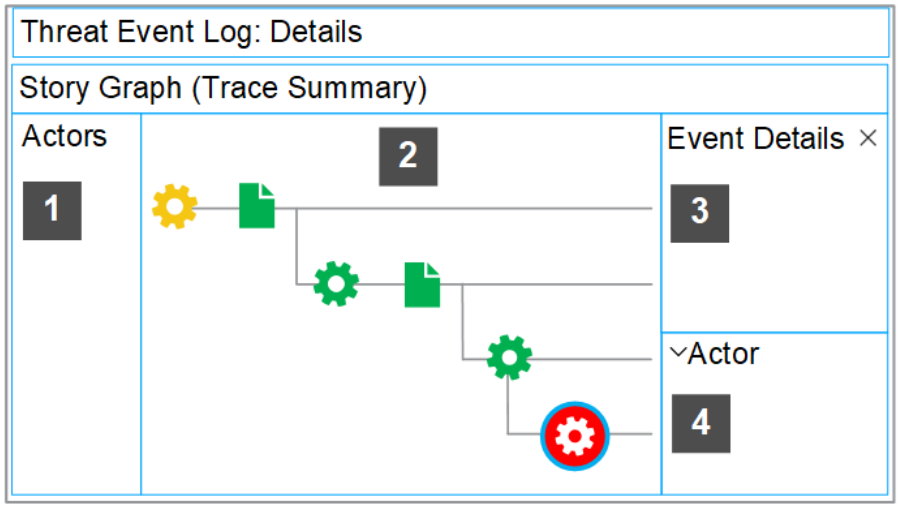
- **Processes** — gear icons
- **Files** — document icons
- **Temp files** — microSD card icons

Temp files represent an event that occurred in memory. AMSI detects these types of events.

Event colors indicate the reputation score. The **Color Legend** shows the reputation score range associated with each color.

Investigating events

The Story Graph is made up of several parts where you can view detection data.



1. View the process name of each actor involved in the detection.
2. Follow the events in the graph, from left to right, to see what led to the detection. A blue border appears around the selected event. The last event is selected by default and is where the detection occurred.
3. Investigate the suspicious activity by examining the data for each event in the graph. Click any event to open the **Event Details** window. The event data provides context that enables you to see why ATP deems the event malicious. For example, you can see the changes in reputation score and command-line parameters from event to event and the primary trigger that started the malicious activity.
4. Review details about the process that started the event. The **Actor** section doesn't appear for events where the target and the actor are the same, for example, if the process was already running.

Additional Story Graph data and any remediation details are available on the client system. ATP retains Story Graph data and remediation details for up to 90 days or 100 events. For more information, see KB90859.

Event data

Event Details window

Item	Definition
Target Name	Identifies the name of the file or process being operated on.
Reputation	Indicates the reputation given by the reputation provider.

Item	Definition
Reputation Score	Indicates the reputation score.
PID	Indicates a unique identifier for the process.
Action Taken	Describes the security action taken on the detected event (the last event in the graph).
SHA-256	Indicates the SHA-256 hash (64-digit hexadecimal number) of the file. **Tip:** Use the SHA-256 hash for file inspections with VirusTotal. To copy the SHA-256 hash, hover over the event icon and click the Copy icon.
MD5	Indicates the MD5 hash (32-digit hexadecimal number) of the file. **Tip:** Use the MD5 hash for adding exclusions.
Command-Line Parameters	Indicates the context in which the event is generated.

Actor section

Item	Definition
Name	Indicates the name of the process that started the event.
Final Reputation	Indicates the overall reputation and reputation score after the event.
Reputation Score	
Initial Reputation	Indicates the overall reputation and reputation score before the event. If the final and initial reputation are

Item	Definition
Reputation Score	the same, then the initial reputation and reputation score is not displayed.
PID	Indicates a unique identifier for the process.

Reputation scores and definitions

Reputation	Reputation score	Definition
Known Clean Updater	100	A trusted file created by a trusted updater
Known Trusted	99	A trusted file
Most Likely Trusted	85	Almost certainly a trusted file
Might Be Trusted	70	Appears to be a benign file
Unknown	50	Can't make a determination
Might Be Malicious	30	Appears to be a suspicious file
Most Likely Malicious	15	Almost certainly a malicious file
Known Malicious	1	A malicious file
Not Set	0	No reputation is specified

Disable the Story Graph

Users can choose whether or not they would like to have the Story Graph feature enabled. Story Graph is enabled by default in order to provide valuable context to ATP detections.

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Adaptive Threat Protection** from the **Product** list.
2. Click the editable policy.
3. Click **Show Advanced**.
4. In the **Story Graph** section, deselect the **Enable Story Graph Tracing** checkbox.

5. Click **Save**.
6. Enforce the policy to the client system.
7. To validate the Story Graph is disabled on the client system: On Trellix ePO - On-prem
    a. Select **Menu** → **Systems** → **System Tree** and select a group in the System Tree.
    b. Click the system name.
    c. Click **Products**, then click **Endpoint Security Adaptive Threat Protection**.
    d. Scroll down to the **Options** section to view the Story Graph on the client system is disabled.

    (On client system)
    a. Click the **Endpoint Security Adaptive Threat Protection** module and make sure the **Enable Story Graph Tracing** checkbox is deselected.

Disable a rule that triggered a detection for a known safe file

When the ATP scanner blocks a file that you know is safe, you might be able to disable the Adaptive Threat Protection rule that triggered the detection.

Note

You can't disable mandatory rules.

Trellix releases new ATP rules in AMCore content. For information about the latest ATP content, see the Trellix TIE and ATP Security Content Release Notes.

For information about ATP rules, including rule IDs and their corresponding rule names and descriptions, see KB82925.

Task

1. Select **Menu** → **Reporting** → **Threat Event Log**.
2. Locate the rule in the **Threat Event Log**.
    a. Select **Actions** → **Choose Columns**, and add these columns.
        - **Threat Name**
        - **Rule ID**
    b. Click the **Threat Name** column to sort the contents.
    c. Note the rule ID associated with the threat name.
    Adaptive Threat Protection rules trigger threats that begin with "JTI/Suspect".

    For example, Rule ID 4 (**Use GTI file reputation to identify trusted or malicious files**) triggers `JTI/Suspect.196612!d18b4dc5c6db`.

    Note

    KB82925 includes alternative methods for identifying the rule.

3. (Optional) Navigate the Story Graph to see the details of events leading up to the detection.

4. Select **Menu** → **Server Settings** → **Adaptive Threat Protection**.
5. Click the tab that matches the rule group associated with the policy: **Productivity**, **Balanced**, or **Security**.
   To view or change the rule group assignment for the policy, see the **Rule Assignment** section in the Adaptive Threat Protection **Options** policy.
6. Click the **Rule ID** column to sort the contents.
7. Locate the rule ID noted in step 4.
8. If the triggered rule shows **False** in the **Mandatory** column, you can disable it or set it to report only.
   a. Click **Edit** in the bottom right.
   b. Select the rule checkbox.
   c. Select **Actions** → **Set Rule(s) to Disabled** or **Set Rule(s) to Observe**.
   d. Click **Save**.

Checking recent events for threats

You can look at recent events to see information about any identified threats to your systems.

You can view enforced or observed events:

- **Enforcement Events** — Events that occur as a result of an enforced Adaptive Threat Protection server policy.
- **Observation Events** — Events, such as `Would Block`, that indicate what the action would be if the policy were enforced. It allows you to view, evaluate, and adjust policy and configuration settings before enforcing them. You can see which files or certificates are causing events, and change their reputation settings so they no longer generate an event.

You can view threat events in several ways and drill down for more information:

Past 30 days — Event summary information for the past 30 days.

Top 10 — The top 10 events by system, file, or certificate.

Certificate — The certificate name, its SHA-1 hash value, and the number of certificates that were cleaned, contained, blocked, or prompted.

File Hash — The file name and SHA-1 hash value, and the number of files that were cleaned, contained, blocked, or prompted.

Rule — The rule name, events where the rule was applied, and the number of rules that were cleaned, contained, blocked, or prompted.

System — The system name, total events for that system, and the number of events that were cleaned, contained, blocked, or prompted on a particular system.

Examples

- You can then see details about the specific files or certificates that are causing the prompts. Select individual files or certificates from the Events page and change their reputation levels to allow or block them so that they no longer generate a prompt.

- If a specific file generates events, select it from the list on the **Events** page and see which systems tried to run it and what action was taken. You can then change the file's reputation so that it no longer generates events. For example, if the file generates a prompt and you want it blocked, change its reputation so that it is blocked and does not generate an event.

Check details about recent threat events

You can view information about recent files and certificates seen in your environment and the actions taken in response to an identified threat.

Task

1. Select **Menu** → **Reporting** → **Adaptive Threat Protection Events**.
   The **Adaptive Threat Protection Events** page shows several views of recent events.
2. In the **Select Event View** drop-down list, select the type of events to show.
   - **Enforcement Events** show enforced policy events and the actions taken.
   - **Observation Events** show the observed policy events, such as `Would Block`, where no action was taken.
3. Select a chart to see detailed information.
4. In the **Select Pivot Point** drop-down list, select how to view events: by certificate, file hash, rule, or system. Then, select a specific item in the list to see more details.

Respond to events

Adjust file and certificate reputations to prevent threats and other events. Use the information on the **Adaptive Threat Protection Events** page.

Task

1. Select **Menu** → **Reporting** → **Adaptive Threat Protection Events**.
   The **Adaptive Threat Protection Events** page shows the items that are generating events.
2. On the **Events** page, you can see the items that are generating events. Click an event to see its details.
3. If you selected a file or certificate that's causing a block or prompt based on its reputation, change its reputation setting to stop the event.

   Use the options on the **Actions** menu to change its reputation.

Using on a client system

Using the Trellix Endpoint Security (ENS) Client

How the Trellix Endpoint Security (ENS) Client works

The Trellix Endpoint Security (ENS) Client enables you to check the protection status and provides access to security features of installed software, such as scans, quarantined files, and event logs.

The Trellix Endpoint Security (ENS) Client provides:

- Access to features, such as viewing support links and logging on as an administrator.
- Quick access to frequent tasks, such as scanning your system and updating the software.
- Information about your protection, such as status, event logs, tasks, and quarantined files.
- **Threat Summary**, which gives you information about threats detected on your system in the last 30 days.

Open the Trellix Endpoint Security (ENS) Client

To display the status of the protection features installed on the computer, open the Trellix Endpoint Security (ENS) Client.

If the interface mode is set to **Lock client interface**, you must enter the administrator password to open the Trellix Endpoint Security (ENS) Client.

Task

1. Use one of these methods to display the Trellix Endpoint Security (ENS) Client:
    - Right-click the system tray icon, then select **Trellix Endpoint Security**.
    - Select **Start** → **All Programs** → **Trellix** → **Trellix Endpoint Security**.
    - On Windows 8 and 10, start the **Trellix Endpoint Security** app.
        - Press the **Windows** key.
        - Enter `Trellix Endpoint Security` in the search area, then double-click or touch the **Trellix Endpoint Security** app.
2. If prompted, enter the administrator password on the **Administrator Log On** page, then click **Log On**.

Results

The Trellix Endpoint Security (ENS) Client opens in the interface mode that the administrator configured.

Get information about your protection

You can get specific information about the software's protection, including management type, protection modules, features, status, version numbers, and licensing.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu  , select **About**.

3. Click the name of a module or feature on the left to jump to information about that item.
4. Click the browser **Close** button to close the **About** page.

Checking for threats

The Trellix Endpoint Security (ENS) Client **Status** page provides a real-time summary of any threats detected on your system in the last 30 days.

As new threats are detected, the **Status** page dynamically updates the data in the **Threat Summary** area in the bottom pane.

Note

The Trellix Endpoint Security (ENS) Client must be in the green state to display the **Threat Summary**.

The **Threat Summary** includes:

- Date of the last eliminated threat
- Top two threat vectors, by category
- Number of threats per threat vector

Note

If the Trellix Endpoint Security (ENS) Client can't reach the **Event Manager**, it displays a communication error message. To view the **Threat Summary**, restart the system.

Check the content date and version on a client system

To provide the best protection, Trellix ENS needs the latest content files to be installed on the system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **About**.
3. Verify that the content date matches today or yesterday's date.

Module	Field
Adaptive Threat Protection	Real Protect content date
Threat Prevention	AMCore content date

4. Verify that the **Threat Prevention Exploit Prevention content date** matches the latest content listed on the Trellix Exploit Prevention Security Content Releases page.

5. (Managed systems) Compare the content versions with the versions in the **Main Repository** in Trellix ePO - On-prem.

Update content and software manually

You can manually check for and download updated security files from the Trellix Endpoint Security (ENS) Client. Manual updates are called on-demand updates.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Update** to check for updates.
   If this button doesn't appear in the Trellix Endpoint Security (ENS) Client, you can enable it in the settings.
   If your endpoint is up to date, the page displays **No Updates Available** and the date and time of the last update.

   To cancel the update, click **Cancel**.

   - If the update completes successfully, the page displays **Update Finished** and the last update as **Today**.
   - If the update was unsuccessful, errors appear in the **Messages** area. View the PackageManager_Activity.log or PackageManager_Debug.log for more information.
3. Click **Close** to close the **Update** page.

Using Threat Prevention on a client system

Check the content date and version on a client system

To provide the best protection, Trellix ENS needs the latest content files to be installed on the system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **About**.
3. Verify that the content date matches today or yesterday's date.

Module	Field
Adaptive Threat Protection	**Real Protect content date**
Threat Prevention	**AMCore content date**

4. Verify that the **Threat Prevention Exploit Prevention content date** matches the latest content listed on the Trellix Exploit Prevention Security Content Releases page.
5. (Managed systems) Compare the content versions with the versions in the **Main Repository** in Trellix ePO - On-prem.

Update content and software manually

You can manually check for and download updated security files from the Trellix Endpoint Security (ENS) Client. Manual updates are called on-demand updates.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Update** to check for updates.
   If this button doesn't appear in the Trellix Endpoint Security (ENS) Client, you can enable it in the settings.
   If your endpoint is up to date, the page displays **No Updates Available** and the date and time of the last update.

   To cancel the update, click **Cancel**.

   - If the update completes successfully, the page displays **Update Finished** and the last update as **Today**.
   - If the update was unsuccessful, errors appear in the **Messages** area. View the PackageManager_Activity.log or PackageManager_Debug.log for more information.
3. Click **Close** to close the **Update** page.

Responding to prompts and threat detections

Respond to a scan prompt

When a scheduled on-demand scan is about to start, Trellix ENS might prompt you for input to continue. The prompt appears only if the scan is configured to allow you to defer, pause, resume, or cancel the scan.

If you don't select an option, the scan starts automatically.

If the scan is configured to run only the scan when the computer is idle, Trellix ENS displays a dialog when the scan is paused. If configured, you can also resume these paused scans or reset them to run only when you're idle.

Note

Windows 8 and 10 use toast notifications — messages that pop up to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

Task

At the prompt, select one of these options.

Note

The options that appear depend on how the scan is configured.

Scan Now	Starts the scan immediately.
View Scan	Views detections for a scan in progress.
Pause Scan	Pauses the scan. Depending on the configuration, clicking **Pause Scan** might reset the scan to run only when you're idle. Click **Resume Scan** to resume the scan where it left off.
Resume Scan	Resumes a paused scan.
Cancel Scan	Cancels the scan.
Defer Scan	Delays the scan for the specified number of hours. Scheduled scan options determine how many times that you can defer the scan for one hour. You might be able to defer the scan more than once.
Close	Closes the scan page.

If the scanner detects a threat, Trellix ENS might prompt you for input to continue, depending on how settings are configured.

Respond to a threat-detection prompt

When the scanner detects a threat, Trellix ENS might prompt you for input to continue, depending on how settings are configured.

Note

Windows 8 and 10 use toast notifications — messages that pop up to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

Task

From the **On-Access Scan** page, select options to manage threat detections.

Note

You can reopen the scan page to manage detections at any time.

The on-access scan detection list is cleared when the Trellix ENS service restarts or the system reboots.

View and respond to threats detected on a client system

Depending on how settings are configured, you can respond to threat detections from Trellix Endpoint Security (ENS) Client.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Scan Now** to open the **Scan System** page.
3. From **On-Access Scan**, click **View Detections**.

Note

This option isn't available if the list contains no detections or the user messaging option is disabled.

The on-access scan detection list is cleared when the Trellix ENS service restarts or the system reboots.

4. From the **On-Access Scan** page, select one of these options.

Clean	Attempts to clean the item (file, registry entry) and place it in the Quarantine. **Note:** Trellix ENS uses information in the content files to clean files. If the content file has no cleaner or the file has been damaged beyond repair, the scanner and denies access to it. In this case, Trellix recommends that you delete the file from the Quarantine and restore it from a clean backup copy.
Delete	Deletes the item that contains the threat.
Remove Entry	Removes the entry from the detection list.
Close	Closes the scan page.

Note

If an action isn't available for the threat, the corresponding option is disabled. For example, **Clean** isn't available if the file has already been deleted.

The on-access scan detection list is cleared when the Trellix ENS service restarts or the system reboots.

Manage quarantined items on a client system

You can delete quarantined items, restore or rescan them, or get more information about the threat.

For example, you might be able to restore an item after downloading a later version of the content that contains information that cleans the threat.

Quarantined items can include various types of scanned objects, such as files, registries, or anything that Trellix ENS scans for malware. Threat Prevention cleans or deletes items that are detected as threats and saves copies in a non-executable format to the Quarantine folder.

For information about malware detection names, see the Trellix Labs page.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Quarantine** on the left side of the page.
   The page shows any items in the Quarantine.

   Note

   If the Trellix Endpoint Security (ENS) Client can't reach the **Quarantine Manager**, it displays a communication error message. In this case, restart the system to view the **Quarantine** page.

3. Select an item from the top pane to display the details in the bottom pane.
4. On the **Quarantine** page, perform actions on selected items.

To...	Follow these steps
Delete items from the quarantine.	Select items, click **Delete**, then click **Delete** again to confirm. Deleted items can't be restored.
Restore items from the quarantine.	Select items, click **Restore**, then click **Restore** again to confirm. Trellix ENS restores items to the original location and removes them from the quarantine. If an item is still a valid threat, Trellix ENS returns it to the quarantine the next time the item is accessed.
Rescan items.	Select items, then click **Rescan**.

To...	Follow these steps
	For example, you might rescan an item after updating your protection. If the item is no longer a threat, you can restore the item to its original location and remove it from the quarantine.
View an item in the **Event Log**.	Select an item, then click the **View in Event Log** link in the details pane. The **Event Log** page opens, with the event related to the selected item highlighted.
Get more information about a threat.	Select an item, then click the **Learn more about this threat** link in the details pane. A new browser window opens to the Trellix Labs website with more information about the threat that caused the item to be quarantined.

How Threat Prevention provides maximum protection when rescanning quarantined items

When rescanning items in the quarantine, Threat Prevention uses scan settings designed to provide maximum protection.

Tip

Best practice: Always rescan items in the quarantine before restoring them. For example, you might rescan an item after updating your protection. If the item is no longer a threat, you can restore the item to its original location and remove it from the quarantine.

Between when a threat was originally detected and the rescan performed, scanning conditions can change, which can affect the detection of quarantined items.

When rescanning quarantined items, Threat Prevention always:

- Scans MIME-encoded files.
- Scans compressed archive files.
- Forces a Trellix GTI lookup on items.
- Sets the Trellix GTI sensitivity level to **Very high**.

Note

Even using these scan settings, the quarantine rescan might fail to detect a threat. For example, if the item's metadata (path or registry location) changes, rescanning might produce a false positive even though the item is still infected.

Scanning for threats

Scan a specific file or folder on a client system

You can immediately scan an individual file or folder that you suspect is infected by right-clicking on it in Windows Explorer.

The behavior of the **Right-Click Scan** depends on how the settings are configured.

Task

1. In Windows Explorer, right-click the file or folder to scan and select **Scan for threats** from the pop-up menu.
   Trellix Endpoint Security (ENS) Client displays the status of the scan in the **Scan for threats** page.
2. Click buttons at the top of the page to control the scan.

Pause Scan	Pauses the scan before it completes.
Resume Scan	Resumes a paused scan.
Cancel Scan	Cancels a running scan.

3. When the scan completes, the page displays the number of files scanned, time elapsed, and any detections.

Detection Name	Identifies the name of the detected malware.
Type	Displays the threat type.
File	Identifies the infected file.
Action Taken	Describes the last security action taken on the infected file: • **Access Denied** • **Cleaned** • **Deleted** • **None**

   The on-demand scan detection list is cleared when the next on-demand scan starts.

4. Select a detection in the table, then click **Clean** or **Delete** to clean or delete the infected file.

   Depending on the threat type and scan settings, these actions might not be available.

5. Click **Close** to close the page.

Scan susceptible areas on a client system

Run a **Quick Scan** on areas of a client system that are most susceptible to infection.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Scan System**.
3. On the **Scan System** page, click **Scan Now** for **Quick Scan**.
   If a scan is already in progress, the **Scan Now** button changes to **View Scan**.

   You might also see the **View Detections** button for the on-access scanner, depending on how settings are configured and whether a threat has been detected. Click this button to open the **On-Access Scan** page to manage detections at any time.

   Trellix Endpoint Security (ENS) Client displays the status of the scan on a new page.

   Tip

   Best practice: The **AMCore content creation date** indicates the last time the content was updated. If the content is more than two days old, update your protection before running the scan.

4. Click buttons at the top of the status page to control the scan.

Pause Scan	Pauses the scan before it completes.
Resume Scan	Resumes a paused scan.
Cancel Scan	Cancels a running scan.

5. When the scan completes, the page displays the number of files scanned, time elapsed, and any detections.

Detection Name	Identifies the name of the detected malware.
Type	Displays the threat type.
File	Identifies the infected file.
Action Taken	Describes the last security action taken on the infected file:

	• **Access Denied** • **Cleaned** • **Deleted** • **None**

The on-demand scan detection list is cleared when the next on-demand scan starts.

6. Select a detection in the table, then click **Clean** or **Delete** to clean or delete the infected file.

   Depending on the threat type and scan settings, these actions might not be available.

7. Click **Close** to close the page.

Scan a client system that might be infected

Run a **Full Scan** of a client system that you suspect is infected.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Scan System**.
3. On the **Scan System** page, click **Scan Now** for **Full Scan**.
   If a scan is already in progress, the **Scan Now** button changes to **View Scan**.

   You might also see the **View Detections** button for the on-access scanner, depending on how settings are configured and whether a threat has been detected. Click this button to open the **On-Access Scan** page to manage detections at any time.

   Trellix Endpoint Security (ENS) Client displays the status of the scan on a new page.

   Tip

   Best practice: The **AMCore content creation date** indicates the last time the content was updated. If the content is more than two days old, update your protection before running the scan.

4. Click buttons at the top of the status page to control the scan.

Pause Scan	Pauses the scan before it completes.
Resume Scan	Resumes a paused scan.
Cancel Scan	Cancels a running scan.

5. When the scan completes, the page displays the number of files scanned, time elapsed, and any detections.

Detection Name	Identifies the name of the detected malware.
Type	Displays the threat type.
File	Identifies the infected file.
Action Taken	Describes the last security action taken on the infected file: • **Access Denied** • **Cleaned** • **Deleted** • **None**

The on-demand scan detection list is cleared when the next on-demand scan starts.

6. Select a detection in the table, then click **Clean** or **Delete** to clean or delete the infected file.

   Depending on the threat type and scan settings, these actions might not be available.

7. Click **Close** to close the page.

Disable Trellix ENS scanners from the Trellix system tray

If configured, users can mitigate performance issues by temporarily disabling Trellix ENS scanners from the Trellix system tray icon. The scanners are reenabled at the next policy enforcement, based on settings in the policy.

Note

This option might not be available, depending on how the settings are configured.

Task

1. Right-click the Trellix system tray icon and select **Disable Endpoint Security Scanners** from the **Quick Settings** menu.

   On Windows 10 systems, when the on-access scanner is disabled, Windows Defender activates.

2. To reenable the scanners, either:
   - Wait for the next policy enforcement.
   - Right-click the Trellix system tray icon and select **Trellix Agent Status Monitor**. In the **Trellix Agent Monitor**, click **Enforce Policies**.

Using Firewall on a client system

Enable and disable Firewall from the Trellix system tray icon

Depending on how settings are configured, you can enable and disable Firewall from the Trellix system tray icon.

Before you begin

Make sure that you have selected the **Allow users to disable Firewall from the Trellix system tray icon** option in the Trellix ePO - On-prem Firewall Option policy.

Task

Right-click the Trellix system tray icon and click **Quick Settings** → **Disable Endpoint Security Firewall**.
When Firewall is enabled, the option to **Disable Endpoint Security Firewall** is active and vice versa.
If you have selected the **Require justification from users when managing Firewall from the Trellix system tray icon** option in the Trellix ePO - On-prem Firewall Option policy, you are prompted to provide your administrator with a reason for disabling Firewall.

Enable or view Firewall timed groups from the Trellix system tray icon

Enable, disable, or view Firewall timed groups from the Trellix system tray icon.

Note

These options might not be available, depending on how the settings are configured.

Task

Right-click the Trellix system tray icon and select an option from the **Quick Settings** menu.

- **Enable Firewall Timed Groups** — Enables timed groups for a set amount of time to allow access to the Internet before rules restricting access are applied. When timed groups are enabled, the option is **Disable Firewall Timed Groups**. Each time you select this option, you reset the time for the groups. Depending on settings, you might be prompted to provide the administrator with a reason for enabling timed groups.
- **View Firewall Timed Groups** — Displays the names of the timed groups and the amount of time remaining for each group to be active.

Using Web Control on a client system

Enable the Web Control plug-in from the browser on a client system

Depending on settings, you must manually enable the Web Control plug-in to be notified about web-based threats when browsing and searching.

Before you begin

The Web Control module must be enabled in the settings.

Plug-ins are also called extensions in Edge, Chromium Edge, Chrome, Internet Explorer, Firefox, and add-ons in Internet Explorer.

When you first start Edge, Chromium Edge, Internet Explorer, Chrome, or Firefox you might be prompted to enable plug-ins. For the latest information, see KB87568.

Task

Depending on the browser, enable the plug-in.

Edge	If the Web Control extension isn't enabled automatically: a. From the menu, select **Extensions**. b. Click the **Endpoint Security Web Control** toggle switch to **On**.
Chromium Edge	When prompted, click **Enable extension**. If Chromium Edge doesn't prompt you to enable the Web Control extension, enable it manually: a. From the menu, select **Extensions**. b. Click the **Endpoint Security Web Control** toggle switch to **On**.
Chrome	If Chrome doesn't prompt you to enable the Web Control plug-in, enable it manually: a. Click **Settings** → **Extensions**. b. Click **Enable** to activate Web Control.
Firefox	If Firefox doesn't prompt you to enable the Web Control add-on, enable it manually: a. From the menu, select **Add-ons** → **Extensions**. b. Click **Enable** to activate Web Control.
Internet Explorer	• When prompted, click **Enable**. • If more than one plug-in is available, click **Choose add-ons**, then click **Enable** for the Web Control toolbar.

	• To enable it manually, from the menu, select **Manage Add-ons**, select **Endpoint Security Web Control**, then click **Enable**. **Note:** In Internet Explorer, if you disable the Web Control toolbar, you are prompted to also disable the Web Control plug-in. If policy settings prevent uninstalling or disabling the plug-in, the Web Control plug-in remains enabled even though the toolbar isn't visible.

Get information about a site that you're viewing

You can get information about a site using the Web Control button on the browser. The button works differently depending on the browser.

Before you begin

- The Web Control module must be enabled.
- The Web Control plug-in must be enabled in the browser.
- The **Hide the toolbar on the client browser** option in the **Options** settings must be disabled.

Task

1. (Internet Explorer only) Display a summary of the safety rating for the site: Hover the cursor over the button in the browser.
2. Display the menu:

Edge	Click the  button in the address bar.
Chrome	
Firefox	
Internet Explorer	Click the button in the toolbar.

3. Display details about the site, including analysis results, rating, and category:
   a. Select **View Site Report** from the menu.
      The **McAfee Threat Center** page opens in another browser window.
   b. From **Search the Library**, select **Website URL / Address**.
   c. Enter the site name and click **Go**.

Get information about a site from search results

You can get detailed information about a site, including rating and category, from the search results page.

Task

1. Hover the cursor over the safety icon, such as  .
   A balloon displays a high-level summary of the safety report for the site.
2. Display details about the site, including analysis results, rating, and category:
   a. Click **View Site Report** in the balloon.
      The **McAfee Threat Center** page opens in another browser window.
   b. From **Search the Library**, select **Website URL / Address**.
   c. Enter the site name and click **Go**.

Using Adaptive Threat Protection on a client system

Check the content date and version on a client system

To provide the best protection, Trellix ENS needs the latest content files to be installed on the system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu  , select **About**.
3. Verify that the content date matches today or yesterday's date.

Module	Field
Adaptive Threat Protection	Real Protect content date
Threat Prevention	AMCore content date

4. Verify that the **Threat Prevention Exploit Prevention content date** matches the latest content listed on the Trellix Exploit Prevention Security Content Releases page.
5. (Managed systems) Compare the content versions with the versions in the **Main Repository** in Trellix ePO - On-prem.

Update content and software manually

You can manually check for and download updated security files from the Trellix Endpoint Security (ENS) Client. Manual updates are called on-demand updates.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Update** to check for updates.
   If this button doesn't appear in the Trellix Endpoint Security (ENS) Client, you can enable it in the settings.

If your endpoint is up to date, the page displays **No Updates Available** and the date and time of the last update.

To cancel the update, click **Cancel**.

- If the update completes successfully, the page displays **Update Finished** and the last update as **Today**.
- If the update was unsuccessful, errors appear in the **Messages** area. View the PackageManager_Activity.log or PackageManager_Debug.log for more information.

3. Click **Close** to close the **Update** page.

Respond to a file-reputation prompt

When a file with a specific reputation tries to run on your system, Adaptive Threat Protection might prompt you for input to continue. The prompt appears only if Adaptive Threat Protection is installed and configured to prompt.

Note

Adaptive Threat Protection depends on the Trellix system tray icon to display prompts. On systems accessed only by RDP, the system tray icon doesn't start and prompts don't appear. To work around this issue, add the UpdaterUI.exe to the logon script. See KB83532.

The administrator configures the reputation threshold, at which point, a prompt is displayed. For example, if the reputation threshold is **Unknown**, Trellix ENS prompts you for all files with an unknown reputation and below.

If you don't select an option, Adaptive Threat Protection takes the default action configured by the administrator.

The prompt, timeout, and default action depend on how Adaptive Threat Protection is configured.

Note

Windows 8 and 10 use toast notifications — messages that pop up to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

Task

1. (Optional) At the prompt, enter a message to send to the administrator.
   For example, use the message to describe the file or explain your decision to allow or block the file on your system.
2. Click **Allow** or **Block**.

Allow	Allows the file.
Block	Blocks the file on your system.

To instruct Adaptive Threat Protection not to prompt for the file again, select **Remember this decision**.

Results

Adaptive Threat Protection acts, based on your choice or the default action, and closes the prompt window.

Disable Trellix ENS scanners from the Trellix system tray

If configured, users can mitigate performance issues by temporarily disabling Trellix ENS scanners from the Trellix system tray icon. The scanners are reenabled at the next policy enforcement, based on settings in the policy.

Note

This option might not be available, depending on how the settings are configured.

Task

1. Right-click the Trellix system tray icon and select **Disable Endpoint Security Scanners** from the **Quick Settings** menu.

   On Windows 10 systems, when the on-access scanner is disabled, Windows Defender activates.

2. To reenable the scanners, either:
   - Wait for the next policy enforcement.
   - Right-click the Trellix system tray icon and select **Trellix Agent Status Monitor**. In the **Trellix Agent Monitor**, click **Enforce Policies**.

Restore quarantined objects on a client system

Restoring objects from the quarantine replaces all objects that the convicted processes created, changed, or deleted, and the files associated with those processes, on the system where they were before the **Clean** action occurred.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Quarantine** on the left side of the page.
   The page shows any items in the Quarantine.

   Note

   If the Trellix Endpoint Security (ENS) Client can't reach the **Quarantine Manager**, it displays a communication error message. In this case, restart the system to view the **Quarantine** page.

3. Select an item from the top pane to display the details in the bottom pane.
4. Select objects, click **Restore**, then click **Restore** again to confirm.

   Trellix ENS restores items to the original location and removes them from the quarantine. If an item is still a valid threat, Trellix ENS returns it to the quarantine the next time the item is accessed.

5. On the **Quarantine** page, you can also perform these actions on objects in the quarantine.

Note

The **Rescan** button doesn't apply to objects quarantined by ATP.

To...	Follow these steps
Delete items from the quarantine.	Select items, click **Delete**, then click **Delete** again to confirm. Deleted items can't be restored.
View an item in the **Event Log**.	Select an item, then click the **View in Event Log** link in the details pane. The **Event Log** page opens, with the event related to the selected item highlighted.
Get more information about a threat.	Select an item, then click the **Learn more about this threat** link in the details pane. A new browser window opens to the Trellix Labs website with more information about the threat that caused the item to be quarantined.

6. After restoring a Windows service, reboot the client system to complete the restore.

Check connection status

To determine whether Adaptive Threat Protection on the client system gets file reputations from TIE server or Trellix GTI , you can check the Trellix Endpoint Security (ENS) Client **About** page.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu , select **About**.
3. Click Adaptive Threat Protection on the left.

   The **Connection status** field indicates one of the following for Adaptive Threat Protection:

   - **Threat Intelligence Connectivity** — Connected to TIE server for enterprise-level reputation information.
   - **Trellix GTI Connectivity only** — Connected to Trellix GTI for global-level reputation information.
   - **Disconnected** — Not connected to TIE server or Trellix GTI . Adaptive Threat Protection determines the file reputation using information on the local system.

Managing on a client system

Managing common features on a client system

Log on as administrator

You can log on to the Trellix Endpoint Security (ENS) Client as administrator to enable and disable features and configure settings.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Standard access**.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **Administrator Logon**.
3. In the **Password** field, enter the administrator password, then click **Log On**.

Results

You can now access all features of the Trellix Endpoint Security (ENS) Client.

To log off, select **Action** → **Administrator Logoff**. The client returns to **Standard access** interface mode.

Disable and enable features

As an administrator, you can disable and enable Trellix ENS features from the Trellix Endpoint Security (ENS) Client.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Note

The **Status** page shows the enabled status of the module, which might not reflect the actual status of features. You can see the status of each feature in the **Settings** page. For example, if the **Enable ScriptScan** setting isn't successfully applied, the status might be **(Status: Disabled)**.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click the module name on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click the module name on the **Settings** page.
3. Select or deselect the **Enable** *module* or *feature* option.

Protect services and files on a client system

One of the first things that malware attempts to do during an attack is to disable your system security software. To prevent services and files from being stopped or modified, configure Self Protection.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

⚠ Caution

Disabling Self Protection leaves your system vulnerable to attack.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu , select **Settings**.
3. Click **Show Advanced**.
4. From **Self Protection**, verify that **Self Protection** is enabled.
5. Specify the action for each of the following resources:
    - **Files and folders** — Prevents users from changing the Trellix database, binaries, safe search files, and configuration files.
    - **Registry** — Prevents users from changing the Trellix registry hive, COM components, and uninstalling using the registry value.
    - **Processes** — Prevents stopping Trellix processes.
6. Click **Apply**.

Set up logging for client activity on a client system

You can configure activity, debug, and event logging, which you can use to determine if you need to change settings to enhance protection or improve system performance.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu , select **Settings**.
3. Click **Show Advanced**.
4. Configure **Client Logging** settings on the page.

    For more information about the **Client Logging** settings, see Advanced options in the *Trellix Endpoint Security (ENS)10.7.x Interface Reference Guide*.

5. Click **Apply**.

Control access to the client interface on a client system

You can set a password to control access to the Trellix Endpoint Security (ENS) Client.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Caution

Client Interface Mode is set to **Full access** by default, allowing users to change their security configuration, which can leave systems unprotected from malware attacks.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **Settings**.
3. Configure **Client Interface Mode** settings on the page.
   Best practice: To improve security, change **Client Interface Mode** to **Standard** or **Lock client interface**. Both of these options require an Administrator password to access Trellix Endpoint Security (ENS) Client settings.
4. Click **Apply**.

Restricting and allowing access to features

Client Interface Mode settings assigned to your computer determine which features you can access.

Change the **Client Interface Mode** in the Common settings.

Note

For managed systems, policy changes from Trellix ePO - On-prem might overwrite changes from the **Settings** page.

These are the **Client Interface Mode** options.

Full access	Enables access to all features, including: • Enable and disable individual modules and features. • Access the **Settings** page to view or modify all settings for the Trellix Endpoint Security (ENS) Client. (Default)

Standard access	Displays protection status and allows access to most features. • Update the content files and software components on your computer (if enabled by the administrator). • Perform a thorough check of all areas of your system, which is recommended if you suspect your computer is infected. • Run a quick (2-minute) check of the areas of your system most susceptible to infection. • Access the **Event Log**. • Manage items in the **Quarantine**. From **Standard access** interface mode, you can log on as administrator to access all features, including all settings.
Lock client interface	Requires a password to access the client. Once you unlock the client interface, you can access all features.

Note

If you can't access the Trellix Endpoint Security (ENS) Client or specific tasks and features that you need to do your job, talk to your administrator.

Unlock the client interface on a client system

If the Trellix Endpoint Security (ENS) Client interface is locked, unlock it with the administrator password to access all settings.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Lock client interface**.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. On the **Administrator Log On** page, enter the administrator password in the **Password** field, then click **Log On**.
   The Trellix Endpoint Security (ENS) Client opens and you can now access all features of the client.
3. Log off and close the client: from the **Action** menu , select **Administrator Logoff**.

Configure proxy server settings on a client system

You can specify proxy server options to redirect web traffic to a proxy server.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu , select **Settings**.
3. Click **Show Advanced**.
4. Configure **Proxy Server** settings on the page.
   Best practice: Exclude the Trellix GTI addresses from the proxy server. For information, see KB79640.
5. Click **Apply**.

Keeping your protection up to date

You can get updated security files manually or automatically.

For example, you might want to update manually to apply an emergency fix to a new threat or include the latest content after a new installation.

Automatic updates

Use the Default Client Update task to automatically update security files. The task updates all content and software. By default, the **Default Client Update** task runs every day at 1:00 a.m. and repeats every four hours until 11:59 p.m.

Manual updates

Manual update methods include:

Update button

From the Trellix Endpoint Security (ENS) Client, immediately download the latest content or software, or both according to settings. You can configure the visibility and behavior of the **Update** button in the Common settings.

Update Security option

From the Trellix system tray icon, update content and software.

Command line

From the client system, run a command to update the AMCore content.

Configure automatic updates for the client

Configure where the client gets its updates

You can configure the sites from which the Trellix Endpoint Security (ENS) Client gets updated security files.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **Settings**.
3. Click **Show Advanced**.
4. From **Common**, click **Options**.
5. Configure **Source Sites for Updates** settings on the page.

   You can enable and disable the default backup source site, **McAfeeHttp**, and the management server, but you can't otherwise modify or delete them.

   You can add, change, import, or export a source site.

   Note

   The order of the sites determines the order Trellix ENS uses to search for the update site.

6. Click **Apply**.

Configure default behavior for updates from the client

You can specify the default behavior for updates initiated from the Trellix Endpoint Security (ENS) Client.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Use these settings to:

- Show or hide the **Update** button in the client.
- Specify what to update when the user clicks the button or the **Default Client Update** task runs.

By default, the **Default Client Update** task runs every day at 1:00 a.m. and repeats every four hours until 11:59 p.m.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **Settings**.
3. Click **Show Advanced**.
4. Configure **Default Client Update** settings on the page.
5. Click **Apply**.

Configure, schedule, and run update tasks from the client

You can configure custom update tasks, or change the **Default Client Update** task schedule.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Use these settings to configure from the client when the **Default Client Update** task runs. You can also configure the default behavior for client updates initiated from the Trellix Endpoint Security (ENS) Client.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu , select **Settings**.
3. Click **Show Advanced**.
4. From **Common**, click **Tasks**.
5. Configure the update task settings on the page.
   You can add, customize, and run an update task. You can also create a copy of an update task and change the schedule.
6. Click **Apply**.

Configure, schedule, and run mirror tasks

You can use mirror tasks to replicate the update files from the first accessible repository, defined in the repository list, to a mirror site on your network.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu , select **Settings**.
3. Click **Show Advanced**.
4. From **Common**, click **Tasks**.
5. Configure the mirror task settings on the page.
   You can add, change, copy, schedule, and run a mirror task.
6. Click **Apply**.

Allow certificate authentication on a client system

Certificates allow a vender to run code within Trellix processes.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu , select **Settings**.
3. Click **Show Advanced**.
4. In the **Certificates** section, select **Allow**.

Caution

This setting might result in compatibility issues and reduced security.

5. Click **Apply**.

Results

The certificate information appears in the table.

Managing Threat Prevention on a client system

Handling new malware with Extra.DAT files on a client system

When new malware is discovered and extra detection is required, Trellix Labs releases an Extra.DAT file. Extra.DAT files contain information that Threat Prevention uses to handle the new malware.

Threat Prevention supports using only one Extra.DAT file at a time. In a situation where you need both a positive Extra.DAT file for Threat Prevention and a negative Extra.DAT for Adaptive Threat Protection, you can request a combined file from Trellix Labs.

Each Extra.DAT file has an expiration date built in. When the Extra.DAT file is loaded, this expiration date is compared against the build date of the AMCore content installed on the system. If the build date of the AMCore content is newer than the Extra.DAT expiration date, the Extra.DAT is considered expired. It is no longer loaded and used by the engine. During the next update, the Extra.DAT is removed from the system.

If the next update of AMCore content includes information in the Extra.DAT, the Extra.DAT is removed.

Trellix ENS stores Extra.DAT files in the c:\Program Files\Common Files\McAfee\Engine\content\avengine\extradat folder.

Download and load an Extra.DAT file on a client system

In a major malware outbreak, you must load an Extra.DAT file to protect client systems until the next scheduled content update. You might need to load an Extra.DAT file on client systems to suppress detections that are considered false positives until the next scheduled content update.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Download the Extra.DAT file.
    a. Click the download link supplied by Trellix Labs, specify a location to save the Extra.DAT file, then click **Save**.
    b. If needed, unzip the EXTRA.ZIP file.
2. Open the Trellix Endpoint Security (ENS) Client.
3. From the **Action** menu, select **Load Extra.DAT**.
4. Click **Browse**, navigate to the location where you downloaded the Extra.DAT file, then click **Open**.
5. Click **Apply**.

Results

The new detections in the Extra.DAT take effect immediately.

Change the AMCore content version on a client system

To change the version of AMCore content on the client system, use Trellix Endpoint Security (ENS) Client.

Trellix ENS stores the currently loaded content file and the previous two versions in the Program Files\Common Files\McAfee\Engine\content folder. If needed, you can revert to a previous version.

Note

Exploit Prevention content updates cannot be rolled back.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **Roll Back AMCore Content**.
3. From the drop-down, select the version to load.
4. Click **Apply**.

Results

The detections in the loaded AMCore content file take effect immediately.

Specify quarantine location and retention time on a client system

You can configure the location of the quarantine folder and how long to keep quarantined items.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Quarantined items can include various types of scanned objects, such as files, registries, or anything that Trellix ENS scans for malware. Threat Prevention cleans or deletes items that are detected as threats and saves copies in a non-executable format to the Quarantine folder. You can delete quarantined items, restore or rescan them, or get more information about the threat. For

example, you might be able to restore an item after downloading a later version of the content that contains information that cleans the threat.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu , select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. Configure settings on the page, then click **Apply**.

Preventing threats from accessing systems

The first line of defense against malware is to protect your client systems from threats. Access Protection protects files, registry keys, registry values, processes, and services. Exploit Prevention prevents buffer overflow, illegal API use, and network exploits.

Trellix delivers Trellix-defined signatures in Exploit Prevention content updates. When the content file is updated, the signatures are updated if needed.

Access protection

Access protection prevents unwanted changes to client systems by restricting access to specified files, shares, registry keys, registry values, and preventing or restricting processes and services from executing threat behavior. .

Access protection uses both Trellix-defined rules (signatures) and user-defined rules (also called custom rules) to report or block access to items. Access Protection compares a requested action against the list of rules and acts according to the rule.

You can also create Expert Rules to restrict access to files, registry keys, registry values, processes, and services, using Trellix-provided syntax templates.

You can create expert rules to stop buffer overflow and illegal API use exploits.

Note

With Microsoft Window 8.1 and later, Access Protection rules no longer support operations for the **Services** subrule type. This is because Microsoft made services.exe a protected process in Windows 8.1 and later.

Buffer Overflow and Illegal API Use

Buffer overflow protection stops exploited buffer overflows from executing arbitrary code. This technology monitors applications in the application protection list and uses signatures in the Exploit Prevention content file to protect those applications. Exploit Prevention monitors user-mode API calls and recognizes when they are called as a result of a buffer overflow.

Illegal API use monitors the Windows Application Programming Interface (API) and protects against malicious API calls being made by unknown or compromised applications running on the system.

You can create Expert Rules to stop buffer overflow and illegal API use exploits, using Trellix-provided syntax templates.

You can create expert rules to stop buffer overflow and illegal API use exploits.

You can view Buffer Overflow and Illegal API Use events in Trellix ePO - On-prem on the **Exploit Prevention Events** page under **Reporting**.

Network IPS

Network Intrusion Prevention (Network IPS) protects against network denial-of-service attacks and bandwidth-oriented attacks that deny or degrade network traffic. Network IPS examines all data that flows between the client system and the rest of the network and compares it to the Trellix Network IPS signatures. When an attack is identified, the offending data is discarded or blocked from passing through the system.

You can't create Network IPS custom rules or Expert Rules.

Note

Host Intrusion Prevention 8.0 can be installed on the same system as Trellix ENS version 10.7. If the **Host IPS** or **Network IPS** options in McAfee Host IPS are enabled, **Exploit Prevention** and **Network Intrusion Prevention** are disabled even if enabled in the Threat Prevention settings.

Protect files, registry, processes, and services with Access Protection rules on a client system

Change the behavior of Trellix-defined rules or create custom rules to protect your system access points.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Tip

Best practice: For information about creating Access Protection rules to protect against ransomware, see KB89335, and KB89540.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Exploit Prevention**.
5. Change a Trellix-defined rule: In the **Rules** section, double-click the rule.
   a. On the **Edit Trellix-defined Rule** page, configure the settings.
   b. In the **Executables** section, click **Add**, configure the settings, then click **Save** twice to save the rule.
6. Create a custom rule: In the **Rules** section, click **Add**.
   a. On the **Add Rule** page, configure the settings.

b. In the **Executables** section, click **Add**, configure executable properties, then click **Save**.

The executable is the process that performs the subrule operation on the subrule target.

An empty **Executables** table indicates that the rule applies to all executables.

c. In the **User Names** section, click **Add**, then configure user name properties.
An empty **User Names** table indicates that the rule applies to all users.

d. In the **Subrules** section, click **Add**, then configure subrule properties.

Note

With Microsoft Window 8.1 and later, Access Protection rules no longer support operations for the **Services** subrule type. This is because Microsoft made services.exe a protected process in Windows 8.1 and later.

e. In the **Targets** section, click **Add**, configure target information, then click **Save** twice.

7. Specify the behavior of the rule: In the **Rules** section, select **Block**, **Report**, or both for the rule.
   - To block or report all, select **Block** or **Report** in the first row.
   - To disable the rule, deselect both **Block** and **Report**.
8. Click **Apply**.

Prevent Access Protection from blocking trusted programs on a client system

If a trusted program is blocked, you can exclude the process by creating a policy-based or rule-based exclusion.

Note

Access Protection exclusions don't apply to the Windows **Services** subrule type.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Exploit Prevention**.
5. Perform one of the following:

To...	Do this...
Exclude items from all rules.	a. In the **Exclusions** section, click **Add** to add items to exclude from all rules. b. On the **Add Executable** page, configure the executable properties.

To...	Do this...
	c. Click **Save**, then click **Apply** to save the settings.
Specify processes for inclusion or exclusion in a user-defined rule.	a. Edit an existing user-defined rule or add a rule. b. On the **Add Rule** or **Edit Rule** page, in the **Executables** section, click **Add** to add an executable to exclude or include. c. On the **Add Executable** page, configure the executable properties, including whether to include or exclude the executable. d. Click **Save** twice, then click **Apply** to save the settings.

Configure Exploit Prevention settings to block threats on a client system

To prevent applications from executing arbitrary code on the client system, you can configure the Exploit Prevention exclusions, default signatures, and application protection rules.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

You can set the action for Trellix-defined signatures. You can enable, disable, delete, and change the inclusion status of Trellix-defined application protection rules. You can also create and duplicate your own application protection rules. Any changes you make to these rules persist through content updates.

For the list of processes protected by Exploit Prevention, see KB58007.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Exploit Prevention**.
5. Configure settings on the page, then click **Apply**.

Exclude items from Exploit Prevention protection on a client system

If Exploit Prevention blocks a trusted program, you can add an exclusion for the process name. For Buffer Overflow and Illegal API Use, you can also exclude by caller module, API or signature ID. For Network IPS, you can exclude by signature ID or IP address. For Services, you can exclude by service name. For Files- Processes – Registry, you can exclude by signature ID.

Note

Upgrade to the latest version of endpoint security to exclude Files- Processes – Registry by signature ID. Otherwise, the exclusion gets added to the global exclusion list.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu , select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Exploit Prevention**.
5. Perform one of the following:

To...	Do this...
Exclude items from all rules.	a. In the **Exclusions** section, click **Add** to add items to exclude from all rules. b. On the **Add Exclusion** page, , select the exclusion type, then configure the exclusion properties. c. Click **Save**, then click **Apply** to save the settings.
Specify processes for inclusion or exclusion in a user-defined Application Protection rule. (*Buffer overflow and illegal API violations only*)	a. Edit an existing user-defined rule or add an Application Protection rule. b. On the **Add Rule** or **Edit Rule** page, in the **Executables** section, click **Add** to add executables to exclude or include. c. On the **Add Executable** page, configure the executable properties. d. Click **Save** twice, then click **Apply** to save the settings.

The signer distinguished name (SDN) is required when you enable a digital signature check and exclude only files signed by a specified process signer.

Task

1. Right-click an executable and select **Properties**.
2. On the **Digital Signatures** tab, select a signer and click **Details**.
3. On the **General** tab, click **View Certificate**.
4. On the **Details** tab, select the **Subject** field.
   The SDN appears.

   For example, Firefox has this SDN:

   CN = Mozilla Corporation

   OU = Release Engineering

   O = Mozilla Corporation

   L = Mountain View

   S = California

   C = US

   Note

   The SDN fields appear in reverse order from the required format.

5. Copy the contents of the **Subject** field to a temporary location.
6. Edit the information to reverse the order of the elements, remove line breaks, and separate the elements with commas.

   For example, the SDN required format is:

   ```
   C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION
   ```

7. When creating exclusions, copy and paste the certificate details as a single line of text to the **Signed by** field.

Scanning for threats on client computers

Types of scans

You can set up your systems to scan files on access automatically and on demand manually or on a schedule.

Threat Prevention **Options** includes settings that apply to all scan types.

- **On-access scan** — Configure the on-access scanner in the **On-Access Scan** settings. When files, folders, and programs are accessed, the on-access scanner intercepts the operation and scans the item, based on criteria defined in the settings.
- **On-demand scan**

Manual	Run a predefined on-demand scan at any time from the Trellix Endpoint Security (ENS) Client by clicking **Scan System**, then selecting a scan type. ▫ **Quick Scan** runs a quick check of the areas of the system most susceptible to infection. ▫ **Full Scan** performs a thorough check of all areas of the system. (Recommended if you suspect the computer is infected.)	Configure the behavior of full and quick scans in the **On-Demand Scan** settings.
	Scan an individual file or folder at any time from Windows Explorer by right-clicking the file or folder and selecting **Scan for threats** from the pop-up menu.	Configure the behavior of the **Right-Click Scan** in the **On-Demand Scan** settings.
	Run a custom on-demand scan as administrator from the Trellix Endpoint Security (ENS) Client: ▫ Select **Settings** → **Common** → **Tasks**. ▫ Select the task to run. ▫ Click **Run Now**. **Tip: Best practice:** Use manual custom on-demand scans to associate a scan task with a reaction, such as a malware infection.	Configure custom scans in the Common **Tasks** settings.
Scheduled	When a scheduled on-demand scan is about to start, Trellix	

	ENS displays a scan prompt at the bottom of the screen. You can start the scan immediately or defer the scan, if configured.	
	Schedule the predefined on-demand scans in the **Settings** → **Common** → **Tasks** settings. ▫ **Quick Scan** — By default, the **Quick Scan** is enabled and scheduled to run every day at 7 p.m. ▫ **Full Scan** — By default, the **Full Scan** is enabled and scheduled to run every Wednesday at 12 midnight. **Tip: Best practice:** Use the weekly **Full Scan** to supplement the continuous protection of the on-access scan. The full scan includes fewer exclusions and actively checks all files for malicious code. Check the OnDemandScan_Activity log file for scan statistics, such as start time, end time, and time to complete the scan. From the **Event Log** page in Trellix Endpoint Security (ENS) Client, click **View Logs Folder**. Most recent scan tasks activity appears at the bottom of the file.	Configure the behavior of full and quick scans in the **On-Demand Scan** settings.
	Schedule custom on-demand scans in the Common **Tasks** settings.	Configure custom scans in the Common **Tasks** settings.

	Tip: Best practice: Use scheduled custom on-demand scans for targeted scans, such as daily memory scans.	

Configure settings for all scans on a client system

Threat Prevention settings that apply to all on-access scans and on-demand scans include the quarantine location and potentially unwanted programs.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

These settings apply to all scans:

- Quarantine location and the number of days to keep quarantined items before automatically deleting them
- Detection names to exclude from scans, including buffer exclusions and command-line suppression for AMSI scanning
- Potentially unwanted programs to detect, such as spyware and adware
- Trellix GTI -based telemetry feedback

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. Configure settings on the page, then click **Apply**.

Define which potentially unwanted programs to detect on a client system

You can specify programs that you want the on-access scanner and on-demand scanner to treat as unwanted programs.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Note

The scanners detect the programs you specify and programs specified in the AMCore content files.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. From **Potentially Unwanted Program Detections**:
   - Click **Add** to specify the name and optional description of a file or program to treat as a potentially unwanted program.

     Note

     The **Description** appears as the detection name when a detection occurs.

   - Double-click the name or description of an existing potentially unwanted program to change.
   - Select an existing potentially unwanted program, then click **Delete** to remove it from the list.

Enable potentially unwanted program detection on a client system

You can enable the on-access and on-demand scanners to detect potentially unwanted programs and specify responses when one is found.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Configure **On-Access Scan** settings.
   a. Open the Trellix Endpoint Security (ENS) Client.
   b. Click **Threat Prevention** on the main **Status** page.
      Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
   c. Click **Show Advanced**.
   d. Click **On-Access Scan**.
   e. Under **Process Settings**, for each **On-Access Scan** type, select **Detect unwanted programs**.
   f. Under **Actions**, configure responses to unwanted programs.
2. Configure **On-Demand Scan** settings.
   a. Open the Trellix Endpoint Security (ENS) Client.
   b. Click **Threat Prevention** on the main **Status** page.
      Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
   c. Click **Show Advanced**.
   d. Click **On-Demand Scan**.
   e. For each scan type (**Full Scan**, **Quick Scan**, and **Right-Click Scan**):

- Select **Detect unwanted programs**.
- Under **Actions**, configure responses to unwanted programs.

Configure scans that run automatically when files are accessed on a client system

On-access scan configuration includes settings based on process type, and defining messages to send when a threat is detected.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu , select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **On-Access Scan**.
5. Select **Enable On-Access Scan** to enable the on-access scanner and change options.
6. Specify whether to use Standard settings for all processes, or different settings for high-risk and low-risk processes.
   - **Use Standard settings for all processes** — Configure the scan settings on the **Standard** tab.
   - **Configure different settings for High Risk and Low Risk processes** — Select the tab (**Standard**, **High Risk**, or **Low Risk**) and configure the scan settings for each process type.
7. Click **Apply**.

Configure Threat Prevention with no connection to Trellix GTI on a client system

For systems with no network connection to Adaptive Threat Protection, such as air-gapped systems, you can improve performance by manually disabling Adaptive Threat Protection.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Note

Policy changes from Trellix ePO - On-prem overwrite changes from the **Settings** page.

Disable Adaptive Threat Protection to eliminate unnecessary attempts to connect to Adaptive Threat Protection when no network path exists and reduce the impact on Trellix ENS performance.

Caution

Disabling Adaptive Threat Protection might result in increased false positives.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. In the **On-Access Scan**, **Trellix GTI** section, deselect **Enable Trellix GTI**.
4. Click **Show Advanced**.
5. Click **Apply**.

Configure, schedule, and run scans on a client system

Schedule the default full and quick scans or create and schedule custom scans from the Trellix Endpoint Security (ENS) Client in the Common **Options Tasks** settings.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. From the **Action** menu, select **Settings**.
3. Click **Show Advanced**.
4. From **Common**, click **Tasks**.
5. Configure settings on the page.

To...	Follow these steps
Create a custom scan.	a. Click **Add**. b. Enter the name, select **Custom scan** from the drop-down list, then click **Next**. c. Configure the scan settings and schedule, then click **OK** to save the scan.
Change the settings for a scan.	• Double-click the scan, make your changes, then click **OK** to save the scan. To change settings for quick and full scans, navigate to Threat Prevention settings, **On-Demand Scan** → **Advanced**, then click the appropriate tab.
Change the schedule for a quick or full scan.	a. Double-click **Quick Scan** or **Full Scan**. b. Click the **Schedule** tab, change the schedule, then click **OK** to save the settings.

To...	Follow these steps
	By default, the **Quick Scan** is enabled and scheduled to run every day at 7 p.m. By default, the **Full Scan** is enabled and scheduled to run every Wednesday at 12 midnight.
Remove a custom scan.	• Select the scan, then click **Delete**.
Create a copy of a scan.	a. Select the scan, then click **Duplicate**. b. Enter the name, configure the settings, then click **OK** to save the scan.
Run a scan.	• Select the task, then click **Run Now**. If the task is already running, including paused or deferred, the button changes to **View**.

Configure predefined scans that can be run manually or scheduled on a client system

You can configure the behavior of three predefined on-demand scans: **Quick Scan**, **Full Scan**, and **Right-Click Scan**.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Best practice: For best practices for configuring on-demand scans, see KB74059.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **On-Demand Scan**.
5. Click a tab to configure settings for the specified scan.
   - **Quick Scan**
   - **Full Scan**
   - **Right-Click Scan**
6. Configure settings on the page, then click **Apply**.

Best practices: Reducing the impact of on-demand scans on users on a client system

To minimize the impact that on-demand scans have on a system, you can select options to avoid impacting system performance and scan only what you need to.

Tip

Best practice: For suggestions on how to improve Trellix ENS performance, see KB88205.

Scan only when the system is idle

The easiest way to make sure that the scan has no impact on users is to run the on-demand scan only when the computer is idle.

When this option is enabled, Threat Prevention pauses the scan when it detects disk or user activity, such as access using the keyboard or mouse. Threat Prevention resumes the scan when the user hasn't accessed the system for three minutes.

You can optionally:

- Allow users to resume scans that have been paused due to user activity.
- Return the scan to run only when the system is idle.

Disable this option only on server systems and systems that users access using Remote Desktop Connection (RDP). Threat Prevention depends on the Trellix notification area icon to determine if the system is idle. On systems accessed only by RDP, the notification area icon doesn't start and the on-demand scanner never runs. To work around this issue, add the UpdaterUI.exe to the logon script.

Select **Scan only when the system is idle** in the **Performance** section of the **Scan Task Settings** tab.

Pause scans automatically

To improve performance, you can pause on-demand scans when the system is running on battery power. You can also pause the scan when an application, such as a browser, media player, or presentation, is running in full-screen mode. The scan resumes immediately when the system is connected to power or is no longer in full-screen mode.

- **Do not scan when the system is on battery power**
- **Do not scan when the system is in presentation mode** (available when **Scan anytime** is enabled)

For custom scans, select these options in the **Performance** section of the **Scan Task Settings** tab. For quick and full scans, select these options in the **Performance** section in **Settings** → **On-Demand Scan** → **Full Scan** or **Quick Scan**.

Allow users to defer scans

If you choose **Scan anytime**, you can allow users to defer scheduled scans in one-hour increments, up to 24 hours, or forever. Each user deferral can last one hour. For example, if the **Maximum number of hours user can defer** option is set to 2, the user can defer the scan twice (two hours). When the maximum specified number of hours elapses, the scan continues.

For custom scans, select **User can defer scans** in the **Performance** section of the **Scan Task Settings** tab. For quick and full scans, select this option in the **Performance** section in **Settings** → **On-Demand Scan** → **Full Scan** or **Quick Scan**.

Limit scan activity with incremental scans

Use incremental, or resumable, scans to limit when on-demand scan activity occurs, and still scan the whole system in multiple sessions. To use incremental scanning, add a time limit to the scheduled scan. The scan stops when the time limit is reached. The next time this task starts, it continues from the point in the file and folder structure where the previous scan stopped.

Select **Stop this task if it runs longer than** in the **Options** section of the **Scan Task Schedule** tab.

Check the OnDemandScan_Activity log file for scan statistics, such as start time, end time, and time to complete the scan. From the **Event Log** page in Trellix Endpoint Security (ENS) Client, click **View Logs Folder**. Most recent scan tasks activity appears at the bottom of the file.

Configure system utilization

System utilization specifies the amount of CPU time that the scanner receives during the scan. For systems with end-user activity, set system utilization to **Low**.

You can use the Windows Task Manager to view CPU utilization consumed by the Trellix Scanner service process (mcshield.exe).

The scan process for **Full Scan** and **Quick Scan** on-demand scans runs at low priority. But, if no other processes are running during a scan, the mcshield.exe process might consume a higher amount of CPU resources. If any other processes make system requests, mcshield.exe releases the CPU resources.

For custom scans, select **System utilization** in the **Performance** section of the **Scan Task Settings** tab. For quick and full scans, select this option in the **Performance** section in **Settings** → **On-Demand Scan** → **Full Scan** or **Quick Scan** tab.

Specify the maximum CPU percentage for scans

As an alternative to using system utilization to automatically determine the amount of CPU the scan uses, you can specify a maximum percentage. In this case, the CPU usage for **Full Scan**, **Quick Scan**, and custom scans is limited to the percentage you specify. For example, if you specify 60%, the full scan consumes 60% of the available CPU.

Because the scan is single-threaded, if the system has multiple CPUs, the scan uses the percentage of 1 CPU. So, if you want to limit the scan to 25% of the total CPU processing power of a 4-CPU system, set the percentage to 25%.

This option only applies to scanning files. It doesn't limit CPU usage when scanning other items, such as memory, registry, and boot sectors.

Note

This option is available only when the **Scan anytime** option is selected.

Custom scans	In the **Scan Task Settings** tab: 1. Select **Scan anytime** in the **Scheduled Scan Options** section.

	2. Select **Limit CPU usage percentage** in the **Performance** section.
Quick and full scans	In the **On-Demand Scan** settings, on the appropriate tab (**Full Scan** or **Quick Scan**): 1. Select **Scan anytime** in the **Scheduled Scan Options** section. 2. Select **Limit maximum CPU usage** in the **Performance** section

Scan only what you need to

Scanning some types of files can negatively affect system performance. For this reason, select these options only if you need to scan specific types of files.

For custom scans, select or deselect these options in the **What to Scan** section of the **Scan Task Settings** tab. For quick and full scans, select or deselect these options in the **What to Scan** section in **Settings** → **On-Demand Scan** → **Full Scan** or **Quick Scan**.

- **Files that have been migrated to storage** Some offline data storage solutions replace files with a stub file. When the scanner encounters a stub file, which indicates that the file has been migrated, the scanner restores the file to the local system before scanning. The restore process can negatively impact system performance.
  Deselect this option unless you have a specific need to scan files in storage.

  Note

  This option doesn't apply to files stored in Microsoft OneDrive. The on-demand scanner doesn't download OneDrive files or scan files that haven't been downloaded.

- **Compressed archive files** Even if an archive contains infected files, the files can't infect the system until the archive is extracted. Once the archive is extracted, the On-Access Scan examines the files and detects any malware.

  Tip

  Best practice: Because scanning compressed archive files can negatively affect system performance, deselect this option to improve system performance.

Managing Firewall on a client system

Enable and configure Firewall on a client system

You can configure settings for Firewall to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Select **Enable Firewall** to make the firewall active and change its options.

   Note

   Host Intrusion Prevention 8.0 can be installed on the same system as Trellix ENS version 10.7. If McAfee Host IPS Firewall is installed and enabled, Trellix ENS Firewall is disabled even if enabled in the settings.

4. Click **Show Advanced**.
5. Configure settings on the page, then click **Apply**.

Block DNS traffic on a client system

To refine firewall protection, you can create a list of FQDNs to block. Firewall blocks connections to the IP addresses resolving to the domain names.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Under **DNS Blocking**, click **Add**.
4. Enter the FQDN of the domains to block, then click **Save**.

   You can use the ***** and **?** wildcards. For example, *domain.com.

   Duplicate entries are removed automatically.

5. Click **Apply**.

Define networks to use in rules and groups on a client system

You can define network addresses, subnets, or ranges to use in rules and groups, or define networks as trusted.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.
   Or, from the **Action** menu , select **Settings**, then click **Firewall** on the **Settings** page.
3. Click **Show Advanced**.
4. From **Defined Networks**, do any of the following:

To...	Steps
Define a network.	Click **Add** and enter the details for the trusted network. From the drop-down list: • Select **Yes** to define the network as trusted. Firewall allows all traffic to and from trusted networks. • Select **No** to define the network for use in rules and groups. You can use networks defined as not trusted for the local or remote network criteria in a rule or group. Defining a network as not trusted adds those networks as exceptions to Trellix GTI rules in Firewall and excludes those networks from a Trellix GTI lookup.
Change a network definition.	For each column, double-click the item and enter the new information.
Delete a network.	Select a row, then click **Delete**.

5. Click **Apply**.

Exclude network addresses from a Trellix GTI lookup on a client system

You can exclude certain network addresses from a Trellix GTI lookup to reduce traffic and improve performance.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Note

Trellix GTI automatically excludes certain IP addresses from a reputation check. For more information, see KB90837.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Click **Show Advanced**.
4. Under **Defined Networks**, click **Add**.
5. From the **Address type** drop-down list, select the address type.
6. In the **Address** field, enter the address.
7. From the **Trusted** drop-down list, select **No**.
8. Click **Apply**.

Configure trusted executables on a client system

Trusted executables are ones that are considered safe for your environment.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Click **Show Advanced**.
4. From **Trusted Executables**, do any of the following:

To...	Steps
Define a new trusted executable.	Click **Add** and enter the details for the trusted executable.

To...	Steps
Change an executable definition.	For each column, double-click the item and enter the new information.
Delete an executable.	Select a row, then click **Delete**.

5. Click **Apply**.

Get the signer distinguished name to specify trusted executables on a client system

The signer distinguished name (SDN) is required when you enable a digital signature check and add only files signed by a specified process signer.

Task

1. Right-click an executable and select **Properties**.
2. On the **Digital Signatures** tab, select a signer and click **Details**.
3. On the **General** tab, click **View Certificate**.
4. On the **Details** tab, select the **Subject** field.
   The SDN appears.

   For example, Firefox has this SDN:

   CN = Mozilla Corporation

   OU = Release Engineering

   O = Mozilla Corporation

   L = Mountain View

   S = California

   C = US

   Note

   The SDN fields appear in reverse order from the required format.

5. Copy the contents of the **Subject** field to a temporary location.
6. Edit the information to reverse the order of the elements, remove line breaks, and separate the elements with commas.

   For example, the SDN required format is:

   ```
   C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION
   ```

7. When specifying trusted executables, paste the certificate details to the **Signed by** field.

Create and manage Firewall rules and groups on a client system

You can use firewall rule groups to group a set of rules with a single purpose.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Firewall processes rules from top to bottom, regardless of whether they are in groups. The groups and rules appear in priority order in the **Firewall Rules** table. You can't sort rules by column.

Rules and groups that you configure from the Trellix Endpoint Security (ENS) Client might be overwritten when the administrator deploys an updated policy.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Use these tasks to manage firewall rules and groups.

To do this...	Follow these steps
View the rules in a firewall group.	Click >.
Collapse a firewall group.	Click ⌄.
Change an existing rule. **Note:** You can change rules in the **User added** group only.	a. Expand the **User added** group. b. Double-click the rule. c. Change the rule settings. d. Click **OK** to save your changes.
View an existing rule in any group.	a. Expand the group. b. Select the rule to view its details in the bottom pane.
Create a rule.	a. Click **Add Rule**. b. Specify the rule settings. c. Click **OK** to save your changes.

To do this...	Follow these steps
	The rule appears at the end of the **User added** group.
Create copies of rules.	a. Select the rule or rules and click **Duplicate**. Copied rules appear with the same name at the end of the **User added** group. b. Change the rules to change the name and settings.
Delete rules. **Note:** You can delete rules from the **User added** and **Adaptive** groups only.	a. Expand the group. b. Select the rule or rules and click **Delete**.
Create a group.	a. Click **Add Group**. b. Specify the group settings. c. Click **OK** to save your changes. The group appears in the **User added** group.
Move rules and groups in and between groups. **Note:** You can move rules and groups in the **User added** group only.	To move elements: a. Select elements to move. The grip appears to the left of elements that can be moved. b. Drag and drop the elements to the new location. A blue line appears between elements where you can drop the dragged elements.

4. Click **Apply**.

Wildcards in firewall rules

You can use wildcards to represent characters for some values in firewall rules. Wildcards match zero or more characters so that you don't have to specify an entire path or value, or set of values.

Firewall supports wildcards in blocked domains and executable paths only.

For paths of files, registry keys, executables, and URLs, use these wildcards.

Note

Registry key paths for firewall group locations don't recognize wildcard values.

?	Question mark	A single character. This wildcard applies only if the number of characters matches the length of the file or folder name. **For example:** The exclusion W?? excludes W**WW**, but doesn't exclude WW or WWWW.
*	Asterisk	Multiple characters, excluding slash (/) and backslash (\). Use this character to match the root-level contents of a folder with no subfolders. **Note:** *\ at the beginning of a file path is not valid. Use **\ instead. For example: **\ABC*.
**	Double asterisk	Multiple characters, including slash (/) and backslash (\). This wildcard matches zero or more characters. For example: C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ.
|	Pipe	Wildcard escape. **Note:** For the double asterisk (**), the escape is |*|*.

Note

Wildcards can appear in front of a backslash (\) in a path. For example, C:\ABC*\XYZ matches C:\ABC\DEF\XYZ.

For values that normally don't contain path information with slashes, use these wildcards.

?	Question mark	A single character.
*	Asterisk	Multiple characters, including slash (/) and backslash (\).
|	Pipe	Wildcard escape.

Wildcard examples

DNS Blocking feature- Use wildcards to match domain names and subdomains names.

*.domain.com
*domain.com
*subdomain.domain.com
*.subdomain.domain.com

Executable file path criteria- Trusted Executables, Firewall Rule Executables, and Firewall Group Executables.

When defining executables in the firewall configuration rules/groups, use executable file extensions such as .exe, .com, etc.

Note

Wildcards can’t be used in FQDN (fully qualified domain name) values, both in local and remote network. They are also restricted for usage in executable file descriptions, hash and signer details.

Example	Description
**\Temp\test.exe	Defines a specific executable file in a folder named Temp anywhere on the system.

Example	Description
**\test.exe	Defines a specific executable file anywhere on the system.
**\test.exe	Defines a specific executable file in any folder on a specific drive.
C:\Users*\Desktop\test.exe	Define a specific executable file on any user's profile Desktop directory.
C:\Program Files*\test.exe	Define a specific executable file to run from either the \Program Files or \Program Files (x86)\ directories.
**\test*.exe	Define a specific executable file to run if the filename starts with "test"
**\test?.exe	Define a specific executable file to run if the filename matches testX.com, where X is any valid character for a file name
C:\Program Files\Test*	Define an executable match for all executables in a specific directory.
C:\Program Files\Test**	Define an executable match for all executables in a specific directory and all sub-directories.

Create connection isolation groups on a client system

A connection isolation firewall rule group instructs Firewall to process only traffic that matches the defined connection type and group criteria.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3. Under **RULES**, click **Add Group**.
4. Under **Description**, specify options for the group.
5. Under **Location**, select **Enable location awareness** and **Enable connection isolation**. Then, select the location criteria for matching.
6. Under **Networks**, for **Connection types**, select the type of connection (**Wired**, **Wireless**, or **Virtual**) to apply to the rules in this group.

Note

Settings for **Transport** and **Executables** aren't available for connection isolation groups.

7. Click **OK**.
8. Create new rules within this group, or move existing rules into it from the firewall rule list.
9. Click **Apply**.

Create timed groups on a client system

You can create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Firewall** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Create a Firewall group with default settings that allow Internet connectivity.
   For example, allow port 80 HTTP traffic.
4. In the **Schedule** section, select how to enable the group.
   - **Enable schedule** — Specifies a start and end time for the group to be enabled.
   - **Disable schedule and enable the group from the Trellix system tray icon** — Allows users to enable the group from the Trellix system tray icon and keeps the group enabled for the specified number of minutes. If you allow users to manage the timed group, you can optionally require that they provide a justification before enabling the group.
5. Click **OK** to save your changes.
6. Create a connection isolation group that matches the VPN network to allow needed traffic.

Tip

Best practice: To allow outbound traffic from only the connection isolation group on the client system, don't place any Firewall rules below this group.

7. Click **Apply**.

Managing Web Control on a client system

Enable Web Control and configure its options on a client system

You can enable Web Control and configure its options from Trellix Endpoint Security (ENS) Client.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Web Control** on the main **Status** page.
   Or, from the **Action** menu  , select **Settings**, then click **Web Control** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. Select **Enable Web Control** to make Web Control active and change its options.

To...	Do this...	Notes
Hide the Web Control toolbar on the browser without disabling protection. (Internet Explorer only)	Select **Hide the toolbar on the client browser**.	
Allow users to run Internet Explorer with the `-extoff` command-line option. (Managed systems) (Internet Explorer only)	Select **Allow user to run Internet Explorer in extension-off mode**.	⚠ **Caution:** In extension-off mode, Internet Explorer doesn't load *any* extensions or add-ons. Although Web Control is enabled on the system, it isn't loaded in the browser, which leaves the system vulnerable to threats.
Track browser events.	Configure settings in the **Event Logging** section.	

To...	Do this...	Notes
Block or warn unknown URLs.	In **Action Enforcement**, select the action (**Block**, **Allow**, or **Warn**) for sites not yet verified by Trellix GTI .	
Scan files before downloading.	In **Action Enforcement**, select **Enable file scanning for file downloads**, then select the Trellix GTI risk level to block.	If users specify the complete URL to a file whose reputation is not malicious, Web Control allows the file download, even if the site is blocked.
Download clean reputation files (Green rated) from unverified URLs.	In **Action Enforcement**, select **Block** and **Allow Green-rated file downloads from not yet verified URL**.	This feature is only available for Google Chrome. **Note:** To view this option, **Enable file scanning for file downloads** must first be selected.
Add external sites to the local private network.	In **Exclusions**, under **Specify IP addresses or ranges to exclude from Web Control rating or blocking**, click **Add**, then enter an external IP address or range.	
Block risky sites from appearing in search results.	In **Secure Search**, select **Enable Secure Search**, select the search engine, then specify whether to block links to risky sites.	**Secure Search** automatically filters the malicious sites in the search result based on their safety rating. Web Control uses Yahoo as the default search engine and supports **Secure Search** on Internet Explorer only. If you change the default search engine, restart the browser for the changes to take effect. The next time the user opens Internet Explorer, Web

To...	Do this...	Notes
		Control displays a pop-up prompting the user to change to Trellix Secure Search with the specified search engine. For Internet Explorer versions where the search engine is locked, the Secure Search pop-up doesn't appear.

6. Configure other options as needed.
7. Click **Apply**.

Specify rating actions and block site access based on web category on a client system

You can specify actions, based on safety ratings, to apply to sites and file downloads. You can also block or allow sites in each web category.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Web Control** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Web Control** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Content Actions**.
5. In the **Web Category Blocking** section, for each **Web Category**, enable or disable the **Block** option.

Note

For sites in the unblocked categories, Web Control also applies the rating actions.

6. In the **Rating Actions** section, specify the actions to apply to any sites and file downloads, based on safety ratings defined by Trellix.

Note

These actions also apply to sites that web category blocking doesn't block.

7. Click **Apply**.

Using safety ratings to control access

Use safety ratings to determine whether users can access a site or access resources on a site.

In the **Content Actions** settings, specify whether to allow, warn, or block sites and file downloads, based on the safety rating. This setting enables a greater level of granularity in protecting users against files that might pose a threat on sites with an overall green rating.

To block file downloads on allowed sites, change the settings on the **Advanced Settings** tab of the **Block and Allow List** settings.

Tip

Best practice: To make sure that users can access specific sites that are important to your business, no matter how they are rated, add them to an allowed list. Users can access sites that appear on an allowed list even if you configured other actions with their ratings.

Using web categories to control access

Trellix defines categories for the types of content on websites. You can allow or block access to sites based on these categories.

When you enable web category blocking in the **Content Actions** settings, the software blocks or allows categories of websites. These web categories include **Gambling**, **Games**, and **Instant Messaging**. Trellix defines and maintains the list of about 105 web categories.

When a client user accesses a site, the software checks the web category for the site. If the site belongs to a defined category, access is blocked or allowed, based on the settings in the **Content Actions** settings. For sites and file downloads in the unblocked categories, the software applies the specified **Rating Actions**.

Managing Adaptive Threat Protection on a client system

Handling new false positives with Extra.DAT files

If Adaptive Threat Protection determines that a detection is a false positive, Trellix Labs might release a negative Extra.DAT file to suppress the detection until the next content update.

Deploying a negative Extra.DAT is optional. If the TIE server is present, you can change the reputation score to eliminate the false positive. For information, see KB82922.

ATP supports using only one Extra.DAT file at a time. In a situation where you need both a negative Extra.DAT file and a positive Extra.DAT file for Threat Prevention, you can request a combined file from Trellix Labs.

Each Extra.DAT file has an expiration date built in. When the Extra.DAT file is loaded, this expiration date is compared against the build date of the AMCore content installed on the system. If the build date of the AMCore content is newer than the Extra.DAT

expiration date, the Extra.DAT is considered expired. It is no longer loaded and used by the engine. During the next update, the Extra.DAT is removed from the system.

If the next update of AMCore content includes information in the Extra.DAT, the Extra.DAT is removed.

Trellix ENS stores Extra.DAT files in the c:\Program Files\Common Files\McAfee\Engine\content\avengine\extradat folder.

Download and load an Extra.DAT file on a client system

In a major malware outbreak, you must load an Extra.DAT file to protect client systems until the next scheduled content update. You might need to load an Extra.DAT file on client systems to suppress detections that are considered false positives until the next scheduled content update.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Download the Extra.DAT file.
    a. Click the download link supplied by Trellix Labs, specify a location to save the Extra.DAT file, then click **Save**.
    b. If needed, unzip the EXTRA.ZIP file.
2. Open the Trellix Endpoint Security (ENS) Client.
3. From the **Action** menu , select **Load Extra.DAT**.
4. Click **Browse**, navigate to the location where you downloaded the Extra.DAT file, then click **Open**.
5. Click **Apply**.

Results

The new detections in the Extra.DAT take effect immediately.

Containing applications dynamically on a client system

Dynamic Application Containment enables you to specify that applications with specific reputations run in a container. Contained applications aren't allowed to perform certain actions, as specified by containment rules.

Based on the reputation threshold, ATP requests that Dynamic Application Containment run the application in a container.

This technology lets you evaluate unknown and potentially unsafe applications by allowing them to run in your environment, while limiting the actions they can take. Users can use the applications, but they might not work as expected if Dynamic Application Containment blocks certain actions. Once you determine that an application is safe, you can configure ATP or TIE server to allow it to run normally.

To use Dynamic Application Containment:

1. Enable ATP and specify the reputation threshold for triggering Dynamic Application Containment in the **Options** settings.
2. Configure Trellix-defined containment rules and exclusions in the **Dynamic Application Containment** settings.

Enable the trigger threshold for Dynamic Application Containment on a client system

With Dynamic Application Containment, you can specify that applications with specific reputations run in a container, limiting the actions they can perform. If the application reputation is at or below the containment reputation threshold, the application is contained.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. Verify that ATP is enabled.
6. Select **Trigger Dynamic Application Containment when reputation threshold reaches**.
7. Specify the reputation threshold at which to contain applications.
   - **Might Be Trusted**
   - **Unknown** (default for the **Security** rule group)
   - **Might Be Malicious** (default for the **Balanced** rule group)
   - **Most Likely Malicious** (default for the **Productivity** rule group)
   - **Known Malicious**

   The Dynamic Application Containment reputation threshold must be above the block and clean thresholds. For example, if the block threshold is set to **Known Malicious**, the Dynamic Application Containment threshold must be set to **Most Likely Malicious** or above.
8. Click **Apply**.

Configure Trellix-defined containment rules on a client system

Trellix-defined containment rules block or log actions that contained applications perform. You can change the block and report settings, but you can't otherwise change or delete these rules.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.

4. Click **Dynamic Application Containment**.
5. In the **Containment Rules** section, select **Block**, **Report**, or both for the rule.
    - To block or report all, select **Block** or **Report** in the first row.
    - To disable the rule, deselect both **Block** and **Report**.
6. In the **Exclusions** section, configure executables to exclude from Dynamic Application Containment.
   Processes in the **Exclusions** list run normally (not contained).
7. Click **Apply**.

Manage contained applications on a client system

When Dynamic Application Containment contains a trusted application, you can exclude it from containment from the Trellix Endpoint Security (ENS) Client.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Excluding the application releases it, removes it from **Contained Applications**, and adds it to **Exclusions**, preventing it from being contained in the future.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.
   Or, from the **Action** menu  , select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Dynamic Application Containment**.
5. In the **Contained Applications** section, select the application and click **Exclude**.
6. On the **Add Executable** page, configure the executable properties, then click **Save**.
   The application appears in the **Exclusions** list. The application remains in the **Contained Applications** list until you click **Apply**. When you return to the **Settings** page, the application appears in the **Exclusions** list only.
7. Click **Apply**.

Prevent Dynamic Application Containment from containing trusted programs on a client system

If a trusted program is contained, you can allow it to run normally by creating a Dynamic Application Containment exclusion.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Trellix ENS treats all file and folder exclusions as case insensitive — all case variations of the specified locations are excluded. For example, if you exclude C:\Temp\ABC, Trellix ENS also excludes C:\temp\abc and C:\TEMP\Abc.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Dynamic Application Containment**.
5. In the **Exclusions** section, click **Add** to add processes to exclude from all rules.
6. On the **Add Executable** page, configure the executable properties.
7. Click **Save**, then click **Apply** to save the settings.

Get the signer distinguished name to exclude executables on a client system

The signer distinguished name (SDN) is required when you enable a digital signature check and exclude only files signed by a specified process signer.

Task

1. Right-click an executable and select **Properties**.
2. On the **Digital Signatures** tab, select a signer and click **Details**.
3. On the **General** tab, click **View Certificate**.
4. On the **Details** tab, select the **Subject** field.
   The SDN appears.

   For example, Firefox has this SDN:

   CN = Mozilla Corporation

   OU = Release Engineering

   O = Mozilla Corporation

   L = Mountain View

   S = California

   C = US

   Note

   The SDN fields appear in reverse order from the required format.

5. Copy the contents of the **Subject** field to a temporary location.
6. Edit the information to reverse the order of the elements, remove line breaks, and separate the elements with commas.

   For example, the SDN required format is:

   ```
   C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION
   ```

7. When creating exclusions, copy and paste the certificate details as a single line of text to the **Signed by** field.

Configure Adaptive Threat Protection on a client system

Adaptive Threat Protection settings determine when a file or process is allowed to run, and if it is contained, cleaned, blocked, or the user is prompted. You can also use these settings to enable Real Protect, enhanced remediation, and enhanced script scanning with AMSI.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Note

Policy changes from Trellix ePO - On-prem overwrite changes from the **Settings** page.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. Configure settings on the page, then click **Apply**.

Exclude processes from Adaptive Threat Protection scanning on a client system

ATP scanning uses exclusions defined in the Threat Prevention **On-Access Scan** settings for **Standard** process types.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Best practice: For suggestions on how to improve Trellix ENS performance, see KB88205.

On-access scan **Standard** process exclusions specified by file name or file path apply to all ATP scanners, including Dynamic Application Containment and Real Protect. On-access scan exclusions specified by file type or age don't apply to ATP. ATP supports the same wildcards in path-based exclusions as Threat Prevention does.

Trellix ENS treats all file and folder exclusions as case insensitive — all case variations of the specified locations are excluded. For example, if you exclude C:\Temp\ABC, Trellix ENS also excludes C:\temp\abc and C:\TEMP\Abc.

Best practice: For information about troubleshooting blocked third-party applications, see KB88482.

For a list of executables that ATP scanned, check the Adaptive Threat Protection debug log (AdaptiveThreatProtection_Debug.log) on the client system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **On-Access Scan**.
5. In the **Process Types** section, select the **Standard** tab.

   Note

   Exclusions specified in the **High Risk** and **Low Risk** tabs don't apply to ATP.

6. In the **Exclusions** section, click **Add** to enter the process to exclude from ATP scanning.

   In the **When to exclude** section, select **When reading from disk**.

   Tip

   If you want to exclude items from ATP scanning only, select this option. Threat Prevention still scans those items when they are being written to or changed on the disk.

7. Click **Apply**.

Configure Adaptive Threat Protection with no connection to Trellix GTI on a client system

For systems with no network connection to Adaptive Threat Protection, such as air-gapped systems, you can improve performance by manually disabling Adaptive Threat Protection.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Note

Policy changes from Trellix ePO - On-prem overwrite changes from the **Settings** page.

Disable Adaptive Threat Protection to eliminate unnecessary attempts to connect to Adaptive Threat Protection when no network path exists and reduce the impact on Trellix ENS performance.

Caution

Disabling Adaptive Threat Protection might result in increased false positives.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu , select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. In the **On-Access Scan**, **Trellix GTI** section, deselect **Enable Trellix GTI**.
4. Click **Adaptive Threat Protection**.
5. Click **Show Advanced**.
6. In the **Reputation Source** section, click the drop-down list and select **Use only the TIE server**.
7. Click **Apply**.

Monitoring activity on a client system

Monitoring your protection on a client system

Check the Event Log for recent activity

The **Event Log** in the Trellix Endpoint Security (ENS) Client displays a record of events that occur on the Trellix-protected system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Event Log** on the left side of the page.
   The page shows any events that Trellix ENS has logged on the system in the last 30 days.

   If the Trellix Endpoint Security (ENS) Client can't reach the **Event Manager**, it displays a communication error message. In this case, reboot the system to view the **Event Log**.

3. Select an event from the top pane to display the details in the bottom pane.
   To change the relative sizes of the panes, click and drag the sash widget between the panes.
4. On the **Event Log** page, sort, search, filter, or reload events.
5. Navigate in the **Event Log**.
   By default, the **Event Log** displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

Log file names and locations

The activity, error, and debug log files record events that occur on systems with Trellix products enabled.

All activity and debug log files are stored here:

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file, EndpointSecurityPlatform_Errors.log.

Log files

Feature or technology	File name
Platform	EndpointSecurityPlatform_Activity.log
	EndpointSecurityPlatform_Debug.log
Self Protection	SelfProtection_Activity.log

Feature or technology	File name
	SelfProtection_Debug.log
Updates	PackageManager_Activity.log
	PackageManager_Debug.log
Errors	EndpointSecurityPlatform_Errors.log Contains error logs for all modules.
Trellix Endpoint Security (ENS) Client	MFEConsole_Debug.log
Scan	OnAccessScan_Activity.log
	OnAccessScan_Debug.log
	OnDemandScan_Activity.log
	OnAccessScan_Debug.log
Firewall	Firewall_Activity.log
	Firewall_Debug.log
	FirewallEventMonitor.log
	FirewallEventMonitor_debug.log
Exploit Prevention	ExploitPrevention_Activity.log
	ExploitPrevention_Debug.log
Threat Prevention	ThreatPrevention_Activity.log
	ThreatPrevention_Debug.log
Web Control	WebControl_Activity.log

Feature or technology	File name
	WebControl_Debug.log

Tip

Best Practice: For information on Trellix ENS event messages, see KB85494.

By default, installation log files are stored here:

- %TEMP%\McAfeeLogs, which is the Windows user TEMP folder. (Managed systems)
- TEMP\McAfeeLogs, which is the Windows system TEMP folder. (Self-managed systems)

Monitoring Threat Prevention activity on a client system

Check the Event Log for recent activity

The **Event Log** in the Trellix Endpoint Security (ENS) Client displays a record of events that occur on the Trellix-protected system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Event Log** on the left side of the page.
   The page shows any events that Trellix ENS has logged on the system in the last 30 days.

   If the Trellix Endpoint Security (ENS) Client can't reach the **Event Manager**, it displays a communication error message. In this case, reboot the system to view the **Event Log**.

3. Select an event from the top pane to display the details in the bottom pane.
   To change the relative sizes of the panes, click and drag the sash widget between the panes.
4. On the **Event Log** page, sort, search, filter, or reload events.
5. Navigate in the **Event Log**.
   By default, the **Event Log** displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

Threat Prevention log file names and locations

The activity, error, and debug log files record events that occur on systems with Trellix ENS enabled.

All activity and debug log files are stored in the following default location:

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file, EndpointSecurityPlatform_Errors.log.

Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.

Log files

Module	Feature or technology	File name
Threat Prevention	Enabling debug logging for any Threat Prevention technology also enables debug logging for the Trellix Endpoint Security (ENS) Client.	ThreatPrevention_Activity.log
		ThreatPrevention_Debug.log
	Exploit Prevention	ExploitPrevention_Activity.log
		ExploitPrevention_Debug.log
	On-Access Scan	OnAccessScan_Activity.log
		OnAccessScan_Debug.log
	On-Demand Scan • **Quick Scan** • **Full Scan** • **Right-Click Scan**	OnDemandScan_Activity.log
		OnDemandScan_Debug.log
	Access Protection	AccessProtection_Activity.log
		AccessProtection_Debug.log
Common		EndpointSecurityPlatform_Errors.log Contains error logs for all modules.

Tip

Best practice: For information on Trellix ENS event messages, see KB85494.

By default, installation log files are stored here:

- TEMP\McAfeeLogs, which is the Windows system TEMP folder. (Managed systems)

- %TEMP%\McAfeeLogs, which is the Windows user TEMP folder. (Self-managed systems)

Monitoring Firewall activity on a client system

Check the Event Log for recent activity

The **Event Log** in the Trellix Endpoint Security (ENS) Client displays a record of events that occur on the Trellix-protected system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Event Log** on the left side of the page.
   The page shows any events that Trellix ENS has logged on the system in the last 30 days.

   If the Trellix Endpoint Security (ENS) Client can't reach the **Event Manager**, it displays a communication error message. In this case, reboot the system to view the **Event Log**.

3. Select an event from the top pane to display the details in the bottom pane.
   To change the relative sizes of the panes, click and drag the sash widget between the panes.
4. On the **Event Log** page, sort, search, filter, or reload events.
5. Navigate in the **Event Log**.
   By default, the **Event Log** displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

Firewall log file names and locations

The activity, error, and debug log files record events that occur on systems with Trellix ENS enabled.

All activity and debug log files are stored in the following default location:

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file, EndpointSecurityPlatform_Errors.log.

Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.

Log files

Module	File name	Notes
Firewall	Firewall_Activity.log	
	Firewall_Debug.log	
	FirewallEventMonitor.log	Logs blocked and allowed traffic events, if configured.

Module	File name	Notes
Common	EndpointSecurityPlatform_Errors.log	Contains error logs for all modules.

Tip

Best practice For information on Trellix ENS event messages, see KB85494.

By default, installation log files are stored here:

- TEMP\McAfeeLogs, which is the Windows system TEMP folder. (Managed systems)
- %TEMP%\McAfeeLogs, which is the Windows user TEMP folder. (Self-managed systems)

Monitoring Web Control activity on a client system

Check the Event Log for recent activity

The **Event Log** in the Trellix Endpoint Security (ENS) Client displays a record of events that occur on the Trellix-protected system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Event Log** on the left side of the page.
   The page shows any events that Trellix ENS has logged on the system in the last 30 days.

   If the Trellix Endpoint Security (ENS) Client can't reach the **Event Manager**, it displays a communication error message. In this case, reboot the system to view the **Event Log**.

3. Select an event from the top pane to display the details in the bottom pane.
   To change the relative sizes of the panes, click and drag the sash widget between the panes.
4. On the **Event Log** page, sort, search, filter, or reload events.
5. Navigate in the **Event Log**.
   By default, the **Event Log** displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

Web Control log file names and locations

The activity, error, and debug log files record events that occur on systems with Trellix ENS enabled.

All activity and debug log files are stored in the following default location:

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file, EndpointSecurityPlatform_Errors.log.

Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.

Log files

Module	File name	Notes
Web Control	WebControl_Activity.log	
	WebControl_Debug.log	
Common	EndpointSecurityPlatform_Errors.log	Contains error logs for all modules.

Tip

Best practice For information on Trellix ENS event messages, see KB85494.

By default, installation log files are stored here:

- TEMP\McAfeeLogs, which is the Windows system TEMP folder. (Managed systems)
- %TEMP%\McAfeeLogs, which is the Windows user TEMP folder. (Self-managed systems)

Monitoring Adaptive Threat Protection activity on a client system

Check the Event Log for recent activity

The **Event Log** in the Trellix Endpoint Security (ENS) Client displays a record of events that occur on the Trellix-protected system.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Event Log** on the left side of the page.
   The page shows any events that Trellix ENS has logged on the system in the last 30 days.

   If the Trellix Endpoint Security (ENS) Client can't reach the **Event Manager**, it displays a communication error message. In this case, reboot the system to view the **Event Log**.

3. Select an event from the top pane to display the details in the bottom pane.
   To change the relative sizes of the panes, click and drag the sash widget between the panes.
4. On the **Event Log** page, sort, search, filter, or reload events.
5. Navigate in the **Event Log**.
   By default, the **Event Log** displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

Disable the Story Graph on a client system

Users can choose whether or not they would like to have the Story Graph feature enabled. Story Graph is enabled by default in order to provide valuable context to ATP detections.

Task

1. Open the Trellix ENS Client.
2. Click **Status** → **ADAPTIVE THREAT PROTECTION**.
3. Click **Show Advanced**.
4. Under **Story Graph** section, deselect **Enable Story Graph Tracing**.

Adaptive Threat Protection log file names and locations

The activity, error, and debug log files record events that occur on systems with Trellix ENS enabled.

All activity and debug log files are stored in the following default location:

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file, EndpointSecurityPlatform_Errors.log.

Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.

Log files

Module	Feature or technology	File name
Adaptive Threat Protection		AdvancedThreatProtection_Activity.log
		AdvancedThreatProtection_Debug.log
	Dynamic Application Containment	DynamicApplicationContainment_Activity.log
		DynamicApplicationContainment_Debug.log
	False positive mitigation	FalsePositiveMitigation_Activity.log

Module	Feature or technology	File name
		FalsePositiveMitigation_Debug.log
	Enhanced Remediation	EnhancedRemediation_Debug.log
Common	Errors	EndpointSecurityPlatform_Errors.log Contains error logs for all modules.

Best practice For information on Trellix ENS event messages, see KB85494.

By default, installation log files are stored here:

- TEMP\McAfeeLogs, which is the Windows system TEMP folder. (Managed systems)
- %TEMP%\McAfeeLogs, which is the Windows user TEMP folder. (Self-managed systems)

Using the command line interface

With the Threat Prevention command line interface you can run Full Scan, Quick Scan, custom on-demand scans, and update security content from the command line or as part of a batch file.

Prerequisites

- The Threat Prevention service (`mfetp.exe`) must already be running for `amcfg.exe` to run.
- The interface mode for the Trellix Endpoint Security (ENS) Client must be set to **Full access** if a user wants to stop, pause or resume an on-demand scan through command line. Administrative rights are required for any task performed with `amcfg.exe`.

Syntax: Command line interface

The syntax for `amcfg.exe` is:

```
installation_path\amcfg.exe [ /scan | /update ] [ command_args ]
```

- *installation_path* — C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention by default
- *command_args* — Commands listed in the *On-demand scan command arguments* or *Custom on-demand scan command arguments* tables

Arguments can appear in any order, except that you must keep each argument with its value.

Note

The command line interface is case sensitive.

Command line interface arguments

Argument	Description
`/?`	Displays help for the command line interface.
`/help`	
`/scan`	Runs the specified scan task.
`/update`	Updates the scan engine, AMCore content, and Exploit Prevention content.

Examples: On-demand scan command line interface

Open a command prompt and change to the installation location of `amcfg.exe` to run these example commands. By default, `amcfg.exe` is located in the C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention folder.

To...	Run this command
Get help on the command line interface.	`amcfg.exe /scan /help`
Start a Quick Scan.	`amcfg.exe /scan`
Run an update.	`amcfg.exe /update`

On-demand scan command line interface

With the on-demand scan command line interface, you can start, stop, pause, resume, and get status for quick, full, and custom on-demand scans from the command line or as part of a batch file. All users can start a scan and check the status of a scan, regardless of the interface mode for the Trellix Endpoint Security (ENS) Client.

Prerequisites

- The Threat Prevention service (`mfetp.exe`) must already be running for `amcfg.exe` to run.
- The interface mode for the Trellix Endpoint Security (ENS) Client must be set to **Full access** if a user wants to stop, pause or resume an on-demand scan through command line.

Syntax: On-demand scan command line interface

The on-demand scan syntax for `amcfg.exe` is:

```
installation_path\amcfg.exe /scan /task [ command_args ]
```

- *installation_path* — C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention by default
- *command_args* — One of the commands in the *On-demand scan command arguments* table

Arguments can appear in any order, except that you must keep each argument with its value.

The scan is executed only if all values are correct. Otherwise, `amcfg.exe` displays a message with the possible values and doesn't run the scan. If the command line includes multiple values for an argument, the scan runs using only the first value. The scanner ignores any invalid configuration arguments.

On-demand scan command arguments

Argument	Value	Description
`/task`	• `quick` — Runs the default Quick Scan. • `full` — Runs the default Full Scan. • *custom_scan_ID* — Runs a custom scan with the specified ID. To get a list of scan IDs for the custom scans that are currently defined, run `amcfg.exe /scan /list`.	Specifies the type of scan task to run. If you enter `amcfg.exe /scan` (without specifying `/task`), a Quick Scan starts by default.
`/action`	• `cancel` — Stops the currently running scan, if applicable. • `pause` — Pauses the currently running scan, if applicable. **Note:** When a scan is paused, if you run `/action start` for the same scan, the scan starts again from the beginning. Use `resume` to continue a paused scan. • `resume` — Continues a paused scan, if applicable. • `start` — Starts the scan. • `status` — Displays the status of the last scan of the specified type. Check the log file for information about any detections.	Specifies the scan action to apply to the previously specified `/task`. **Note:** The `/task` argument is required with the `/action` argument. All users can start a scan and check the status of a scan, regardless of the interface mode for the Trellix Endpoint Security (ENS) Client. **Note:** Avoid using other arguments while executing `/action status` for the custom scan.

Examples: On-demand scan command line interface

Open a command prompt and change to the installation location of `amcfg.exe` to run these example commands. By default, `amcfg.exe` is located in the C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention folder.

To...	Run this command
Start a Quick Scan.	`amcfg.exe /scan`
	`amcfg.exe /scan /task quick /action start`
Display the status of a Quick Scan.	`amcfg.exe /scan /task quick /action status`
Pause the currently running Quick Scan.	`amcfg.exe /scan /task quick /action pause`
Resume the currently paused Quick Scan.	`amcfg.exe /scan /task quick /action resume`
Stop a Quick Scan.	`amcfg.exe /scan /task quick /action cancel`
Start a Full Scan.	`amcfg.exe /scan /task full /action start`
Display the status of a Full Scan.	`amcfg.exe /scan /task full /action status`
Pause the currently running Full Scan.	`amcfg.exe /scan /task full /action pause`
Resume the currently paused Full Scan.	`amcfg.exe /scan /task full /action resume`
Stop a Full Scan.	`amcfg.exe /scan /task full /action cancel`
Display a list of defined custom scan names and their scan IDs.	`amcfg.exe /scan /list`
Start a custom scan with the specified ID.	`amcfg.exe /scan /task scan_ID /action start`
Display the status of a custom scan with the specified ID.	`amcfg.exe /scan /task scan_ID /action status`
Pause the currently running custom scan with the specified ID.	`amcfg.exe /scan /task scan_ID /action pause`
Resume the currently paused custom scan with the specified ID.	`amcfg.exe /scan /task scan_ID /action resume`

To...	Run this command
Stop a custom scan with the specified ID.	`amcfg.exe /scan /task scan_ID /action cancel`

Custom on-demand scan command line interface

With the custom on-demand scan command line interface, you can run a previously defined custom on-demand scan with new settings, without changing the settings of the original custom scan.

Threat Prevention creates a clone of the original custom on-demand scan, applies your changes to the settings, and logs the changes. The new cloned custom scan is named as `<name>_cloned`. The `<name>` refers to original custom on-demand scan. Once the scan is completed, the clone is available for 15–20 minutes. The original scan settings remain unchanged.

Note

You can't change the Quick Scan or Full Scan with the command line interface.

Prerequisites

- The Threat Prevention service (`mfetp.exe`) must already be running for `amcfg.exe` to run.
- The interface mode for the Trellix Endpoint Security (ENS) Client must be set to **Full access** if a user wants to stop, pause or resume an on-demand scan through command line. All users can start a scan and check the status of a scan, regardless of the interface mode for the Trellix Endpoint Security (ENS) Client.

Syntax: Custom on-demand scan command line interface

The custom on-demand scan syntax for `amcfg.exe` is:

```
installation_path\amcfg.exe /scan [ /list | /task /scan_ID [ command_args ] [ /action start ] ]
```

- *installation_path* — C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention by default
- *command_args* — One of the commands in the *Custom on-demand scan command arguments* table

Arguments can appear in any order, except that you must keep each argument with its value.

The scan is executed only if all values are correct. Otherwise, `amcfg.exe` displays a message with the possible values and doesn't run the scan. If the command line includes multiple values for an argument, the scan runs using only the first value. The scanner ignores any invalid configuration arguments.

While cloning a custom scan, you can add new `/targets` with already defined custom scan task. The new cloned custom scan, `<name>_cloned`, not only scans the new `/targets` but also the paths mentioned in the original custom scan.

When changing a custom scan, the only valid `/action` argument is `start`. But, when a cloned scan task is running, you can apply all actions (start, pause, resume, cancel, status) to it as long as the interface mode is set to **Full access**.

Custom on-demand scan command arguments

Argument	Value	Description
`/list`		Displays the list of currently defined custom on-demand scan tasks, including temporary cloned scan tasks.
`/task`	*scan_ID*	Specifies the ID of the custom on-demand scan to change and run. If the scan ID includes spaces, you must enclose it in double-quote characters ("). **Note:** Cloned scan task IDs might include spaces.
`/targets`	*file path*	Specifies a single complete file path to scan.
`/insidefolders`	• `0` — Don't scan subfolders. • `1` — Scan subfolders.	Examines all subfolders of the specified folder.
`/usecleancache`	• `0` — Don't use clean scan cache. • `1` — Use clean scan cache.	Enables the scanner to use the existing clean scan results. **Best practice:** Select this option to reduce duplicate scanning and improve performance. If you enable logging of files scanned during an on-demand scan, the scanner doesn't log files in the clean scan cache.
`/gtisensitivity`	• `0` — **Disabled** • `1` — **Very low** • `2` — **Low** • `3` — **Medium** • `4` — **High**	Configures the Trellix GTI sensitivity level to use when determining if a detected sample is malware.

Argument	Value	Description
	• `5` — **Very high**	When enabled, fingerprints of samples, or hashes, are submitted to Trellix Labs to determine if they are malware. By submitting hashes, detection might be made available sooner than the next AMCore content file release, when Trellix Labs publishes the update. The higher the sensitivity level, the higher the number of malware detections. But, allowing more detections might result in more false positive results. Trellix GTI sensitivity levels are: • **Disabled** — No fingerprints or data is submitted to Trellix Labs. • **Very low** — The detections and risk of false positives are the same as with regular AMCore content files. A detection is made available to Threat Prevention when Trellix Labs publishes it instead of in the next AMCore content file update. Use this setting for desktops and servers with restricted user rights and strong security configurations. Average results: 10–15 queries per day, per computer. • **Low** — This setting is the minimum recommendation for laptops, desktops, and servers with strong security configurations. Average results: 10–15 queries per day, per computer.

Argument	Value	Description
		• **Medium** — Use this setting when the regular risk of exposure to malware is greater than the risk of a false positive. Trellix Labs proprietary, heuristic checks result in detections that are likely to be malware. But, some detections might result in a false positive. With this setting, Trellix Labs checks that popular applications and operating system files don't result in a false positive. This setting is the minimum recommendation for laptops, desktops, and servers. Average results: 20–25 queries per day, per computer. • **High** — Use this setting for deployment to systems or areas which are regularly infected. Average results: 20–25 queries per day, per computer. • **Very high** — Use this setting for non-operating system volumes. Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. Use this setting only to scan volumes and directories that don't support executing programs or operating systems. Average results: 20–25 queries per day, per computer.
`/sysutilization`	• `1` — **Low** • `2` — **Below normal**	Enables the operating system to specify the amount of CPU time

Argument	Value	Description
	• `3` — **Normal**	that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. • **Low** — Provides improved performance for other running applications. Sets the number of threads for the scan to 1. **Best practice:** Select this option for systems with end-user activity. • **Below normal** (Default for the preconfigured **Full Scan** and **Quick Scan**) — Sets the number of threads for the scan to be equal to the number of CPUs. • **Normal** (Default for custom scans) — Enables the scan to finish faster. Sets the number of threads for the scan to twice the number of CPUs. **Best practice:** Select this option for systems with large volumes and little end-user activity.

`/firsttaction`
`/secondtaction`
`/firstpupaction`
`/secondpupaction`
	• `0` — Removes the threat from the detected file, if possible.
	• `1` — Deletes files with potential threats.
	• `2` — Continues scanning files, without cleaning or deleting, when a threat is detected. The scanner doesn't move items to the quarantine.
		Specifies how the scanner responds when it detects a threat:
		• `firsttaction` — Specifies the first action for the scanner to take when a threat is detected.
		• `secondtaction` — Specifies the action for the scanner to take when a threat is detected if the first action fails.
		• `firstpupaction` — Specifies the first action for the scanner to take when a potentially unwanted program is detected.

Argument	Value	Description
		This option is available only if `detectup` is set to 1. • `secondpupaction` — Specifies the action for the scanner to take when an unwanted program detection is detected if the first action fails. This option is available only if `detectup` is set to 1. Remember: • If the first action is 0, the second action can be either 1 or 2. • If the first action is 1, the second action must be 2. • If the first action is 2, the second action is disabled. • The second action can never be 0.
`/mime`	• `0` — Don't scan MIME-encoded files. • `1` — Scan MIME-encoded files.	Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
`/archive`	• `0` — Don't scan compressed archive files. • `1` — Scan compressed archive files.	Examines the contents of archive (compressed) files, including .jar files. **Best practice:** Select this option only in scans scheduled during off hours when the system isn't being used. Scanning compressed archive files can negatively affect system performance.
`/detectup`	• `0` — Don't detect unwanted programs.	Enables the scanner to detect potentially unwanted programs. The scanner uses the information you configured in the Threat

Argument	Value	Description
	• `1` — Detect unwanted programs.	Prevention **Options** settings to detect potentially unwanted programs.
`/detectmt`	• `0` — Don't detect unknown macro threats. • `1` — Detect unknown macro threats.	Enables the scanner to detect unknown macro threats.
`/detectpt`	• `0` — Don't detect unknown program threats. • `1` — Detect unknown program threats.	Uses Trellix GTI to detect executable files that have code resembling malware.
`/filestoscan`	• `all` • `default` • *Comma-separated file extensions*	Specifies file types to scan. • `all` — Scans all files, regardless of extension. • `default` — Scans: ▫ Default list of file extensions defined in the current AMCore content file, including files with no extension. ▫ File extensions already defined in the original scan. You can't add new extensions to scan with the command-line scanner. The scanner uses the value of the original scan to determine whether to scan known macro threats in the list of file extensions. • *Comma-separated file extensions* — Scans only files with the extensions that you specify. The scanner uses the value of the original scan to determine

Argument	Value	Description
		whether to scan files with no extension.

Examples: Custom on-demand scan command line interface

Open a command prompt and change to the installation location of `amcfg.exe` to run these example commands. By default, `amcfg.exe` is located in the C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention folder.

To...	Run this command
Get help on the command line interface.	`amcfg.exe /scan /help`
List the currently defined custom on-demand scans.	`amcfg.exe /scan /list`
Start a custom scan with the specified ID.	`amcfg.exe /scan /task scan_ID`
	`amcfg.exe /scan /task scan_ID /action start`
Change a custom scan to scan a particular folder.	`amcfg.exe /scan /task scan_ID /targets "C:\Users\Documents"`
Specify these settings and run the custom scan: • Don't scan compressed MIME-encoded files. • Detect unknown macro threats. • Scan subfolders. • Set the Trellix GTI sensitivity level to very high.	`amcfg.exe /scan /task scan_ID /mime 0 /detectmt 1 /insidefolders 1 /gtisensitivity 5`
Scan only files with .exe extensions in the user Elmo's Downloads folder.	`amcfg.exe /scan /task scan_ID /filestoscan "exe" /targets "C:\Users\Elmo\Downloads"`
Get status of a cloned scan task.	`amcfg.exe /scan /task "Test 1_cloned" /action status`

Update command line interface

The update command line interface enables to you update the scan engine, AMCore content, and Exploit Prevention from the command line or as part of a batch file. All users can run updates, regardless of the interface mode for the Trellix Endpoint Security (ENS) Client.

Prerequisites

The Threat Prevention service (`mfetp.exe`) must already be running for `amcfg.exe` to run.

Syntax: Update command line interface

The update syntax for `amcfg.exe` is:

```
installation_path\amcfg.exe /update
```

installation_path — C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention by default

Examples: Update command line interface

Open a command prompt and change to the installation location of `amcfg.exe` to run these example commands. By default, `amcfg.exe` is located in the C:\Program Files (x86)\McAfee\Endpoint Security\Threat Prevention folder.

To...	Run this command
Run an update.	`amcfg.exe /update`

Using Expert Rules

What are Expert Rules

Expert Rules are text-based custom rules that can protect specified resources from unauthorized access and prevent exploits from known attacks. The system administrators can configure the Expert Rules in the **Exploit Prevention** policy available within Threat Prevention and enforce it to the endpoints.

Expert Rules provide additional parameters and allow much more flexibility than the custom rules you create in the **Access Protection** policy.

The Trellix predefined Expert Rules available in **Exploit Prevention** policy can be:

- enabled or disabled
- customized to Block and Report or Report only

You can write your own Expert Rules by understanding these Trellix proprietary syntaxes along with basic knowledge on the Tool Command Language (Tcl) programming:

Arbitrary Access Control (AAC)	Legacy McAfee Host IPS-based Expert Rules
Arbitrary Access Control (AAC) is a Trellix proprietary technology in Threat Prevention protect key resources. You can extend this protection by creating rules to protect specific files, processes, and registry items. AAC-based Expert Rules use a new syntax from the Tool Command Language (Tcl) interpreter version 7.6. Expert Rules enforced for: • **Files** — Protects files from unauthorized access. • **Processes** — Prevent the specific programs and processes from tampering and terminating . • **Registry** — Protects registry keys and registry values from unauthorized access. You can also create custom Files, Processes, and Registry rules in the **Access Protection** policy in Threat Prevention. But, these rules don't provide the complete functionality available with Expert Rules.	These Expert Rules follow the same syntax as rules created using the Expert method in McAfee Host IPS. Trellix ENS supports these **legacy class types**: • **Buffer Overflow** — Prevents buffer overflow exploits for applications in the Application Protection list. • **Illegal API Use** — Prevents illegal use of the Exploit Prevention API. The Expert Rules can only extend the functionality of the Illegal API Use signatures provided by Exploit Prevention content. This rules can't see APIs that aren't already covered in an Illegal API Use signature available in content. • **Services** — Protects Windows Services (Windows versions 8.0 and earlier only). You can also create custom Services rules in the **Access Protection** policy in Threat Prevention. But, these rules don't provide the complete functionality available with Expert Rules.

For more information about the Expert Rules commands in detail, see Learn Expert Rules commands for Files, Processes, and Registry.	For more information about the Expert Rules commands in detail, see Learn Expert Rules to protect Buffer overflow, Illegal API use, and Services.

Note

Each Expert Rule supports only one rule engine type. You can't mix different rule engine types in the same rule. That is, you can't combine a McAfee Host IPS-based rule (for example, Illegal API Use), with AAC-based rule (for example, Files).

Expert Rule types and supported syntaxes

Trellix ENS provides two syntaxes for creating the different Expert Rule types.

Rule type	AAC-based syntax	Legacy McAfee Host IPS-based syntax
Files	✓	✗
Registry	✓	✗
Processes	✓	✗
Buffer Overflow	✗	✓
Illegal API Use	✗	✓
Services	✗	✓
Program (McAfee Host IPS only)	✗	✗

The new AAC **Processes** rule type replaces the McAfee Host IPS **Program** rule type, which is not supported in Trellix ENS.

Note

You can't create Network IPS Expert Rules.

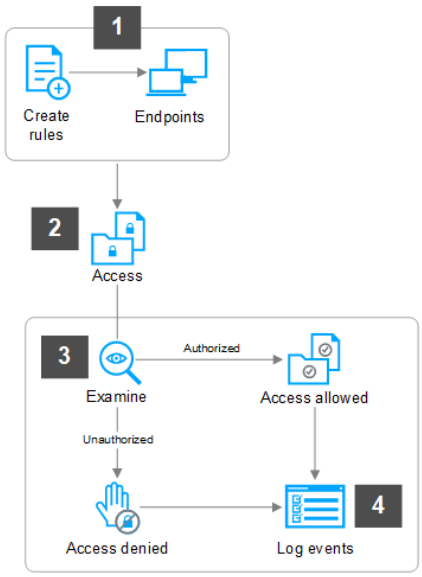
How Expert Rules work

Threat Prevention enforces Expert Rules on the client system the same as any other rule.

The signatures in the Exploit Prevention content provide default protection from Trellix Labs. If you need to protect additional resources, you can create custom rules in the Access Protection policy. For even further customization, create Expert Rules in the Exploit Prevention policy.

Here is the workflow of Expert rules:

1. An administrator creates the Expert rules and enforces them on the client system or self-managed endpoints.
2. A user or application tries to access the specific object on which the Expert rules are enforced.
3. Rules examine and perform one of these actions: a) allow access if user identity, access types, and other match values comply with the rule. b) block access if user identity, access types, and other match values do not comply with the rule.
4. Log events in the Event Log page of ENS.



Expert Rules to protect files

Create Expert Rules to protect Files using ePO

Expert rules control the access to files in a specific file path. Based on the access permission you set in the rule, it blocks and triggers an event, if any unauthorized source access the protected file.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.

2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the Signatures section, click **Add Expert Rule**.
6. In the **Expert Rules Properties** page, complete the fields.
   ENS assigns the ID number for the rule automatically starting with 20000.
   a. In the **Rule Name**, provide a unique name for the Expert rule.
   b. Select the severity level according to the Expert rule.
      The severity provides information only; it has no effect on the rule action.
   c. Select **Block** and **Report** actions for the rule by selecting the corresponding checkboxes.
      Trellix recommends selecting **Report** action for initial validation. You can select **Block** and **Report** check boxes after validating that the rule triggers the appropriate events.
   d. Select the **Use Expert Rule template** checkbox. This populates a template rule in the Rule content box based on the Rule type you select.
      To get a blank template for writing the Expert rules, deselect **Use Expert Rule template**.
   e. Select **Files** in the Rule type drop-down list.
7. Save the rule, then save the settings.
8. Validate the new policy on a client system.
9. Enforce the policy on the client systems.

Create Expert Rules to protect Files on a client system

You can create Expert rules directly on a client system or self-managed endpoints that aren't managed by Trellix ePO - On-prem.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to Full access or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Launch the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. In the **Signatures** section:
   - Create a rule — Click **Add Expert Rule**.
   - Edit an existing user-defined rule — Double-click the rule in the table.
5. In the **Expert Rule Checker** page, complete the fields.
   Trellix ENS assigns the ID number automatically starting with 20000.
   a. Select the severity and action for the rule.
      The severity provides information only; it has no effect on the rule action.
   b. Select **Files** in the Rule Type drop-down list.
   c. Add the rule code to the **Rule content** field.
6. Save the rule, then save the settings.

7. Validate the new Expert Rule on the client system.

Expert Rule syntax to protect Files

To write an expert rule to protect your files, you need to ensure that it follows the correct syntax. Expert rules consist of process, one or more targets, and the matching conditions that rules must examine before allowing the source to access the files.

Here is a sample Expert rule for registry rule type and their respective definitions:

⚠ Caution

Expert Rule commands are case-sensitive.

```
Rule {
    Process {
        Include OBJECT_NAME {
            -v "**"
        }
        Exclude .. {..}
    }
    Target {
        Match FILE {
            Include OBJECT_NAME {
                                -v "c:\\temp\\**"  #Specify file directory here
                        }
            Include -access "#define access type here"
                        Exclude -access "#define access type here"
        }
    }
}
```

To add more commands in Expert rules, see Learn Expert Rules commands for Files, Processes, and Registry.

Sections of Expert Rule syntax in detail

The above Expert rule syntax is described here:

`Rule`	Formulates the execution of commands defined within `Process` and `Target`.
`Process`	Executes the set of actions defined within the `Include` and `Exclude` commands. It does not take any other commands.

`Include OBJECT_NAME {`
`-v "**"`
`}`
`Exclude .. {..}`
	In this section,
	• The `Include` command considers the specified object name during file processing. When you specify `-v "**"`, all possible interfaces that users

	can interact with Windows are involved. To be more specific, you can write the object names such as `powershell.exe`, or `explorer.exe`, or `cmd.exe`. • The `Exclude` command eliminates the defined object name while processing. For more information, see Object name guidelines and Match types values.
`Target`	Defines the target matches for the rule. This command takes no arguments and can contain only `Match` commands. A rule must contain at least one or more `Target` commands.
`Match FILE`	Defines an object, that an Expert rule is intended to protect and to match an event. This command requires at lease one match object type value. For Files rule type, `FILE` is the match object type value.
`Include OBJECT_NAME { -v "c:\\temp\\**"`	In this section, you can define the target match type and the matching data. For example, `OBJECT_NAME` is used to specify the file directory and `-v` is specified to interpret the data as a single value.
`Include -access "#define access type here"` `Exclude -access "#define access type here"`	Defines the access flags. This flag applies when the protected file/file directory is accessed. The files rule type supports these access flags: • CONNECT_NAMED_PIPE • CREATE • DELETE • EXECUTE • POST • OPEN_FOR_DELETE • POST • READ • READ_DATA • RENAME • SET_REPARSE • WRITE • WRITE_ATTRIBUTE • WRITE_DATA

	To know more about the access flags, refer ACCESS_MASK flags.

For more Expert Rules examples, visit the Trellix Github repository.

Sample Expert Rules to protect files

Match Loaded_DLLs with AND/OR check

This Expert rule describes the usage of Loaded_DLL extension file along with the AND/OR matching on the loaded DLL files.

This Expert rule matches if "Test_DLL_Loaded.exe" has loaded "TestA.dll" AND "TestB.dll" AND "TestC.dll" AND ("TestD.dll" OR "TestE.dll"), then tries to launch "notepad.exe". The -xtype name must be unique as shown in the example. This is primarily useful in narrowing initiator matches.

Attention

Ensure to test this Expert rule on a client system before enforcing.

```
Rule  {
              Reaction BLOCK
                Process {
                                Include OBJECT_NAME { -v Test_DLL_Loaded.exe }
                                Include AggregateMatch -xtype "testa" {
                                                Include DLL_LOADED -name "testa" { -v 0x1 }
                                }
                                Include AggregateMatch -xtype "testb" {
                                                Include DLL_LOADED -name "testb" { -v 0x1 }
                                }
                                Include AggregateMatch -xtype "testc" {
                                                Include DLL_LOADED -name "testc" { -v 0x1 }
                                }
                                Include AggregateMatch -xtype "testd_or_teste" {
                                                Include DLL_LOADED -name "testd" { -v 0x1 }
                                                Include DLL_LOADED -name "teste" { -v 0x1 }
                                }
                }
                Target {
                                Match FILE {
                                                Include OBJECT_NAME { -v notepad.exe }
                                                Include -access "EXECUTE"
                                }
                }
}
```

For more Expert Rules examples, visit the Trellix Github repository.

Prevent file creation in a network path

This example rule prevents cmd.exe from creating files in a network path.

```
Rule {
        Process {
                Include OBJECT_NAME { -v cmd.exe  }
        }
        Target {
                Match FILE {
                        Include OBJECT_NAME { -v ** }
   Include -file_properties "FILE_NETWORK"
   Include -access "CREATE"
                }
        }
}
```

For more Expert Rules examples, visit the Trellix Github repository.

Prevent file creation

This example Expert rule triggers an event, when users create or access specific files in a file path, through Windows Command Prompt or File Explorer.

These are the file names and file path used in this example: test.txt and test.dat c:\\temp\\.

Attention

Make sure to test this Expert rule on a client system before enforcing wider.

```
Rule {
        Process {
                Include OBJECT_NAME {
                -v cmd.exe
                -v explorer.exe
                }
        }
        Target {
                Match FILE {
                        Include OBJECT_NAME { -v "c:\\temp\\*test.txt"}
                        Include -access "CREATE"
                }
                Match FILE {
                        Include OBJECT_NAME { -v "c:\\temp\\*test.dat"}
                        Include -access "CREATE WRITE READ"
                }
        }
}
```

Sections of Expert Rule syntax in detail

The above Expert rule is described here:

`Rule`	Formulates the execution of commands defined within `Process` and `Target`.
`Process`	Executes the set of actions defined within the `Include` and `Exclude` commands. It does not take any other commands.

`Include OBJECT_NAME {`
`-v cmd.exe`
`-v explorer.exe`
`}`
	In this section, `Include` command considers the defined object names in processing. As written in this rule, users are restricted to interact with Windows through the command prompt and File Explorer.
	For more information, see Object name guidelines and Match types values.

`Target`	Defines the target matches for the rule. This command takes no arguments and can contain only `Match` commands. A rule must contain at least one or more `Target` commands.
`Match FILE`	Defines an object, that an Expert rule is intended to protect and to match an event. This command requires at lease one match object type value. For Files rule type, `FILE` is the match object type value.

`Include OBJECT_NAME { -v "c:\\temp\`
`\*test.txt"}`
`Include -access "CREATE"`
	In this section,
	• `Include` command involves the file path defined within OBJECT_NAME.
	• `Include -access "CREATE"` blocks user to create test.txt in c:\\temp\\ directory.

`Match FILE {`
`Include OBJECT_NAME { -v "c:\`
`\temp\\*test.dat"}`
`Include -access "CREATE WRITE`
`READ"`
`}`
	As more than one file needs protection, subrules are defined in this Expert rule. Within the file directory c:\\temp\\, users cannot create, write, and read the file called test.dat.

For more Expert Rules examples, visit the Trellix Github repository.

Detect InstallUtil execution

Most of the malicious software uses InstallUtil to execute the untrusted files. This sample Expert rule detects when InstallUtil is used to execute .exe or .dll files.

You can exclude the known and trusted applications in the rule, to allow the regular processes for executing .exe and .dll files.

Attention

Make sure to test this Expert rule on a client system before enforcing wider.

```
Rule {
Process {
    Include DESCRIPTION { -v ".NET Framework installation utility" }
}
Target {
    Match FILE {
        Include OBJECT_NAME { -v "**.EXE**"  }
        Include OBJECT_NAME { -v "**.DLL**"  }

Exclude AggregateMatch {
        Include OBJECT_NAME { -v "C:\\WINDOWS\\**" }
        Include OBJECT_NAME { -v "C:\\PROGRAM FILES\\MCAFEE\\**" }
        Include OBJECT_NAME { -v "C:\\PROGRAM FILES\\COMMON FILES\\MCAFEE\\**" }
        Include OBJECT_NAME { -v "C:\\PROGRAM FILES (X86)\COMMON FILES\\MCAFEE\\**" }
        }

# Excluding known apps
        Exclude AggregateMatch {
            Include OBJECT_NAME { -v "**snake1.exe*" }
            Include MD5 { -v 2f3b994e836d731d04ad4cf0f37f10ab }
        }
        Include -access "READ WRITE CREATE EXECUTE"
        }
    }
}
```

For more Expert Rules examples, visit the Trellix Github repository.

Manage users from creating symbolic links and junctions

You can block non-privileged users or allow specific users from creating the symbolic links (symlinks) and junctions through cmd.exe, powershell.exe, or powershell_ise.exe by enforcing an Expert Rule using ePO.

Before you begin

- Identify the Security Identifiers(SID) groups or users that should be blocked or allowed to create symbolic links and junctions, in accordance with your corporate security policies. For more information about SID, refer Security identifiers on Microsoft's documentation.

- To allow the blocked users, ask them to run `whoami/groups` command in the Windows command prompt and know the SID groups they belong to.
- The Expert rule shown in this page is generic and covers the following permissions. For more information about security groups, refer Security identifiers on Microsoft's documentation.
    - System and High permissions — The groups that are allowed to run processes at Administrator permission level.
    - Medium and Low permissions — The groups that are allowed to run limited processes at Standard user and guest user level.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the **Signatures** section, click **Add Expert Rule**.
6. In the **Expert Rules Properties** page, specify the following fields.
   ENS assigns the ID number for the rule automatically starting with 20000.
    a. Enter **Rule name**.
    b. Select **Severity**.
       Trellix recommends selecting **High** severity for initial validation.
    c. Select **Action**.
       Trellix recommends selecting **Report** action for initial validation. You can select Block and Report check boxes after validating that the rule works appropriately.
    d. Select the **Use Expert Rule template** checkbox. This populates a template rule in the Rule content box based on the Rule type you select.
    e. Select **Files** in the Rule type drop-down list.
    f. Analyze which SID groups are appropriate to have permissions to create symbolic links and junctions, in accordance with your corporate security policies. Then, change the template code as shown here.
        - To allow specific users or groups, add their SID within Exclude AggregateMatch.
        - To block specific users or groups, remove their SID or do not mention their SIDs within Exclude AggregateMatch.

Attention

Make sure to validate this Expert rule on a client test system before enforcing wider.

```
Rule {
    Process {
        Include OBJECT_NAME { -v cmd.exe }
        Include OBJECT_NAME { -v powershell.exe }
        Include OBJECT_NAME { -v powershell_ise.exe }

        # exclude admin groups
        Exclude AggregateMatch {
            Include GROUP_SID { -v "S-1-16-12288" }
            Include GROUP_SID { -v "S-1-16-16384" }
```

```
        }
    }
    Target {
        Match FILE {
            Include -access SET_REPARSE
        }
    }
}
```

In this rule, the High Mandatory Level (S-1-16-12288) and System Mandatory Level (S-1-16-16384) Security IDs are included within the Exclude AggregateMatch section. This blocks the non-privileged users and runs the process at administrative and system integrity level.

7. Save the rule, then save the settings.
8. Validate the new Expert Rule on the client system.
9. Enforce the policy on a client system.
   For more Expert Rules examples, visit the Trellix Github repository.

Expert Rules to protect processes

Create Expert Rules to protect processes using ePO

Expert rules can prevent endpoints from corrupting critical system processes and terminating security applications. You can create the Expert rules using ePO and protect processes by enforcing it in endpoints.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the Signatures section, click **Add Expert Rule**.
6. In the **Expert Rules Properties** page, complete the fields.
   ENS assigns the ID number for the rule automatically starting with 20000.
   a. In the **Rule Name**, provide a unique name for the Expert rule.
   b. Select the severity level according to the Expert rule.
      The severity provides information only; it has no effect on the rule action.
   c. Select **Block** and **Report** actions for the rule by selecting the corresponding check boxes.
      Trellix recommends selecting **Report** action for initial validation. You can select **Block** and **Report** checkboxes after validating that the rule triggers the appropriate events.
   d. Select the **Use Expert Rule template** checkbox. This populates a template rule in the Rule content box based on the Rule type you select.
      To get a blank template for writing the Expert rules, deselect **Use Expert Rule template**.
   e. Select **Processes** in the Rule type drop-down list.
7. Save the rule, then save the settings.
8. Validate the new policy on a client system.

9. Enforce the policy on the client systems.

Create Expert Rules for processes on client system

You can create Expert rules directly on a client system or self-managed endpoints that aren't managed by ePO.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to Full access or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Launch the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. In the **Signatures** section:
   - Create a rule — Click **Add Expert Rule**.
   - Edit an existing user-defined rule — Double-click the rule in the table.
5. In the **Expert Rule Checker** page, complete the fields.
   Trellix ENS assigns the ID number automatically starting with 20000.
   a. Select the severity and action for the rule.
      The severity provides information only; it has no effect on the rule action.
   b. Select **Processes** in the Rule Type drop-down list.
   c. Add the rule code to the **Rule content** field.
6. Save the rule, then save the settings.
7. Validate the new Expert Rule on the client system.

Expert Rule syntax to protect processes

To write an expert rule to protect the Windows processes, you need to ensure that it follows the correct syntax. Expert rules consist of process, one or more targets, and the matching conditions that rules must examine before allowing the source to access the processes.

Here is a sample Expert rule for registry rule type and their respective definitions:

Caution

Expert Rule commands are case-sensitive.

```
Rule {
    Process {
        Include OBJECT_NAME {
            -v "**"
        }
    }
```

```
    Target {
        Match PROCESS {
            Include OBJECT_NAME {..}
            Include -access "DELETE TERMINATING" ; # Define access types
                   Exclude -access "CREATE"
        }
    }
}
```

To add more commands in Expert rules, see Learn Expert Rules commands for Files, Processes, and Registry.

Sections of Expert Rule syntax in detail

The above Expert rule syntax is described here:

`Rule`	Formulates the execution of commands defined within `Process` and `Target`.
`Process`	Executes the set of actions defined within the `Include` and `Exclude` commands. It does not take any other commands.

`Include OBJECT_NAME {`
`-v "**"`
`}`
`Exclude .. {..}`
	In this section,
	• The `Include` command involves the specified object name during processing. When you specify `-v "**"`, all possible interfaces that users/applications can interact with Windows are involved. To be more specific, you can write the object names such as `powershell.exe`, or `explorer.exe`, or `cmd.exe`.
	• The `Exclude` command eliminates the defined object name while processing.
	For more information, see Object name guidelines and Match types values.

`Target`	Defines the target matches for the rule. This command takes no arguments and can contain only `Match` commands. A rule must contain at least one or more `Target` commands.
`Match PROCESS`	Defines an object, that an Expert rule is intended to protect and to match an event. This command requires at lease one match object type value.

Based on the object that needs protection, you use can one of these match object type values:

Match object_type_value	Description	Valid match object value
`PROCESS`	Controls access to an entire process handle.	• Initiator • Target **Note:** If PROCESS is not used in the Initiator match, you must use THREAD.
`SECTION`	Controls access to creating a section object.	Target

		Note: If the access to be blocked is CREATE, the object type must be SECTION rather than PROCESS.
`THREAD`	Controls access to a threat handle.	• Initiator • Target **Note:** If THREAD is not used in the Initiator match, you must use PROCESS.

`Include OBJECT_NAME {` `  -v notepad.exe`	This section defines the target object name, that is, Windows program to be secured.
`Include -access "DELETE TERMINATING"` `Exclude -access "CREATE"`	During processing, the `Include -access` and `Exclude-access` commands denote the access types for the specified program. You can write multiple access types together. For example, in this code snippet: • `Include -access "DELETE TERMINATING"` blocks the deletion and termination of object `notepad.exe`. • `Exclude -access "CREATE"` allows the creation of process or thread. The processes rule type supports these access types: • CREATE • DELETE • LOAD/IMAGE • TERMINATING • WRITE To know more about the access flags, refer ACCESS_MASK flags.

For more Expert Rules examples, visit the Trellix Github repository.

Sample Expert Rules to protect Processes

Prevent notepad execution

This Expert rule prevents users from executing notepad.exe through Windows File explorer. It also considers the size of the main module memory section.

Attention

Make sure to test this Expert rule on a client system before enforcing wider.

```
Rule {
    Process {
        Include OBJECT_NAME {
            -v explorer.exe
        }
    }
```

```
    Target {
        Match SECTION {
            Include OBJECT_NAME {
                -v "notepad.exe"
            }
            Include OBJECT_SIZE {
                -v 12345678
            }
            Include -access "EXECUTE" ; # Prevents section execution
        }
    }
}
```

When you validate this rule, execute the file C:\Windows\notepad.exe. This triggers an event in Trellix Endpoint Security (ENS) Client.

For more Expert Rules examples, visit the Trellix Github repository.

Block specific PowerShell parameters

This example rule prevents PowerShell from executing with specific command-line parameters, except for the encoded command, which is "dir c:\program files".

```
Rule {
        Process {
                Include OBJECT_NAME      { -v "*PowerShell*" }
                Include PROCESS_CMD_LINE { -v "*-NoLogo*" }
                Include PROCESS_CMD_LINE { -v "*-File*" }
                Include PROCESS_CMD_LINE { -v "*-EncodedCommand*" }
                Include PROCESS_CMD_LINE { -v "*-Command*" }
                Exclude PROCESS_CMD_LINE { -v "*-EncodedCommand
                                ZABpAHIAIAAnAGMAOgBcAHAAcgBvAGcAcgBhAG0AIABmAGkAbABlAHMAJwAgAA==" }
        }
        Target {
                Match SECTION { Include -access "CREATE" }
        }
}
```

For more Expert Rules examples, visit the Trellix Github repository.

Trigger a process scan

These examples show how to use the Reaction SCAN in the Expert Rule to trigger a process scan.

Example 1: Expert Rule with Reaction SCAN to scan actor process

When abc.exe launches xyz.exe, the Reaction SCAN ACTOR_PROCESS scans the actor process (abc.exe).

```
Rule {
    Reaction SCAN ACTOR_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
    Process {
        Include OBJECT_NAME { -v abc.exe}
    }
```

```
    Target {
        Match PROCESS {
            Include OBJECT_NAME { -v xyz.exe}
            Include -access "CREATE"
        }
   }
}
```

Example 2: Expert Rule with Reaction SCAN to scan target process

When abc.exe launches xyz.exe, the Reaction SCAN TARGET_PROCESS scans the target process (xyz.exe).

```
Rule {
    Reaction SCAN TARGET_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
    Process {
        Include OBJECT_NAME { -v abc.exe}
    }
    Target {
        Match PROCESS {
            Include OBJECT_NAME { -v xyz.exe}
            Include -access "CREATE"
        }
   }
}
```

Example 3: Expert Rule with Reaction SCAN to scan actor process when it accesses specific registry location

When the actor process (abc.exe) accesses a registry location that starts with HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options, it triggers a process scan of abc.exe.

```
Rule {
    Reaction SCAN ACTOR_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
    Process {
        Include OBJECT_NAME { -v abc.exe }
    }
    Target {
        Match KEY {
       Include OBJECT_NAME { -v "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File
Execution Options**"}
            Include -access "READ"
        }
   }
}
```

Example 4: Expert Rule with Reaction SCAN to scan actor and target process

When abc.exe launches xyz.exe, the Reaction SCAN ACTOR_PROCESS scans the actor process (abc.exe) and the Reaction SCAN TARGET_PROCESS scans the target process (xyz.exe).

```
Rule {
    Reaction SCAN ACTOR_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
    Reaction SCAN TARGET_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
    Process {
        Include OBJECT_NAME { -v abc.exe}
```

```
    }
    Target {
        Match PROCESS {
            Include OBJECT_NAME { -v xyz.exe}
            Include -access "CREATE"
        }
   }
}
```

Example 5: Chain rule (Next_Process_Behavior)

The Reaction SCAN command supports the Next_Process_Behavior chained rule ability. This Expert Rule shows that each Reaction SCAN command can have different scan actions.

```
Rule {
    Reaction SCAN ACTOR_PROCESS ScanAction REPORT
    Process {
        Include OBJECT_NAME { -v abc.exe }
    }
    Target {
        Match PROCESS {
            Include OBJECT_NAME { -v xyz.exe }
            Include -access "CREATE"
        }
        Next_Process_Behavior {
            Reaction SCAN ACTOR_PROCESS ScanAction REPORT_DELETE_PROCESS
            Reaction SCAN TARGET_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
            Target {
                Match PROCESS {
                    Include OBJECT_NAME { -v rmg.exe }
                    Include -access "CREATE"
                }
            }
        }
   }
}
```

For more Expert Rules examples, visit the Trellix Github repository.

Expert rules to protect Registry

Create Expert Rules to protect registry using ePO

Expert rule protects a specific registry by preventing users/unauthorized applications from accessing and modifying the registry keys or values in the registry. Based on the access permission you set in the rule, it blocks and triggers an event, if any unauthorized source access the protected registry.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.

4. Click **Show Advanced**.
5. In the **Signatures** section, click **Add Expert Rule**.
6. In the **Expert Rules Properties** page, complete the fields.
   Trellix ENS assigns the ID number for the rule automatically starting with 20000.
   a. In the **Rule Name**, provide a unique name for the Expert rule.
   b. Select **Block** and **Report** actions for the rule by selecting the corresponding check boxes.
      Trellix recommends selecting **Report** action for initial validation. You can select **Block** and **Report** check boxes after validating that the rule triggers the appropriate events.
   c. Select the **Severity** level according to the Expert rule.
      The severity provides information only; it has no effect on the rule action.
   d. Select the **Use Expert Rule template** checkbox. This populates a template rule in the Rule content box based on the Rule type you select.
      To get a blank template for writing the Expert rules, deselect **Use Expert Rule template**.
   e. Select **Registry** in the Rule type drop-down list.
7. Save the rule, then save the settings.
8. Validate the new policy on a client system.
9. Enforce the policy on the client systems.

Create Expert Rules for registry on client system

You can create Expert rules directly on a client system or self-managed endpoints that aren't managed by ePO.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to Full access or log on to the client system as administrator.

Task

1. Launch the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu  , select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. In the **Signatures** section:
   - Create a rule — Click **Add Expert Rule**.
   - Edit an existing user-defined rule — Double-click the rule in the table.
5. In the **Expert Rule Checker** page, complete the fields.
   Trellix ENS assigns the ID number automatically starting with 20000.
   a. Select the severity and action for the rule.
      The severity provides information only; it has no effect on the rule action.
   b. Select **Registry** in the Rule Type drop-down list.
   c. Add the rule code to the **Rule content** field.
6. Save the rule, then save the settings.
7. Validate the new Expert Rule on the client system.

Expert Rule syntax to protect registry

To write an expert rule to protect your registry, you need to ensure that it follows the correct syntax. Expert rules consist of process, one or more targets, and the matching conditions that rules must examine before allowing the source to access the registry.

Here is a sample Expert rule for registry rule type and their respective definitions:

⚠ Caution

Expert Rule commands are case-sensitive.

```
Rule {
        Process {
                Include OBJECT_NAME {
                        -v regedit.exe
                }
        }
        Target {
                Match KEY {
                        Include OBJECT_NAME {
                                -v "HKLMS\\test**"
                        }
                Include -access "CREATE WRITE DELETE REPLACE_KEY RESTORE_KEY"
                }
        }
}
```

For more Expert rules examples, visit the GitHub repository.

To add more commands in Expert rules, see Learn Expert Rules commands for Files, Processes, and Registry.

Sections of Expert Rule syntax in detail

The above Expert rule syntax is described here:

`Rule`	Formulates the execution of commands defined within `Process` and `Target`.
`Process`	Executes the set of actions defined within the `Include` and `Exclude` commands. It does not take any other commands.
`Include OBJECT_NAME {` `-v regedit.exe`	`Include` command defines the Match types. These match types are supported for the Registry rule type: • ACCESS_MASK • AUTHENTICATION_ID

<table>
<tr><td></td><td>

- NT_ACCESS_MASK
- OBJECT_NAME
- OS_VERSION
- REGVAL_DATA

For example, the <code>OBJECT_NAME</code> match type is uses here to specify the name of interface object, regedit.exe, the Registry Editor.
For more information, see Object name guidelines and Match types values.
</td></tr>
<tr><td>

```
Target
```

</td><td>Defines the target matches for the rule. This command takes no arguments and can contain only <code>Match</code> commands. A rule must contain at least one or more <code>Target</code> commands.</td></tr>
<tr><td>

```
Match KEY
```

</td><td>Defines an object, that an Expert rule is intended to protect and to match an event. This command requires at lease one match object type value. For registry rule type, <code>KEY</code> and <code>VALUE</code> are the match object type values.</td></tr>
<tr><td>

```
                        Include
OBJECT_NAME {
                                -v
"HKLMS\\test**"
```

</td><td>This section defines the target object name, that is, registry key path. These root keys are recognized:
<table>
<tr><th>Key</th><th>Matches</th></tr>
<tr><td>HKLM</td><td>HKLM is equivalent to HKEY_LOCAL_MACHINE.</td></tr>
<tr><td>HKCU</td><td>All user registry keys (not just the current user) and the .default user key.
HKCU is equivalent to:
• HKEY_CURRENT_USER
• HKEY_USERS</td></tr>
</table>
</td></tr>
</table>

	Note: Matching against specific user SIDs is not supported.
HKCUC	All user classes (HKCU/*_CLASSES).
HKCR	System classes and all user classes (HKCU/*_CLASSES). HKCR is equivalent to HKEY_CLASSES_ROOT.
HKCCS	• HKLM/SYSTEM/CurrentControlSet • HKLM/SYSTEM/ControlSet00X
HKLMS	• HKLM/Software on 32-bit and 64-bit systems • HKLM/Software/Wow6432Node on 64-bit systems only
HKCUS	• HKCU/Software on 32-bit and 64-bit systems • HKCU/Software/Wow6432Node

	<table><tr><td></td><td>on 64-bit systems only</td></tr><tr><td>HKULM</td><td>• HKLM • HKCU</td></tr><tr><td>HKULMS</td><td>• HKLMS • HKCUS</td></tr><tr><td>HKALL</td><td>• HKLM • HKU</td></tr></table> **Note:** If the rule specifies a name where the root starts or contains a wild character, the AAC code performs no name normalization and that name might never match correctly. For example, ****\mcshield\start** is a valid name, but **H*L*\mcshield\start** is not. HKEY_CURRENT_CONFIG is not supported.
`Include -access "CREATE WRITE DELETE REPLACE_KEY RESTORE_KEY"`	Defines the access flags. This flag applies when the protected registry key or value is accessed. The registry rule type supports these access flags: • CREATE • DELETE • ENUM • LOAD_KEY • QUERY • READ • RENAME • REPLACE_KEY • RESTORE_KEY • WRITE To know more about the access flags, refer ACCESS_MASK flags.

For more Expert Rules examples, visit the Trellix Github repository.

Sample Expert Rules to protect registry

Prevent changing registry value

This Expert rule prevents changing the registry value available in the hive HKLMS\test through the Registry Editor.

Attention

Make sure to validate this rule in a client test system before enforcing it wider.

```
Rule {
        Process {
                Include OBJECT_NAME {
                        -v regedit.exe
                }
        }
Target {
        Match KEY {
                Include OBJECT_NAME {
                        -v "HKLMS\\test**"
                }
                Include -access "CREATE WRITE DELETE REPLACE_KEY RESTORE_KEY"
                }
        }
}
```

For more Expert Rules examples, visit the Trellix Github repository.

Prevent DLL injection through AppInit_DLLs

This Expert rule detects the untrusted process of injecting custom DLLs into the critical processes through AppInit_DLLs registry entry. When DLL adds into this registry entry, it forces user32.dll to load the DLL module during process startup.

Attention

Make sure to validate this rule in a client test system before enforcing it wider.

```
Rule {
    Process {
        Include VTP_TRUST true
    }
    Target {
        Match KEY {
            Include OBJECT_NAME {
                -v "HKLMS\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION\\WINDOWS\\*_DLLs"
            }
            Include -access "CREATE WRITE DELETE REPLACE_KEY RESTORE_KEY"
        }
```

```
        Match VALUE {
            Include OBJECT_NAME {
                                -v "HKLMS\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION\\WINDOWS\\*_DLLs"
            }
            Include -access "CREATE WRITE DELETE REPLACE_KEY RESTORE_KEY"
        }
    }
}
```

Sections of Expert Rule in detail

`Rule`	Formulates the execution of commands defined within `Process` and `Target`.
`Process`	Executes the set of actions defined within the `Include` and `Exclude` commands. It does not take any other commands.
`Include VTP_TRUST true`	Checks if VTP trusts the process or file. The value is treated as Boolean. That is, a value of 1 in the match type matches only processes trusted by VTP. A value of 0 matches non-trusted processes.
`Target`	Executes the `Match` command.
`Match KEY { Include OBJECT_NAME { -v "HKLMS\\MICROSOFT\\WINDOWS NT\ \CURRENTVERSION\\WINDOWS\\*_DLLs" } Include -access "CREATE WRITE DELETE REPLACE_KEY RESTORE_KEY"`	This section controls create, edit and delete access to key data in a key object, available in the folder, `HKLMS\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION\ \WINDOWS\\*_DLLs`.
`Match VALUE { Include OBJECT_NAME { -v "HKLMS\\MICROSOFT\ \WINDOWS NT\\CURRENTVERSION\\WINDOWS\ \*_DLLs" } Include -access "CREATE WRITE DELETE REPLACE_KEY RESTORE_KEY"\\*_DLLs"`	This section controls create, edit and delete access to value data in a key object, available in the folder, `HKLMS\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION\ \WINDOWS\\*_DLLs`.

The following actions can trigger events in the Event log page of ENS client:

- accessing the hive, `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows`

- creating a key, test.DLLs
- creating a DWORD value, test_DLLs
- creating a key, test_DLAs

For more Expert Rules examples, visit the Trellix Github repository.

Detect exporting SAM from registry

This Expert rule detects when unauthorized users/applications access Windows registry to export the Security Account Manager (SAM) database file.

Attention

Make sure to test this Expert rule on a client system before enforcing wider.

```
Rule {
    Process {
        Include AggregateMatch -xtype "1" {
            Exclude VTP_PRIVILEGES -type BITMASK { -v 0x8 }
        }
        Include AggregateMatch -xtype "2" {
            Exclude OBJECT_NAME { -v "TIWORKER.EXE" }
            Exclude OBJECT_NAME { -v "DEVICECENSUS.EXE" }
            Exclude OBJECT_NAME { -v "TRUSTEDINSTALLER.EXE" }
            Exclude OBJECT_NAME { -v "TASKHOSTW.EXE" }
            Exclude OBJECT_NAME { -v "OMADMCLIENT.EXE" }
            Exclude OBJECT_NAME { -v "SERVICES.EXE" }
            Exclude OBJECT_NAME { -v "CSRSS.EXE" }
            Exclude OBJECT_NAME { -v "SVCHOST.EXE" }
            Exclude OBJECT_NAME { -v "WINLOGON.EXE" }
            Exclude OBJECT_NAME { -v "SCHTASKS.EXE" }
            Exclude OBJECT_NAME { -v "REGEDIT.EXE" }
            Exclude OBJECT_NAME { -v "UpdateNotificationMgr.exe" }
            Exclude OBJECT_NAME { -v "**\\Program Files\\Common Files\\microsoft shared\\ClickToRun\
\*.exe" }
            Exclude OBJECT_NAME { -v "**\\Program Files (x86)\\Common Files\\microsoft shared\\ClickToRun\
\*.exe" }
            Exclude OBJECT_NAME { -v "**\\program files\\microsoft office\\**.exe" }
            Exclude OBJECT_NAME { -v "**\\program files (x86)\\microsoft office\\**.exe" }
            }
      }
      Target {
          Match KEY {
Include OBJECT_NAME { -v "HKLM\\SAM" }
Include OBJECT_NAME { -v "HKLM\\SAM\\Domain\\Account" }
Include OBJECT_NAME { -v "HKLM\\SECURITY\\Policy\\Secrets"}
Include -access "READ"
}
}
}
```

For more Expert Rules examples, visit the Trellix Github repository.

Expert rules to protect Buffer overflow

Create Expert Rules to prevent Buffer Overflow using ePO

You can create Expert rules to prevent buffer overflow exploits for the applications listed in the **Application Protection**. If not prevented, an attacker could use this vulnerability to execute custom hacking code on the machine and compromise security and data integrity.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the Signatures section, click **Add Expert Rule**.
6. In the **Expert Rules Properties** page, complete the fields.
   ENS assigns the ID number for the rule automatically starting with 20000.
   a. In the **Rule Name**, provide a unique name for the Expert rule.
   b. Select **Block** and **Report** actions for the rule by selecting the corresponding checkboxes.
      Trellix recommends selecting **Report** action for initial validation. You can select **Block** and **Report** check boxes after validating that the rule works appropriately.
   c. Select the **Severity** level according to the Expert rule.
      The severity provides information only; it has no effect on the rule action.
   d. Select the **Use Expert Rule template** checkbox. This populates a template rule in the Rule content box based on the Rule type you select.
      To get a blank template for writing the Expert rules, deselect **Use Expert Rule template**.
   e. Select **Buffer Overflow** in the Rule type drop-down list.
7. Save the rule, then save the settings.
8. Validate the new policy on a client system.
9. Enforce the policy on the client systems.

Create Expert Rules for Buffer Overflow on client system

You can create Expert rules directly on a client system or self-managed endpoints that aren't managed by ePO.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to Full access or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Launch the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.

4. In the **Signatures** section:
    - Create a rule — Click **Add Expert Rule**.
    - Edit an existing user-defined rule — Double-click the rule in the table.
5. In the **Expert Rule Checker** page, complete the fields.
   Trellix ENS assigns the ID number automatically starting with 20000.
    a. Select the severity and action for the rule.
       The severity provides information only; it has no effect on the rule action.
    b. Select **Buffer Overflow** in the Rule Type drop-down list.
    c. Add the rule code to the **Rule content** field.
6. Save the rule, then save the settings.
7. Validate the new Expert Rule on the client system.

Sample Expert Rule to prevent Buffer Overflow

To write an expert rule to prevent buffer overflow exploits, you need to ensure that it follows the correct syntax. This rule type is built based on the legacy McAfee Host IPS.

Here is a sample Expert rule for buffer overflow rule type and their respective definitions:

⚠ Caution

Expert Rule commands are case-sensitive.

```
Rule {
   time {Include "*"}
   application {Include "*"}
   user_name {Include "*"}
   attributes -no_trusted_apps -not_auditable
   directives "-d" "-c" "bo:stack" "bo:heap"
}
```

To add more commands in Expert rules, see Learn Expert Rules commands for Buffer overflow, Illegal API use and Services..

Sections of Expert Rule in detail

The above Expert rule is described here:

`Rule`	Formulates the execution of the defined commands.
`time {Include "*"}`	A section works based on the value mentioned in the `Include` keyword. For more information, see Include and Exclude keywords.

`application {Include "*"}`	Indicates that this rule is valid for all processes. To limit the rule to specific processes, list the pathname to each process.
`user_name {Include "*"}`	Indicates that this rule is valid for all users (or more precisely, the security context in which a process runs). To limit the rule to specific user contexts, list them using the form Local/user or Domain/user.
`attributes -no_trusted_apps -not_auditable`	Defines an object, that an Expert rule is intended to protect and to match an event. This command requires at lease one match object type value. For Files rule type, `FILE` is the match object type value.
`attributes -no_trusted_apps -not_auditable`	In this section, • `-no_trusted_apps` — Specifies that the trusted application list doesn't apply to this signature. • `-not_auditable` — Generates no exceptions for the signature when Adaptive mode is enabled.
`directives "-d" "-c" "bo:stack" "bo:heap"`	Directives add these behaviors: • `bo:stack` — Examines the memory location that is executing and detects if it is running from writable memory that is part of the current thread's stack. • `bo:heap` — Examines the memory location that is executing and detects if it is running from writable memory that is part of a heap. For more directives, see Buffer Overflow class type.

Expert rules to protect Illegal API use

Create Expert Rules to prevent Illegal API use using ePO

You can create Expert rules to prevent illegal use of the Exploit Prevention API. The Expert Rules can only extend the functionality of the Illegal API Use signatures provided by Exploit Prevention content. Expert Rules can't refer to APIs that aren't already covered in an Illegal API Use signature available in content.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.
2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the Signatures section, click **Add Expert Rule**.
6. In the **Expert Rules Properties** page, complete the fields.
   ENS assigns the ID number for the rule automatically starting with 20000.
   a. In the **Rule Name**, provide a unique name for the Expert rule.
   b. Select **Block** and **Report** actions for the rule by selecting the corresponding checkboxes.
      Trellix recommends selecting **Report** action for initial validation. You can select **Block** and **Report** check boxes after validating that the rule works appropriately.
   c. Select the **Severity** level according to the Expert rule.
      The severity provides information only; it has no effect on the rule action.
   d. Select the **Use Expert Rule template** checkbox. This populates a template rule in the Rule content box based on the Rule type you select.
      To get a blank template for writing the Expert rules, deselect **Use Expert Rule template**.
   e. Select **Illegal API Use** in the Rule type drop-down list.
7. Save the rule, then save the settings.
8. Validate the new policy on a client system.
9. Enforce the policy on the client systems.

Create Expert Rules for Illegal API Use on client system

You can create Expert rules directly on a client system or self-managed endpoints that aren't managed by ePO.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to Full access or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Launch the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu , select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. In the **Signatures** section:
   - Create a rule — Click **Add Expert Rule**.
   - Edit an existing user-defined rule — Double-click the rule in the table.
5. In the **Expert Rule Checker** page, complete the fields.
   Trellix ENS assigns the ID number automatically starting with 20000.
   a. Select the severity and action for the rule.

The severity provides information only; it has no effect on the rule action.

b. Select **Illegal API Use** in the Rule Type drop-down list.

c. Add the rule code to the **Rule content** field.

6. Save the rule, then save the settings.
7. Validate the new Expert Rule on the client system.

Sample Expert Rule to prevent Illegal API Use

To write an expert rule to prevent illegal API use, you need to ensure that it follows the correct syntax. This rule type is built based on the legacy Trellix Host IPS.

Here is a sample Expert rule for illegal API use rule type:

⚠ Caution

Expert Rule commands are case-sensitive.

```
Rule {
        time {Include "*"}
        if { $EAGENT_64Bit_Process } {
                                          application {Include "[iEnv SystemRoot]\\system32\
\WindowsPowerShell\\*\\powershell.exe" \
                                                       "[iEnv SystemRoot]\\syswow64\\WindowsPowerShell\
\*\\powershell.exe"
                                                       }
                                       } else {
                                              application {Include "[iEnv SystemRoot]\\system32\
\WindowsPowerShell\\*\\powershell.exe" }
                                       }
        user_name {Include "*"}
        Vulnerability_Name {Include "Powershell Command Restriction - NoLogo"}
        directives "-d" "-c" "illegal_api_use:bad_parameter" "illegal_api_use:invalid_call"
        attributes -not_auditable
}
```

To know more about Expert rules commands, see Learn Expert Rules commands for Buffer overflow, Illegal API use and Services..

Expert rules to protect Services

Create Expert Rules to protect Services using Trellix ePO - On-prem

You can create Expert rules to protect the Windows Services (Windows versions 8.0 and earlier only). You can also create custom Services rules in the Access Protection policy in Threat Prevention. But, these rules don't provide the complete functionality available with Expert rules.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Products** list in the left pane.

2. From the **Category** list in the right pane, select **Exploit Prevention**.
3. Click the **Edit** link for an editable policy.
4. Click **Show Advanced**.
5. In the Signatures section, click **Add Expert Rule**.
6. In the **Expert Rules Properties** page, complete the fields.
   Trellix ENS assigns the ID number for the rule automatically starting with 20000.
   a. In the **Rule Name**, provide a unique name for the Expert rule.
   b. Select **Block** and **Report** actions for the rule by selecting the corresponding checkboxes.
      Trellix recommends selecting **Report** action for initial validation. You can select **Block** and **Report** check boxes after validating that the rule works appropriately.
   c. Select the **Severity** level according to the Expert rule.
      The severity provides information only; it has no effect on the rule action.
   d. Select the **Use Expert Rule template** checkbox. This populates a template rule in the Rule content box based on the Rule type you select.
      To get a blank template for writing the Expert rules, deselect **Use Expert Rule template**.
   e. Select **Services** in the Rule type drop-down list.
7. Save the rule, then save the settings.
8. Validate the new policy on a client system.
9. Enforce the policy on the client systems.

Create Expert Rules to protect Services on client system

You can create Expert rules directly on a client system or self-managed endpoints that aren't managed by ePO.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to Full access or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Task

1. Launch the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. In the **Signatures** section:
   - Create a rule — Click **Add Expert Rule**.
   - Edit an existing user-defined rule — Double-click the rule in the table.
5. In the **Expert Rule Checker** page, complete the fields.
   Trellix ENS assigns the ID number automatically starting with 20000.
   a. Select the severity and action for the rule.
      The severity provides information only; it has no effect on the rule action.
   b. Select **Services** in the Rule Type drop-down list.
   c. Add the rule code to the **Rule content** field.
6. Save the rule, then save the settings.

7. Validate the new Expert Rule on the client system.

Sample Expert Rule to protect Services

To write an expert rule to protect Windows Services (Windows versions 8.0 and earlier only), you need to ensure that it follows the correct syntax. This rule type syntaxes are built based on the legacy Trellix Host IPS.

Here is a sample Expert rule for services rule type that prevents deactivation of Alerter service:

⚠ Caution

Expert Rule commands are case-sensitive.

```
Rule {
services { Include "Alerter" }
application { Include "*"}
user_name { Include "*" }
directives services:stop
}
```

To add more commands in Expert rules, see Learn Expert Rules commands for Buffer overflow, Illegal API use and Services..

Sections of Expert Rule in detail

The above Expert rule is described here:

`Rule`	Formulates the execution of the defined commands.
`services { Include "Alerter" }`	Indicates that the rule applies to the service with name **Alerter**. If the rule applies to multiple services, add them in this section in different lines.
`application {Include "*"}`	Indicates that this rule is valid for all processes. To limit the rule to specific processes, list the pathname to each process.
`user_name {Include "*"}`	Indicates that this rule is valid for all users (or more precisely, the security context in which a process runs). To limit the rule to specific user contexts, list them using the form Local/user or Domain/user.

`directives services:stop`	Indicates that this rule applies to deactivation of a service.

Validate and enforce an Expert Rule on a client system

Once you deploy a new Expert Rule to a client test system, validate that the syntax is correct and that it is working properly before deploying more widely. Validate that the syntax for an Expert Rule is correct and enforce it on a client test system to verify that it is working properly before deploying more widely. Syntax checking is available for Files, Registry, and Processes rule types only.

Before you begin

Make sure that the interface mode for the Trellix Endpoint Security (ENS) Client is set to **Full access** or log on to the Trellix Endpoint Security (ENS) Client as administrator.

Policy changes from Trellix ePO - On-prem might overwrite changes that you make to Expert Rules on the client system. Make sure to copy your changes back to the **Exploit Prevention** policy in the Threat Prevention module in Trellix ePO - On-prem.

Task

1. Open the Trellix Endpoint Security (ENS) Client.
2. Click **Threat Prevention** on the main **Status** page.
   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Exploit Prevention**.
5. In the **Signatures** section, double-click a user-defined Expert Rule.
6. In the **Expert Rule Checker** window, click **Check**.
   The **Check** button isn't available for Buffer Overflow, Illegal API Use, or Services rule types.
   If the syntax checker finds any errors:
   a. Review the EndpointSecurityPlatform_errors.log file for information about the syntax error.
   b. In Trellix Endpoint Security (ENS) Client, correct the error.
   c. Click **Check**.
   The **Enforce** button enables when the errors are resolved.
7. Copy any updated Expert Rules to the **Exploit Prevention** policy in the Threat Prevention module in Trellix ePO - On-prem.
8. Click **Enforce** to save and enforce the rule or **Close** to cancel any changes and close the **Expert Rule Checker** window.
9. Perform the restricted actions that you have written in the rule.
10. Navigate back to the **Event Log** page in ENS.
    You can view the events that are triggered for violating the rule. If intended action is not reported, make sure that you have selected **Report** check box while creating or enforcing Expert rules.

Learn Expert Rules for files, processes, and registry

AAC rule structure

Rules define the boundaries of acceptable behavior and tell AAC how to react when the filtered action matches the rule specifications.

The `Rule` command at the root level defines the rule. Each Expert Rule identifier can contain only one rule definition and multiple subrules. The `Match` command defines subrules, each of which has an assigned role: `Initiator` or `Target`.

Because `Initiator` subrules always apply to PROCESS objects, the `Process` command provides a shortcut method for defining `Initiator` sections.

Note

Commands for building AAC rules are case sensitive.

Here is the basic structure of AAC-based rules:

```
Rule {
        Initiator {
                Match … {
                        Include … { … }
                        Exclude … { … }
                }
        }
        Target {
                Match … {
                        Include … { … }
                        Exclude … { … }
                }
        }
}
```

Note

Trellix ENS doesn't support signatures with multiple rules.

Expert Rule commands

Rule command

The `Rule` command defines an AAC rule. Each Expert Rule identifier can contain only one rule definition.

Description

This command takes no arguments and can contain one or more `Initiator`, `Process`, and `Target` commands. Only the `Target` command is required.

Syntax

```
Rule    {
        Initiator …
        Process …
        Target …
}
```

Initiator command

The `Initiator` command in a `Rule` command defines the AAC initiator matches. Only processes can be initiators.

Description

This command takes no arguments and can contain only `Match` commands.

A `Rule` command must contain at least one Initiator command and can contain multiple `Initiator` commands. If the value isn't specified, the rule uses ****** to indicate all processes.

Syntax

```
Rule {
        …
        Initiator       {
                Match …
        }
        …
}
```

Process command

The `Process` command provides a shortcut method for defining `Initiator` `Match` sections.

Description

This command takes no arguments and can contain multiple `Include` and `Exclude` commands.

A `Rule` command can contain multiple `Process` commands. The `Process` command is optional. If not specified, the rule uses the value ****** to indicate all processes.

Syntax

```
Rule {  ...
        Process {
        }
        ...
}
```

This syntax is a shortcut for:

```
Rule    { ...
        Initiator {
```

```
                Match PROCESS {
                }
        }
        ...
}
```

Target command

The `Target` command defines the AAC target matches for the rule.

Description

This command takes no arguments and can contain only `Match` commands.

A `Rule` must contain at least one `Target` command and can contain multiple `Target` commands.

Syntax

```
Rule {
        Target  {
                Match …
        }
 ...
}
```

Next_Process_Behavior command

The `Next_Process_Behavior` command defines a new chained link in the AAC target. You can use this command to create behavioral rules to block a specific sequence of actions.

Description

This command takes no arguments and can contain only `Target` commands.

A `Rule` command can contain multiple chained links definitions. Each `Next_Process_Behavior` command must be defined together with a `Match` command with the PROCESS *object_type_value* within a `Target` command.

Syntax

```
Rule { ...
 Target {
   Match PROCESS {
     ...
   }
   Next_Process_Behavior {
     Target {
       ...
     }
   }
 ...
 }
}
```

Match command

The `Match` command defines the criteria that AAC uses to match an event.

Description

This command takes one required argument, *object_type_value*, which specifies the case-sensitive AAC object type to match, and can contain multiple `Include` and `Exclude` commands.

The `Match` command can be used in `Initiator` and `Target` commands only.

Important

It is recommended to use a single `Match type - Object type`. When using two or more of the same `Match type - Object type`, it can lead to logic conflicts and will not work as expected if the rule contains logical contradictions. If use of a second `Match type - Object type` is required, the recommendation is to use a different `Object type`. For example, if the first `Match type` is *OBJECT_NAME*, then the second should use a different `Object type` like *TARGET_OBJECT_NAME*.

Syntax

```
Rule    {
        Initiator
                        Match object_type_value {
                                Include …
                                Exclude …
                        }
        }
        Target
                        Match object_type_value {
                                Include …
                                Exclude …
                        }
        }
}
```

Include and Exclude commands

The `Include` and `Exclude` commands specify the data used for matching.

Description

The `Include` and `Exclude` commands take two required arguments:

- *MATCH_type*, which determines the entries in an `Include` or `Exclude` that are ORed or ANDed
- The actual data to match The body of the command can contain multiple data entries. Each data entry must begin with either `-v` or `-l`.

Syntax

```
Rule    {
        Initiator
                Match   {
```

```
                        Include MATCH_type < -type PATH > {
                                -v data | -l data
                                ...
                        }
                }
        }
}
```

```
Rule    {
        Initiator
                Match   {
                        Exclude MATCH_type < -type PATH > {
                                -v data | -l data
                                ...
                        }
                }
        }
}
```

Arguments

Argument	Description
-v	Specifies to interpret the following entry as a single value.
-l	Specifies to interpret the following entry as a Tcl list — each entry in the list is automatically broken out into its own match entry.
-pfx	Specifies a string to prepend to all following data entries. The strings remain in effect until another `-pfx` option. To remove the current value, use this option with no string.
-sfx	Specifies a string to append to all following data entries. The strings remain in effect until another `-sfx` option. To remove the current value, use this option with no string.
-type PATH	Treats all entries in the body as paths and automatically removes any trailing directory separators: **/** or ****.

Argument	Description
	This is useful to avoid double separators when you are appending strings to the values with the `-sfx` option.

Shortcuts for MATCH_type

You can use the following shortcuts instead of building the entire *MATCH_type* entry.

Syntax

```
Include/Exclude -processor_mode  user|kernel
```

```
Include/Exclude -vtp_trust  true|false
```

```
Include/Exclude -access access_types
```

The *access_types* value is a list of access tokens separated by a delimiter and is case insensitive. The valid delimiters are a space, tab, comma, or pipe |.

The valid access tokens are:

- CLEANUP
- CLOSE
- CONNECT_NAMED_PIPE
- CREATE
- DELETE
- ENUM
- EXECUTE
- LOAD_IMAGE
- LOAD_KEY
- OBJECT_EXISTS
- OPEN_NAMEDSECTION
- POST
- QUERY
- READ
- REPLACE_KEY
- RESTORE_KEY
- SET_REPARSE
- SET_SECURITY
- START_DEVICE

- TERMINATING
- WRITE
- WRITE_ATTRIBUTE

AggregateMatch command

The `AggregateMatch` command defines a list of data that AAC uses to match an event. You can use this command to create a list of values to match in a rule so you can use the same data without having to rewrite the values.

Description

This command takes no arguments and can be used in `Include` and `Exclude` commands only.

The *Match_type* value is required for each item in `AggregateMatch`.

Syntax

```
Rule    {
 Initiator {
   Match object_type_value {
     Include AggregateMatch {
       Include ...
       Exclude ...
     }
     Exclude AggregateMatch {
       Include ...
       Exclude ...
     }
   }
 }
  ...
 Target {
   Match object_type_value {
     Include AggregateMatch {
       Include ...
       Exclude ...
     }
     Exclude AggregateMatch {
       Include ...
       Exclude ...
     }
   }
 }
 ...
}
```

Reaction SCAN command

The Reaction SCAN command defines the ability to perform process scans when a rule matches.

Description

Note

The Reaction SCAN command is available with Trellix ENS 10.7 November 2020 Update and later.

This command takes two arguments:

- Process to be scanned (ACTOR_PROCESS and/or TARGET_PROCESS).
- ScanAction, the action to take when a detection occurs.

Syntax

An example of a rule with the Reaction SCAN command. The command precedes the Process clause in this example of a simple Expert Rule where the Reaction SCAN command is used.

```
Rule {
    Reaction SCAN ACTOR_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
    Reaction SCAN TARGET_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
    Process {
        Include OBJECT_NAME { -v abc.exe}
    }
    Target {
        Match PROCESS {
            Include OBJECT_NAME { -v xyz.exe}
            Include -access "CREATE"
        }
   }
}
```

The Reaction SCAN command can also be used in chained Expert Rules. The command is placed at the top of the Next_Process_Behavior clause.

```
Rule {
    Reaction SCAN ACTOR_PROCESS ScanAction REPORT
    Process {
        Include OBJECT_NAME { -v abc.exe }
    }
    Target {
        Match PROCESS {
            Include OBJECT_NAME { -v xyz.exe }
            Include -access "CREATE"
        }
        Next_Process_Behavior {
                Reaction SCAN TARGET_PROCESS ScanAction REPORT
            Target {
                Match PROCESS {
                    Include OBJECT_NAME { -v rmg.exe }
                    Include -access "CREATE"
                }
            }
        }
    }
  }
```

Example

```
Reaction SCAN ACTOR_PROCESS ScanAction REPORT_CLEAN_DELETE_PROCESS
```

When the Expert Rule matches, the actor process is scanned with a scan action that tries to clean the process. If the clean action is not successful, it attempts to delete the process and will log the detection to On-Demand Scan Activity log and report the detection to Trellix ePO - On-prem.

```
Reaction SCAN TARGET_PROCESS ScanAction REPORT
```

When the Expert Rule matches, the target process is scanned with a scan action that will log the detection to On-Demand Scan Activity log and report the detection to Trellix ePO - On-prem.

For more detailed examples on how to use Reaction SCAN, see Expert rule triggered process scan.

Note

The process scan only works on processes, it does not work on files and registry. The process scan takes around 2 seconds to complete; on a detection the complete scan takes between 2–9 seconds to fix it.

Scan actions

These are the scan actions and their descriptions.

Scan action	Description
CLEAN_PROCESS	Attempts to clean the process. The detection is logged to the On-Demand Scan Activity log.
DELETE_PROCESS	Attempts to delete the process. The detection is logged to the On-Demand Scan Activity log.
CLEAN_DELETE_PROCESS	First attempts to clean the process, if unsuccessful then attempt to delete the process. The detection is logged to the On-Demand Scan Activity log.
REPORT	No action is taken on the detected process. The detection is logged to the On-Demand Scan Activity log and a detection event is sent to Trellix ePO - On-prem.

Scan action	Description
REPORT_CLEAN_PROCESS	Attempts to clean the process. The detection is logged to the On-Demand Scan Activity log and a detection event is sent to Trellix ePO - On-prem.
REPORT_DELETE_PROCESS	Attempts to delete the process. The detection is logged to the On-Demand Scan Activity log and a detection event is sent to Trellix ePO - On-prem.
REPORT_CLEAN_DELETE_PROCESS	First attempts to clean the process, if unsuccessful then attempt to delete the process. The detection is logged to the On-Demand Scan Activity log and a detection event is sent toTrellix ePO - On-prem.

If multiple Reaction SCAN commands are included in an Expert Rule, each command can have a different scan action.

Task-less process scan

When the Expert Rule matches, a process scan request is sent asynchronously to On-Demand Scan. The On-Demand Scan performs the process scan as a Task-less On-Demand Scan. This scan happens immediately and does not depend on the scheduled scan task.

Events and log details

Detection logging

If a detection occurs, the detection is logged in the On-Demand Scan Activity log. The detection information in the log includes the rule ID, rule name which triggered the scan, the name of the detected process, and the scan action (remediation action) taken.

Trellix ePO - On-prem events

If one of the report scan actions (REPORT, REPORT_CLEAN_PROCESS, REPORT_DELETE_PROCESS, REPORT_CLEAN_DELETE_PROCESS REPORT) is used, a detection event is sent to Trellix ePO - On-prem. The detection event follows the same format as of On-Demand Scan process scan detection events except for the fields **Task Name**, **Analyzer Rule ID**, and **Analyzer Rule Name**.

These fields are named in these format:

- **Expert Rule On-Demand Process Scan**
- **Expert Rule ID**
- **Expert Rule Name**

Scanned or not scanned log details

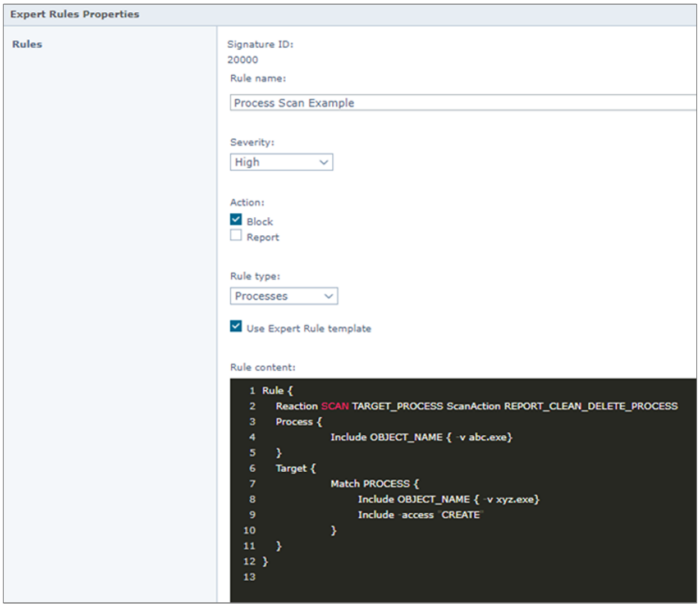
Each scan is logged to the On-Demand Scan Debug log. If a scan does not occur for some reason, the rule ID, rule name, process name, and the reason why the scan could not be completed is logged in the On-Demand Scan Activity log.

Debug logging

The complete flow of an Expert Rule triggering a process scan can be seen by enabling debug logging for Exploit Prevention and On-Demand Scan. The Expert Rule sending the scan request is seen in the Exploit Prevention Debug log, and the handling of the process scan is seen in On-Demand Scan Debug log.

Special consideration

- The process scan is not able to scan Windows protected process because it can't get access to the process memory. The inability to scan a process due to this is logged in the On-Demand Activity log, citing that the process scan is unable to access the process for scanning.
- It is possible to create Expert Rules which match thousands of times a second, and if the Expert Rule includes the Reaction SCAN command then, if unchecked, could request a process scan thousands of times a second. Therefore safeguards are in place that will limit one process scan, per process at a time.
- Expert Rule action can be executed to block and report. In the given example, the Expert Rule is configured to block creating xyz.exe and it also has a reaction to scan the target process, xyz.exe. In this case, the process scan does not occur because the process launch is blocked. The attempt to perform process scan on xyz.exe fails because the scanner is not able to access the xyz.exe process.



How match criteria in AAC-based subrules are evaluated

The match criteria in each subrule specifies either the `Include` or `Exclude` directive. The rule engine evaluates the filtered event against the match criteria in the subrule.

The subrule matches the filtered event if both of the following are true:

- At least one `Initiator` subrule matches the process that initiated the action described by the event.
- At least one `Target` subrule matches the object type that is the subject of the action.

When evaluating a filtered event against a subrule, the rule engine performs logical OR between matching criteria of the same type and logical AND between matches of different type. The rule engine first evaluates the matches with the `Exclude` directive, and then evaluates the matches with the `Include` directive.

The subrule evaluates to TRUE if both of the following are true:

- Exclude matches evaluate to FALSE.
- Include matches evaluate to TRUE.

Example

```
Rule {
        Initiator {
                Match PROCESS {
                                Include OBJECT_TYPE_A      { … }
                                Include OBJECT_TYPE_B      { condition 1 }
                                Include OBJECT_TYPE_B      { condition 2 }
                                Exclude OBJECT_TYPE_C      { … }
                        }
                Target {
                        Include OBJECT_TYPE_D     { condition 1 }
                        Include OBJECT_TYPE_D     { condition 2 }
                }
}
```

This rule evaluates to TRUE if both the following are TRUE:

- One of the following `Initiator` conditions is TRUE:
  - OBJECT_TYPE_A and OBJECT_TYPE_B condition 1 are TRUE.
  - OBJECT_TYPE_A and OBJECT_TYPE_B condition 2 are TRUE.
  - OBJECT_TYPE_A is TRUE and OBJECT_TYPE_C is FALSE.
- One of the following `Target` conditions is TRUE:
  - OBJECT_TYPE_D condition 1 is TRUE.
  - OBJECT_TYPE_D condition 2 is TRUE.

Valid parent-child relationships between AAC commands

The AAC syntax defines which commands can be the parent or children of other commands.

Command	Parent	Children
Rule	Not applicable	Initiator
		Process

Command	Parent	Children
		Target
Initiator	Rule	Match
Process	Rule	Include
		Exclude
Target	Rule	Match
Match	Initiator	Include
	Target	Exclude
Include	Process	Not applicable
	Match	
Exclude	Process	Not applicable
	Match	

Match object type values

The `Match` command takes one required argument, *object_type_value*, which is the case-sensitive AAC object type to match.

This table lists the valid values of *object_type_value*.

Match object_type_ value	Description	Valid match object type	Notes
FILE	Controls access to a file.	Target	
KEY	Controls access to both key and value data in a key object.	Target	

Match object_type_value	Description	Valid match object type	Notes
PROCESS	Controls access to a process handle.	• Initiator • Target	If PROCESS is not used in the Initiator match, you must use THREAD. If the access to be blocked is CREATE, the object type must be SECTION rather than PROCESS.
SECTION	Controls access to creating a section object.	Target	
THREAD	Controls access to a thread handle.	• Initiator • Target	If THREAD is not used in the Initiator match, you must use PROCESS.
VALUE	Controls access to value data in a key object.	Target	

Match type values

The *MATCH_type* value determines which entries in an `Include` or `Exclude` are ORed or ANDed. Commands with the same *MATCH_type* value evaluate to either value (OR). Commands with different *MATCH_type* values evaluate to both values (AND).

Each *Match_type* value uses a specific data type for its possible values. The supported data types are:

- **INT*x*/UINT*x*** — All match 32-bit or 64-bit numeric values.
- **STRING** — A null-terminated text string.
- **BITMASK** — A numeric value expressed in hexadecimal notation, which is logically evaluated, such as 0xfe340ead.
- **BINARY** — Binary data specified as a hexadecimal value, such as fe340ead.
- **MULTI_STRING** — Sequence of null-terminated strings that are terminated by two null characters, such as "string1\0string2\0string3\0\0".
- **EXPANDABLE_STRING** — A null-terminated string that contains unexpanded references to environment variables, such as "%PATH%".

Note

MATCH_types values are case sensitive.

Match type value	Description	Data type	Valid in object types
ACCESS_MASK	Specifies the access type.	UINT64 - BITMASK	All
AUTHENTICATION_ID	Matches a textual account SDDL SID identifier. This match can be used to identify a specific user-account in policy enforcement.	STRING	All
CACHE_ATTRIBUTE	Matches a cache attribute for the given object. Because it is a bitmask match type, any matching bits are considered a match.	BITMASK	• FILE • PROCESS
CERT_HASH	Matches the certificate hash; doesn't check whether the cert is chained to the root. If the object is of type PROCESS or THREAD, the certificate is obtained from the main entry module. This match never evaluates to true if the object is not signed.	UINT8[16]	• PROCESS • SECTION • THREAD
CERT_NAME	Matches the object's signing certificate name, but doesn't check whether the	STRING	• PROCESS • SECTION • THREAD

Match type value	Description	Data type	Valid in object types
	certificate is chained to the root. If the object is of type PROCESS or THREAD, the certificate is obtained from the main entry module. This match never evaluates to true if the object is not signed.		
CERT_NAME_CHAINED	Matches the object's signing certificate name, and the signing certificate must be chained to the root of the certificate store. If the object is of type PROCESS or THREAD, the certificate is obtained from the main entry module. This match never evaluates to true if the object is not signed.	STRING	• PROCESS • SECTION • THREAD
DESCRIPTION	Matches the "FileDescription" resource extracted from the resource section for the PE.	STRING	• FILE • PROCESS • SECTION
DISKIO_HOOK	Specifies the source for the filtered disk IO, where `upper` designates IO origin to be the upper disk filter, mfedisk.sys and `miniport` and `firmware` refer to IOs originating	UINT32	DISK

Match type value	Description	Data type	Valid in object types
	from the CAPI library, mfecapik.sys.		
DISK_REGION	Specifies the accessed disk region types as defined by AAC. This matching criteria aids in creating minimal rules protecting special/ interesting disk areas. The defined bits are: • MBR — Matches access to the MBR (Master Boot Record) and the subsequent 63 sectors. For GPT-style disks, this bit also applies to accesses to the partition table (LBAs 1–33 inclusive), including the mirror table at the end of the disk. • VBR — Matches access to the VBR (Volume Boot Record). • PARTITION — The accessed LBAs are in a single partition. • NOT_PARTITIONED — One or more of the accessed LBAs are in an area that is not partitioned. This bit always matches access to RAW/uninitialized disks.	UINT64 - BITMASK	DISK

Match type value	Description	Data type	Valid in object types
	• MULTI_PARTITION — The accessed LBAs span more than one partition.		
DLL_LOADED	Matches a loaded DLL in a specified PROCESS object. This is primarily useful for narrowing `Initiator` matches, such as svchost.exe service exclusions. The DLL name generally is the base name of the DLL without a path or file extension. That is, “MFEVTPA” matches, whereas “MFEVTPA.DLL” or “c:\program files\common files\mcafee\systemcore\mfevtpa.dll”. The match data is pulled directly from the process structures where the DLL is known by its base name and the associated image file name is not present. To match when the DLL is loaded, set the value part of the name-value bitmask to 1. To match when the DLL is not loaded, set it to 0.	BITMASK	PROCESS
ENV_VAR	Specifies an environment variable	Named value pair: STRING, STRING	• PROCESS • THREAD

Match type value	Description	Data type	Valid in object types
	name and its value. This criteria matches only if both name and value match the environment variables extracted from the PEB.		
EXP_USER_NAME	Selects the local account SID, when an authenticating authority isn't defined in the rule.	STRING	• FILE • PROCESS
FILE_ATIME	Matches against the file last accessed time.	INT64	• FILE • PROCESS
FILE_ATTRIBUTES	Matches against the file attribute bits.	BITMASK	• FILE • PROCESS
FILE_CTIME	Matches against the file create time.	INT64	• FILE • PROCESS
FILE_MTIME	Matches against the file last changed time.	INT64	• FILE • PROCESS
FILE_PROPERTIES	Matches the bitmask against file properties reported by the `Target`. The defined bits are: • NETWORK (0x1) — File is in a network path. • REMOVABLE (0x2) — File is on a removable drive. • FLOPPY (0x4) — File is on a floppy drive.	UINT64 - BITMASK	FILE

Match type value	Description	Data type	Valid in object types
	• CD (0x8) — File is on a CD drive. • DFS (0x10) — File is over on DFS. • REDIRECTOR (0x20) — File is opened using a redirector.		
GROUP_NAME	Matches the provided textual name against the groups that the user token belongs to. The criteria evaluates to true if at least one matching group is found.	STRING	• PROCESS • THREAD
GROUP_SID	Matches the provided textual SID (that is, S-1-5-18) against the groups that the user token belongs to. The criteria evaluates to true if at least one matching group is found.	STRING	• PROCESS • THREAD
IMAGE_BASE_ADDRESS	Specifies the virtual base address for an image. This is useful for retrieving the base address for an image during an image load notification.	UINT64	SECTION Available only during load image callbacks, access mask set to LOAD_IMAGE.
IMAGE_ENTRY_POINT	Specifies the entry point offset (in bytes) for an image.	UINT64	SECTION Available only during load image callbacks,

Match type value	Description	Data type	Valid in object types
	This is useful for retrieving the entry point address for an image during an image load notification.		access mask set to LOAD_IMAGE.
IMAGE_PROPERTIES	Specifies different image properties, as available during an image load notification. The defined bits are: • 64-bit — 64-bit image. • SYSTEM_MODE — System mode image. • MAPPED_TO_ALL_PROCESSES — The image is mapped to all processes.	UINT64 - BITMASK	SECTION Available only during load image callbacks, access mask set to LOAD_IMAGE.
IS_DIRECTORY	Matches operations against files or directories: • 0 — files • 1 — directories	UINT8 - Boolean	FILE
IS_TRANSACTED	Matches (true) if the file is part of an NTFS TxF transaction. For PROCESS or THREAD object types, matches if the backing file object for the main executable is part of an NTFS TxF transaction.	UINT8 - Boolean	• FILE • PROCESS • SECTION • THREAD
KERNEL_CALLER_NAME	Matches the name of the kernel module that issued the disk IO.	STRING	DISK Valid only in the context of DeepStore.

Match type value	Description	Data type	Valid in object types
LBA	Compares the specified LBA (Logical Block Address) to the one that is being accessed. The location of the MBR (Master Boot Record) is always LBA 0.	UINT64	DISK
LBA2FILE	While filtering disk I/O, matches the specified name against the name, according to the CAPI content driver, of the file in the filtered LBA.	STRING	DISK
LBA_FROM_END	Calculates the accessed LBA using a reverse scheme in which the last sector on the disk is considered to carry LBA 0. For example, match data that specifies range 0..1 matches access to the last 2 sectors. On a disk with N+1 blocks/sectors, where LBAN is the last block (using a 0-based scheme), match data 1..2 corresponds to access to LBAN-2 and LBAN-1. This criterion is provided for convenience, so that rules can protect several sectors, starting from an offset	UINT64	DISK

Match type value	Description	Data type	Valid in object types
	calculated from the end of the disk, without knowing the disk size.		
MD5	Indicates the MD5 digest of the backing file. If object is of type PROCESS or THREAD, MD5 is calculated against its main executable module.	UINT8	• FILE • PROCESS • SECTION • THREAD
NT_ACCESS_MASK	Matches against the native NT access mask of the I/O operation for file, registry, process, and thread access attempts. Make sure to use access masks appropriate for the object type as described in Microsoft MSDN. For example, to use NT_ACCESS_MASK to block calls to CreateFile() with GENERIC_WRITE, the bit mask must be FILE_GENERIC_WRITE.	UINT64 - BITMASK	• FILE • PROCESS • REGISTRY • THREAD

Match type value	Description	Data type	Valid in object types
	Note: Due to operating system limitations, you can't block PROCESS_QUERY_LIMITED_INFORMATION but you can use it in ALLOW rules for reporting purposes.		
OBJECT_NAME	Specifies the object name. Any combination of wildcards is accepted.	STRING	All
OBJECT_SIZE	Matches against the size of the file or, for a section, the image size during load.	INT64	• FILE • SECTION
OPERATION_STATUS	Matches the operation status for a post-event. Not useful with non-post events.	INT32	FILE
OS_VERSION	Compares the specified operating system version to the actual version. The operating system version must be specified in the format: `OS_Version = Major_Version * 1000 + Minor_Version * 10 + ServicePack.` By way of example: `VistaRtm = 6000; VistaSp1=6001; Win7=6010; Win7Sp1=6011; Win8=6020`	UINT32	All

Match type value	Description	Data type	Valid in object types
PARTITION_STYLE	Compares the match criteria with the partition style of the disk `Target`.	UINT32	DISK
PE	Matches a data value of "1" if the target file is a PE (Portable Executable, Windows executable binary) file. **Note:** `Initiator` PROCESS/THREAD matches are not supported because, by definition, they are PE files.	UINT8	FILE
PE_MD5	Compares MD5 digest calculated across PE against the match criteria. The digest is calculated according to Microsoft Authenticode PE hash value calculations – 4-byte PE header check sum is omitted as well as the Certificate Table Entry, which is part of Optional Header Directories.	UINT8	• FILE • PROCESS • SECTION • THREAD
PE_SHA1	Compares the match data with the SHA-1 hash sum calculated across the PE.	UINT8	• FILE • PROCESS • SECTION • THREAD

Match type value	Description	Data type	Valid in object types
PE_SHA2_256	Compares the match data with the SHA2-256 hash sum calculated across the PE.	UINT8	• FILE • PROCESS • SECTION • THREAD
PE_SHA2_384	Compares the match data with the SHA2-384 hash sum calculated across the PE.	UINT8	• FILE • PROCESS • SECTION • THREAD
PE_SHA2_512	Compares the match data with the SHA2-512 hash sum calculated across the PE.	UINT8	• FILE • PROCESS • SECTION • THREAD
PROCESSOR_MODE	Matches if the match is evaluated in the context of an I/O operation originating from user-mode or kernel-mode. This is most useful for excluding processes from matching a rule if the process is executing in user-mode. **Note:** Do not use this type with registry operations.	UINT8 - KPROCESSOR_MODE (0 = kernelmode, 1 = usermode)	• PROCESS • THREAD
PROCESS_CMD_LINE	Matches the process command line, extracted from the PEB (Process Environment Block), a data structure used by Microsoft Windows to hold	STRING	• PROCESS • THREAD

Match type value	Description	Data type	Valid in object types
	information about running processes.		
PROCESS_ID/ THREAD_ID	Matches a specified thread ID. **Note:** Remember when using this match type that thread IDs and process IDs are rapidly recycled in the Windows environment.	UINT64 - Thread ID	• PROCESS • THREAD
PROCESS_STATE_BITS	Compares the specified name/bitmask with the stateID/stateBits carried by the `Initiator` or `Target` ProcessInfo object. The comparison evaluates to true if stateBits with stateID are present in ProcessInfo and the “bitwise and” between the stateBits and the bitmask carried by the match object yields a non-zero result.	BITMASK	• PROCESS • THREAD
PRODUCT_NAME	Matches the "ProductName" resource extracted from the resource section of the PE.	STRING	• FILE • PROCESS • SECTION
REGVAL_DATA	Matches against registry value data in	This data type is variable. You must	REGISTRY

Match type value	Description	Data type	Valid in object types
	the context of a registry value set operation, either when a registry variable is created or its value is changed. You can use this *MATCH_type* value to control or filter the data being written or changed in a registry value.	specify it using the `-type` flag. Valid data types are the same as accepted by the Windows registry: • INT32 • INT64 • BINARY • STRING • MULTI_STRING • EXPANDABLE_STRING	
REMOTE_MACHINE_ADDRESS	**Note:** This type is for reporting only. If used for matching, matches the specified type against file I/O initiated by a specific SMB client IP address in either IPv4 or IPv6 format. In other words, this type does not match for file I/O initiated on the local system going to an SMB server. It only matches for client I/O going to the local SMB server. This match type is mostly useful for generating event details.	STRING	This match type is valid in PROCESS `Initiator` (requires OBJECT_NAME to match SYSTEM:REMOTE) or FILE `Target` match.
SESSION_ID	Compares the specified match criteria against the session ID that the process/thread belongs to and can apply to	UINT32	• PROCESS • THREAD

Match type value	Description	Data type	Valid in object types
	both `Initiator` and `Target` objects.		
SHA1	Compares the SHA-1 hash sum of the backing file with the match data. If the object is of type PROCESS or THREAD, the hash sum is calculated against its main executable module.	UINT8	• FILE • PROCESS • SECTION • THREAD
SHA2_256	Compares the SHA2-256 hash sum of the backing file with the match data. If the object is of type PROCESS or THREAD, the hash sum is calculated against its main executable module.	UINT8	• FILE • PROCESS • SECTION • THREAD
SHA2_384	Compares the SHA2-384 hash sum of the backing file with the match data. If the object is of type PROCESS or THREAD, the hash sum is calculated against its main executable module.	UINT8	• FILE • PROCESS • SECTION • THREAD
SHA2_512	Compares the SHA2-512 hash sum of the backing file with the match data.	UINT8	• FILE • PROCESS • SECTION

Match type value	Description	Data type	Valid in object types
	If the object is of type PROCESS or THREAD, the hash sum is calculated against its main executable module.		• THREAD
STORAGE_BUS_TYPE	Compares the match criteria with the storage bus type that the disk is attached to.	UINT32	DISK
TARGET_OBJECT _NAME	Specifies the object name. Any combination of wildcards is accepted. Names follow the same conventions as OBJECT_NAME. But, they only match against the target of a file rename operation. This enables rules to be written that only apply to rename operations based on both source (OBJECT_NAME) and target (TARGET_OBJECT_NAME) name. • OBJECT_NAME is not required. If it is not specified, any source matches. • ACCESS_MASK for a rename is DELETE, because it's from the perspective of the source file, even if the	STRING	FILE

Match type value	Description	Data type	Valid in object types
	OBJECT_NAME is not specified.		
USER_NAME	Matches the text representation of the user name.	STRING	• PROCESS • THREAD
USER_SID	Matches the text representation of the user account SID (that is, S-1-5-21-22-23-24-1168) .	STRING	• PROCESS • THREAD
VERSION_RESOURCE	Matches the “FileVersion” resource extracted from the resource section for the PE.	STRING	• FILE • PROCESS • SECTION
VERSION	Matches the version extracted from the resource section for the file.	STRING	• PROCESS • SECTION • THREAD
VTP_PRIVILEGES	Matches the bitmask against the VTP privileges of the target. The defined bits are: • PRIVILEGE_IOCTL (0x1) — Signed by a VTP-trusted certificate. • PRIVILEGE_ISG (0x8) — Signed by a Trellix certificate specifically. Files signed by Microsoft:	UINT64 - BITMASK	• FILE • PROCESS • THREAD

Match type value	Description	Data type	Valid in object types
	• **VTP_TRUST** — Yes • **VTP_PRIVILEGES** — Yes • **=0x08** — No • **=0x09** — Yes Files signed by Trellix: • **VTP_TRUST** — Yes • **VTP_PRIVILEGES** — Yes • **=0x08** — Yes • **=0x09** — Yes Files signed by 3rd party: • **VTP_TRUST** — No • **VTP_PRIVILEGES** — No • **=0x08** — No • **=0x09** — No		
VTP_TRUST	Checks if VTP trusts the process or file. The value is treated as Boolean. That is, a value of 1 in the match type matches only processes trusted by VTP. A value of 0 matches non-trusted processes.	UINT8	• PROCESS • SECTION • THREAD
WOW64	Matches a data value of "1" if the process/thread is a WOW64 process. This can only be true on 64-bit platforms and always matches a "0" on 32-bit platforms.	UINT8	• PROCESS • THREAD

Match type value	Description	Data type	Valid in object types
	This match can apply to both `Initiator` and `Target` objects.		

OBJECT_NAME guidelines

Use these guidelines when specifying the OBJECT_NAME match value in a *Match_type* value. You can use any combination of wildcards.

OBJECT_NAME value	Notes
Disk name	Accepted formats are: • HardDiskXX — HardDisk0 • $(SystemDrive) — The disk that contains the system volume.
Fully qualified file path	**Note:** AAC doesn't support short paths. • System — Specifies the system process name. To match based on the thread running in the system process context, the rule must set an `Initiator` command to "System". • System:Remote — Specifies the system process name for remote systems. To match file operations for a remote system, the rule must set an `Initiator` command to "System:Remote". To match based on both “System” and “System:Remote”, configure the rule to specify 2 matches or specify “System*”.
Fully qualified registry key/value path	These root keys are recognized: **Key** — **Matches** HKLM — HKLM is equivalent to

<table>
<tr><th>OBJECT_NAME value</th><th>Notes</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>HKEY_LOCAL_MACHINE.</td></tr>
<tr><td>HKCU</td><td>All user registry keys (not just the current user) and the .default user key.
HKCU is equivalent to:
HKEY_CURRENT_USER
HKEY_USERS
Note: Matching against specific user SIDs is not supported.</td></tr>
<tr><td>HKCUC</td><td>All user classes (HKCU/*_CLASSES).</td></tr>
<tr><td>HKCR</td><td>System classes and all user classes (HKCU/*_CLASSES).
HKCR is equivalent to HKEY_CLASSES_ROOT.</td></tr>
<tr><td>HKCCS</td><td>HKLM/SYSTEM/CurrentControlSet</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>OBJECT_NAME value</th><th>Notes</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>• HKLM/SYSTEM/ControlSet00X</td></tr>
<tr><td>HKLMS</td><td>• HKLM/Software on 32-bit and 64-bit systems
• HKLM/Software/Wow6432Node on 64-bit systems only</td></tr>
<tr><td>HKCUS</td><td>• HKCU/Software on 32-bit and 64-bit systems
• HKCU/Software/Wow6432Node on 64-bit systems only</td></tr>
<tr><td>HKULM</td><td>• HKLM
• HKCU</td></tr>
<tr><td>HKULMS</td><td>• HKLMS
• HKCUS</td></tr>
<tr><td>HKALL</td><td>• HKLM
• HKU</td></tr>
</table>

Note: If the rule specifies a name where the root starts or contains a wild character, the AAC code performs no name normalization and that name might never match correctly. For example, **\mcshield\start is a valid name, but H*L*\mcshield\start is not.
</td></tr>
</table>

OBJECT_NAME value	Notes
	HKEY_CURRENT_CONFIG is not supported.
Fully qualified section name	
Process name or fully qualified process path	Process name must also be specified for thread objects.
Volume name	• Must be specified in the format: `Volume{35FC9B67-54AC-49ff-AB99-33FFA2999670}` • $(SystemDrive) — Immutable and always applies to the system volume.

ACCESS_MASK flags

Use these flags with the ACCESS_MATCH *Match_type* value.

Flag	Applies to object types	Applies when
CONNECT_NAMED_PIPE	FILE (representing a named pipe)	Attempt to connect to a named pipe.
CREATE	• FILE • KEY • PROCESS • THREAD • SECTION	• File, Key, Process, or Thread is created. If the Target to be blocked is a process, specify the object type as SECTION rather than PROCESS. • File is open for execute (SECTION object). This doesn't mean that the SECTION object itself is created, rather that a SECTION object can be created. The SECTION object might not be created for execute.

Flag	Applies to object types	Applies when
DELETE	• FILE • KEY • PROCESS • THREAD	• File or Key (not registry values) is deleted or set security is called. • Process is opened with PROCESS_TERMINATE. • Thread is opened with THREAD_TERMINATE.
ENUM	• KEY • VALUE	• Key is opened with KEY_ENUMERATE_SUB_KEYS. • Values are enumerated with RegEnumValue.
EXECUTE	FILE	• File is opened with FILE_EXECUTE access. • SECTION object is created with SECTION_MAP_EXECUTE. **Tip: Best practice** Blocking SECTION objects might cause Windows to call a NtRaiseHardError(). To block loading unwanted code without this side-effect, use CREATE with SECTION. • Directory is opened with traverse access.
LOAD_IMAGE	SECTION	Notification only (cannot block the image load).
LOAD_KEY	KEY	Registry hive is loaded into a key with ZwLoadKey or RegLoadKey.
LOCK_RANGE		Attempt to lock or unlock a byte-range lock on a file.

Flag	Applies to object types	Applies when
		Use this access mask to protect a log file. You don't need to use this access mask for files that you aren't going to WRITE to at runtime, but byte-range locks don't stop reading and executing files.
OPEN_FOR_DELETE	FILE	Create/open event that requested delete access.
POST	FILE	Post-operation event. Events that carry this bit only match against rules that have this bit set. Also, if the access mask contains other bits set (not including POST), the rule evaluates to true only if at least one other bit matches the event.
QUERY	• KEY • VALUE	Attempt to query a registry key/value occurs.
READ	• FILE • KEY • VALUE	Existing file/key is being opened for read access. **Note:** This does not match with registry key/value enum/query operations. See ENUM and QUERY for matching against registry query/enum operations.
READ_DATA	FILE	An actual read file I/O occurs (ReadFile executed from user-space).

Flag	Applies to object types	Applies when
RENAME	• FILE • KEY • VALUE	Registry key or file rename operation occurs.
REPLACE_KEY	KEY	Registry key is replaced (RegReplaceKey).
RESTORE_KEY	KEY	Registry key is restored (RegRestoreKey).
SET_FILE_LENGTH	FILE	Any operation that changes the file length (ZwSetInformationFile), where class is one of: • FileEndOfFileInformation • FileAllocationInformation • FileValidDataLengthInformation This access bit helps with file-copy detection, when the destination file is extended and then written to.
SET_REPARSE	FILE	Attempt to set the reparse data on a file or directory object. Do not use this access mask with IS_DIRECTORY. Attempts to set a reparse point on an alternate data stream don't match correctly. This is because the file system always considers alternate data streams as "file" objects, even if the base file object is a directory. But, reparse data is configurable from an alternate data stream file handle on a directory, which causes STATUS_REPARSE to be returned

Flag	Applies to object types	Applies when
		for all streams of a directory or file object.
TERMINATING	• PROCESS • THREAD	Notification only (cannot block a terminate action).
WRITE	• FILE • KEY • VALUE • PROCESS	• Existing file is opened for write (FILE_GENERIC_WRITE and disposition TRUNCATE_EXISTING). File rules, using this flag, and specifying the file name as a fully qualified path including drive letter, also matches rename operations for any of the upper-level directories. For example, if the rule specifies "c:\program files\mcafee\systemcore**", this rule matches rename operations against: ▫ c:\program files\mcafee\systemcore ▫ c:\program files\mcafee ▫ c:\program files\ But the rule doesn't match: ▫ c:\program files\microsoft ▫ c:\program files\mcafee\VSE • Existing key is opened for write (KEY_WRITE). • Process is opened for write access: ▫ PROCESS_CREATE_PROCESS ▫ PROCESS_CREATE_THREAD ▫ PROCESS_DUP_HANDLE ▫ PROCESS_SET_QUOTA ▫ PROCESS_SET_INFORMATION ▫ PROCESS_SUSPEND_RESUME

Flag	Applies to object types	Applies when
		▫ PROCESS_VM_OPERATIONS ▫ PROCESS_VM_WRITE • Handle to the thread is opened with write access: ▫ THREAD_DIRECT_IMPERSONATION ▫ THREAD_IMPERSONATE ▫ THREAD_SET_CONTEXT ▫ THREAD_SET_INFORMATION ▫ THREAD_SET_LIMITED_INFORMATION ▫ THREAD_SET_THREAD_TOKEN ▫ THREAD_SUSPEND_RESUME • Registry value is created, written, or deleted. Values are considered the data of a key.
WRITE_ATTRIBUTE	FILE	File or directory's attributes are written to.
WRITE_DATA	FILE	Actual write file I/O (WriteFile executing from user-space).

Commands to query system state

iDump command

The `iDump` command dumps global variables defined in the rule to the log file if debug logging is enabled.

Syntax

```
iDump filter
```

If *filter* is not specified, this command dumps all variables.

Parameter

Parameter	Description
filter	String that represents the names of the global variables to dump. The *filter* parameter can contain wildcards.

For more Expert Rules examples, visit the Trellix Github repository.

iEnv command

The `iEnv` command returns the specified environment variable value or an empty string if the variable does not exist.

Syntax

```
iEnv name
```

Parameter

Parameter	Returns
name	Value of the specified environment variable.

Example

```
set PingExe [iEnv SystemRoot]\\system32\\ping.exe
```

For more Expert Rules examples, visit the Trellix Github repository.

iList command

The `iList` command sorts the values in the list in ascending order and removes duplicate values.

Syntax

```
iList -d list
```

Parameter

Parameter	Description
-d	Indicates that the *list* contains directory names and converts all directory characters to the proper format for the operating system. Any duplicate separators are combined into one before the comparisons are done, any trailing directory characters are removed before the list is returned. If an entry is a subdirectory of another element, only the parent directory is returned.

Example

```
set alist {{c:/tmp\\ } {c:\tmp\a} {c:\tmp/b/c} {d:\debug}}
set blist [iList -d $alist]
```

The "blist" list now contains:

```
{{c:\tmp} {d:\debug}}
```

For more Expert Rules examples, visit the Trellix Github repository.

iReg command

The `iReg` command reads information from the local registry.

Syntax

```
iReg [-32] param
```

Parameters

To read the 32-bit hive on a 64-bit operating system, specify `-32` as the first argument.

Parameter	Description
open *keyname*	Opens a registry key named *keyname* and returns "1" if successful or "0" otherwise. Closes the key when the scanning session is over.

Parameter	Description
exist *keyname*	Tests to see if a registry key named *keyname* exists and returns "1" if it exists or "0" otherwise.
value *keyname valuename*	Reads information from the registry key *keyname* with the value name of *valuename*. If the value is type: • `string` — Returns the string value. • `int` — Returns the string value. • `MULTI_SZ` — Returns a Tcl list.
keys *keyname*	Returns a list of subkeys that exist under the key specified by *keyname*.
v_exists *keyname valuename*	Tests to see if the *valuename* item exists under the key specified by *keyname* and returns "1" if exists or "0" otherwise.

You can use the following shortcuts for the registry *keyname*.

Keyname	Shortcut
HKEY_LOCAL_MACHINE	HKLM
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_CONFIG	HKCC
HKEY_CURRENT_USER	HKCU
HKEY_USERS	HKUS

For example, to specify the software hive on the local system, use HKLM\\Software.

For more Expert Rules examples, visit the Trellix Github repository.

iSystem command

The `iSystem` command returns information about the client system where the rule is executed.

Syntax

```
iSystem param
```

Parameters

Parameter	Returns
version	Version of the operating system in the format *major.minor.build*.
major	Major version of the operating system.
minor	Minor version of the operating system.
build	Build number of the operating system.
csd	CSD value. Usually, this is the Service Pack in the form of a string, such as "Service Pack 1".
platform	String with the platform name, for example, "Windows 7".
type	System type: • Workstation • Server • Unknown
cpu_arch	CPU architecture: • 320 for 32-bit CPU • 640 for 64-bit AMD type CPU • 641 for 4-bit Itanium type CPU
os_arch	Operating system architecture: • 320 for 32-bit operating system

Parameter	Returns
	• 640 for 64-bit operating system
install_dir	Location of the Windows installation directory.
sys32_dir	Location of the System32 folder.
users_folders *folder_types*	List of folder locations for all users created on the system. You can specify the types of folders to return. The valid folder types are listed in `HKEY_USERS\<user sid>\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` In addition, you can specify these special folder types: • Temp — All temp folders on the system • Profile — All users' profile root folder • Downloads — All users' download locations • -no_defaults —All folders that are not changed from their default values.

For more Expert Rules examples, visit the Trellix Github repository.

iTerminate command

The `iTerminate` command stops building the rules and adds the specified message text to the error log.

Syntax

```
iTerminate "msg"
```

Parameter

Parameter	Description
msg	The message to add to the error log.

iUser command

The `iUser` command returns information about users on a system.

Syntax

```
iUser param
```

Parameters

Parameter	Returns
username	"1" if the user exists on the system, otherwise "0".
list	List of all users on the system.
groups *username*	List of the groups a user belongs to.

For more Expert Rules examples, visit the Trellix Github repository.

iUtil command

The `iUtil` command converts the specified string into arguments and pass it to the function.

Syntax

```
iUtil cvt2args name
```

Parameter

Parameter	Description
cvt2args	Converts the specified strings into arguments.

Example

```
set test_var10 [iUtil cvt2args $test_var10]
```

For more Expert Rules examples, visit the Trellix Github repository.

Learn Expert Rules for Buffer overflow, Illegal API use and Services

Legacy McAfee Host IPS rule structure

Rules contain both required and optional sections, one section per line. Each section defines a rule category and its value. One section always identifies the class of the rule, which defines the rule's overall behavior. Optional sections vary according to the class of the rule.

Here is the basic structure of a McAfee Host IPS rule:

```
Rule {
        SectionA value
        SectionB value
        SectionC value
        ...
}
```

Because the structure and class types for legacy Expert Rules are identical to those in McAfee Host IPS, you can copy existing McAfee Host IPS rules into Trellix ENS Expert Rules.

Note

Trellix ENS doesn't support signatures with multiple rules.

Legacy Syntax

Wildcards

You can use wildcards for section values in Expert Rules.

Wildcard character	Represents
? (question mark)	A single character.
***** (one asterisk)	Multiple characters, including **/** and ****. **Note:** For paths and addresses, use ****** (2 asterisks) to include **/** and ****. Use ***** (one asterisk) to exclude **/** and ****.
& (ampersand)	Multiple characters except **/** and ****.

Wildcard character	Represents
	Use **&** to match the root-level contents of a folder, but no subfolders. For example: `Include "C:\test\\&.txt"`
! (exclamation point)	Wildcard escape. For example: `Include "C:\test\\yahoo!.txt"`

Environment variables

Use environment variables to specify file and directory path names.

The `iEnv` command takes one parameter (the variable name) in square brackets **[ ]**.

Environment variable	Represents
iEnv SystemRoot	C:\winnt\, where C is the drive that contains the Windows System folder. For example: `Include [iEnv SystemRoot]\\system32\ \abc.txt`
iEnv SystemDrive	C:\, where C is the drive that contains the Windows System folder. For example: `Include [iEnv SystemDrive]\\system32\ \abc.txt`

Using the Include and Exclude keywords

When you select a section value as `Include`, the section works on the value indicated. When you select a section value as `Exclude`, the section works on all values except the one indicated.

The keywords `Include` and `Exclude` are supported for all sections except `directives` and `attributes`.

Enclose the `Include` and `Exclude` keywords in brackets { ... }.

Note

For a standard subrule, use a single backslash in file paths. The standard subrule translates the single slashes to required double slashes. For a subrule in an Expert Rule, use double backslashes in file paths. The expert subrule performs no translation.

For example, to monitor all text files in C:\test\:

```
files { Include C:\\test\\*.txt }
```

To monitor all files except the text files in C:\test\:

```
files { Exclude C:\\test\\*.txt }
```

Combine keywords to exclude values from a set of included values.

For example, to monitor all text files in folder C:\test\ except file abc.txt:

```
files { Include C:\\test\\*.txt }
files { Exclude C:\\test\\abc.txt }
```

Each time you add the same section with the same keyword, you add an operation.

For example, to monitor any text file in folder C:\test\ whose name starts with the string “abc”:

```
files { Include C:\\test\\*.txt }
files { Include C:\\test\\abc* }
```

`Exclude` takes precedence over `Include`. For example:

- If a single subrule includes a particular user marketing\jjohns and excludes the same user marketing\jjohns, the signature doesn't trigger even when the user marketing\jjohns performs an action that triggers the signature.
- If a subrule includes all users but excludes the particular user marketing\jjohns, the signature triggers if the user isn't marketing\jjohns.
- If a subrule includes user marketing* but excludes marketing\jjohns, the signature triggers only when the user is marketing\anyone, unless the user is marketing\jjohns, in which case it doesn't trigger.

Sections that are common to all class types

Use these sections when defining rules of all class types.

All section names are case sensitive. Section values are not case sensitive.

For sections that apply to a specific class type only, see the section lists for that class type.

Section	Value	Description	Required?
user_name	{Include/Exclude user's name or system account}	Specifies the users that rule applies to. Specify particular users or all users. • **Local users**: *machine name/local user name* • **Domain users**: *domain name/domain user name* • **Local system**: Local/System Some remotely initiated actions don't report the ID of the remote user, but use the local service and its user context instead. You must plan accordingly when developing rules. When a process occurs in the context of a Null Session, the user and domain are "Anonymous". If a rule applies to all users, use the ***** wildcard.	Yes
Executable	{Include/Exclude file path name, fingerprint, signer, or description}	Specifies the executables that the rule applies to. Specify each executable inside brackets using: • -path — File path name • -hash — MD5 hash	Yes

Section	Value	Description	Required?
		• -sdn — Signer • -desc — Description Each section can have multiple brackets and, inside the brackets, one or more options. The `-path`, `-sdn`, and `-desc` values are strings and must be Tcl-escaped if they contain spaces or other Tcl-reserved characters. The `-hash` value is a 32-character hexbin string. For example: `Executable { Include -path "C:\\Program Files (x86)\ \McAfee Endpoint Security\\ Threat Prevention\ \mfetp.exe" -sdn "CN=\"McAfee, Inc.\", OU=Engineering, O=\"McAfee, Inc.\", L=Santa Clara, ST=California, C=US" -desc "on-access scanner service" }` If a rule applies to all executables, use the ***** wildcard.	
directives	operation type	Specifies the class-dependent operation types. For the operation type, see the directives in each class type description.	Yes

Section	Value	Description	Required?
dependencies	{Include/Exclude “ID of a rule”}	Defines dependencies between rules and prevents triggering dependent rules. Add the dependencies section to prevent a more general rule from being triggering with a more specific rule. For example, use ID 428 for Buffer Overflow signatures.	No
attributes	-no_log	Sends no events from the signature to the Trellix ePO - On-prem server. Sends no events from the signature.	No
	-not_auditable	Generates no exceptions for the signature when Adaptive mode is enabled.	
	-no_trusted_apps	Specifies that the trusted application list doesn't apply to this signature.	
	-inactive	Disables the signature.	

Class types

Buffer Overflow class type

The `Buffer Overflow` class type prevents buffer overflow exploits for applications in the application protection list.

Section	Value	Notes
user_name		
Executable		
dependencies	428	Specifies Signature 428, Generic Buffer Overflow, a generic buffer overflow rule. (Optional) We recommend including section "dependencies 428" to avoid triggering the generic signature.
caller module	Path to a module (for example, a DLL) loaded by an executable that calls and causes a buffer overflow	
directives	bo:stack	Examines the memory location that is executing and detects if it is running from writable memory that is part of the current thread's stack.
	bo:heap	Examines the memory location that is executing and detects if it is running from writable memory that is part of a heap.
	bo:writeable_memory	Examines the memory location that is executing and detects if it is running from writable memory that is not part of the current thread's stack or a heap.
	bo:invalid_call	Checks that an API is called from a proper call instruction.

Section	Value	Notes
	bo:target_bytes	A hexadecimal string representing 32 bytes of instructions that can be used to create a targeted exception for a false positive without disabling buffer overflow for the entire process.
	bo:call_not_found	Checks that the code sequence before the return address isn't a call.
	bo:call_return_unreadable	Checks that the return address isn't readable memory.
	bo:call_different_target_address	Checks that the call target doesn't match the hooked target.
	bo:call_return_to_api	Checks that the return address is an API entry point.

Illegal API Use class type

The `Illegal API Use` class type prevents illegal use of the Exploit Prevention API.

Section	Value	Notes
user_name		
Executable		
vulnerability_name	Name of the vulnerability	
detailed_event_info	One or more CLSIDs.	This value is a 128-bit number that represents a unique ID for a software component, such as:

Section	Value	Notes
		`"{FAC7A6FB-0127-4F06-9892-8D2FC56E3F76}"`
directives	illegal_api_use:bad_parameter	
	illegal_api_use:invalid_call	

Use this class to create a custom killbit signature. The killbit is a security feature in web browsers and other applications that use ActiveX. A killbit specifies the object class identifier (CLSID) for ActiveX software controls that are identified as security vulnerability threats. Applications that use ActiveX don't load specified ActiveX software with a corresponding killbit in place.

The primary purpose of a killbit is to close security holes. Killbit updates are typically deployed to Microsoft Windows operating systems using Windows security updates.

Here is an example of a killbit signature:

```
Rule {
tag "Sample4"
Class Illegal_API_Use
Id 4001
level 4
Executable { Include "*"}
user_name { Include "*"}
vulnerability_name {Include "Vulnerable ActiveX Control Loading ?"}
detailed_event_info { Include
"0002E533-0000-0000-C000-000000000046"\"0002E511-0000-0000-C000-000000000046"}
directives files:illegal_api_use:bad_parameter illegal_api_use:invalid_call
attributes -not_auditable
}
```

Services class type

The `Services` class type protects Windows Services operations.

Section	Values	Notes
user_name		
Executable		
services	Name of the service to protect.	(Required) The name of the service is in the corresponding registry key under

Section	Values	Notes
		HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.
display_names	Display name of the service.	Required. This name appears in the Services manager and in the registry value HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<name-of-service>\
directives	services:delete	Deletes a service.
	services:create	Creates a service.
	services:start	Starts a service.
	services:stop	Stops a service.
	services:pause	Pauses a service.
	services:continue	Continues a service after a pause.
	services:startup	Changes the startup mode of a service.
	services:profile_enable	Enables a hardware profile.
	services:profile_disable	Disables a hardware profile.
	services:logon	Changes the logon information of a service.

Troubleshooting Expert rules

This example log shows some of the possible cause of errors while writing Expert Rules. Trellix Endpoint Security (ENS) provides information in the EndpointSecurityPlatform_Errors.log file about rules that didn't successfully compile and so were not enforced.

Because all Expert Rules are compiled into a single group, when an Expert Rule generates an error, no Expert Rules are enforced.

Tip

Best practice: To isolate any potential issues, every time you create a rule, verify that it was successfully enforced on the client system.

The EndpointSecurityPlatform_Errors.log file includes detailed information, such as the content of the rule and the parameter that caused the error. For example, this log error shows the Expert Rules error, which is an extra `Include` command:

```
08/11/2017 11:57:34.403 AM   mfeesp(4016.4412) <SYSTEM> ApBl.AP.Error: Syntax error: Include: Invalid
number of arguments
    while executing
"Include Include OBJECT_NAME  { -v "*PowerShell*" }"
        Include Include OBJECT_NAME  { -v "*PowerShell*" }
        Include PROCESS_CMD_LINE { -v "*-extoff* script.scp" }
        Include ..."
    invoked from within
"Process {
        Include OBJECT_NAME      { -v "*PowerShell*" }
        Include PROCESS_CMD_LINE { -v "*-extoff*" }
        Include PROCE ..."
    invoked from within
"Rule -id "4100" {
    Reaction BLOCK
    Group "ExPExpertRules"
    Description "testrule"
    Process {
         Include AggregateMatch {
         Include OBJECT_NAME      {  ..."
    invoked from within
"Policy {
Rule -id "4100" {
    Reaction BLOCK
    Group "ExPExpertRules"
    Description "testrule"
    Process {
         Include AggregateMatch {
         Include OBJECT_NA ..."LastErr 0x000010dd The operation identifier is not valid.
08/11/2017 11:57:34.403 AM   mfeesp(4016.4412) <SYSTEM> ApBl.AP.Error: ERR: BLError 0xc0380102, Could not
process content file
```

COPYRIGHT

Trellix