

Overview

HPE IMC Endpoint Admission Defense Software

Models

HPE IMC Endpoint Admission Defense Software Module with 50-user E-LTU

JG754AAE

Key features

- Enforces posture compliance
- Fully integrates all functions
- Reduces infection risk of network terminal
- Automatically blocks suspicious traffic
- Protects sensitive data

Product overview

HPE Intelligent Management Center (IMC) software is a modular, comprehensive resource management platform. With its extensive device support, IMC software provides true end-to-end management for the entire network, as well as the open operation cycle.

HPE IMC Endpoint Admission Defense (EAD) Software reduces network exposure by integrating security policy management and endpoint posture assessment to identify and isolate risks at the network edge. The security policy component allows administrators to control endpoint admission based on an endpoint's identity and posture. If an endpoint is not compliant with software, network assets can be protected by blocking or isolating an endpoint's access.

EAD reduces the risk of malicious code infections or other security breaches by detecting endpoint patches, viruses, Address Resolution Protocol attacks, abnormal traffic, the installation and running of sensitive software, as well as the status of system services. EAD provides continual monitoring of endpoints. The software now supports a concurrent licensing model.

Features and benefits

Management

- **Endpoint access and control**
 - **The System**
supplies control and management of endpoint equipment; this module requires that a fully licensed version of the IMC User Access Management (UAM) Software module be installed.
 - **EAD integrates**
With MobileIron and Citrix® to certify that the device is compliant with MDM policies before receiving access to the network
- **Enhancement of hierarchy management**
sets security policies for the entire network and distribute the policies to lower-level nodes; the lower-level nodes can send security and system status to the parent node, enabling the parent node to monitor lower-level nodes in real time; reports are also provided to administrators
- **Anti-X software policy management**
enables administrators to set an Anti-X checking rule for each security policy made in IMC, rather than having a single rule for all security policies
- **IPv6 communication with endpoints**
is supported by EAD policy server and Desktop Asset Management (DAM) server.
- **Change of authorization support**

Overview

contains change-of-authorization attributes for a session; this feature offers a quarantine mode for devices, including other vendor devices

- **eAPI for DAM**

is found inside IMC Extended API and assists in database activity monitoring.

Security

- **Complete security evaluation**

reduces network vulnerabilities by determining endpoint compliance to defined policies; security checks can include antivirus, anti-spyware, anti-phishing, firewall, required patches, and hard disk encryption software; EAD supports auto-remediation options with integration to patch management software like Microsoft® Systems Management Server (SMS)/Windows® Server Update Services (WSUS), and with antivirus software from Symantec, McAfee, and Trend Micro

- **Endpoint identity**

integrates with the UAM module to leverage existing user directories and groups to aid in the access and posture of policy creation; in addition to user name credentials, smart card and certificate authentication are supported

- **Integration of user management and device management**

- **Report correlation**

uses the IMC module design, data across modules can be shared to create richer, more informative reports (e.g., network devices can display end-user statistics)

- **Policy correlation**

lets administrators can set policy based on shared data (e.g., policies or actions can be location-specific)

- **Module correlation**

displays user-specific traffic analysis

- **Integration of user management and topology management**

improves upon user management operations, which are provided in the menus of the access devices or access terminals (e.g., view user information, disconnect online users, and perform security checks); this makes user management more flexible

- **Desktop asset management**

- **Supported asset management features**

allows for hardware specifications to be auto-discovered (e.g., CPU, memory), and software inventory can be completed to generate reports or run queries

- **Policy setting**

aids in preventing data theft by controlling the computer peripherals, like USB storage; DAM also includes password and share controls and power management across endpoints

- **MDM Collaboration**

supports API integration with MobileIron and Citrix to certify that the device is compliance with MDM Policies before getting access to the network

Warranty and support

- **Electronic and telephone support**

limited electronic and business-hours telephone support is available from Hewlett Packard Enterprise; to reach our support centers, refer to <http://www.hpe.com/networking/contact-support>; for details on the duration of support provided with your product purchase, refer to <http://www.hpe.com/networking/warrantysummary>.

- **Software releases**

to find software for your product, refer to <http://www.hpe.com/networking/support>; for details on the software releases available with your product purchase, refer to <http://www.hpe.com/networking/warrantysummary>

Technical Specifications

HPE IMC Endpoint Admission Defense Software Module with 50-user E-LTU (JG754AAE)

Platform required

Server:
HPE Intelligent Management Center Enterprise Software
HPE Intelligent Management Center Standard Software

Notes

See the HPE IMC Standard or Enterprise Platform data sheet for the required software environment.
EAD and UAM are installed with the platform on the same server.
One server's managed user size can range from 1 to 50,000 users.
If there are more than 10,000 users, an array controller or RAID card is needed: Dual-Channel Ultra 320 SCSI card array controller or higher configuration, with a cache of 192 MB;
Supporting RAID 0, 1, 1+0, and 5.
Database can be Oracle 11g Enterprise Edition or Microsoft SQL Server 2005/2008.

Services

Refer to the HPE website at <http://www.hpe.com/networking/services> for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HPE sales office.

Accessories

License

HPE IMC Endpoint Admission Defense Software Module Additional 50-user E-LTU	JG755AAE
---	----------

Summary of Changes

Date	Version History	Action	Description of Change:
17-June-2016	From Version 9 to 10	Changed	Product descriptions updated.
01-Dec-2015	From Version 8 to 9	Changed	QuickSpecs name changed to HPE IMC Endpoint Admission Defense Software Product overview, Features and benefits and Technical Specifications
29-Sep-2014	From Version 7 to 8	Changed	Updated Product Overview, Features and benefits and Technical Specifications
30-Sep-2013	From Version 6 to 7	Changed	The Product overview, Key Features, Features and Benefits, model specifications and Options were updated.
30-Aug-2013	From Version 5 to 6	Changed	The title was changed.
13-Jun-2013	From Version 4 to 5	Removed	License models were removed.
25-Jun-2012	From Version 3 to 4	Changed	The QS was completely revised, including a name change.
13-Feb-2012	From Version 2 to 3	Changed	The Features and Benefits, model names and Options were updated.
06-Apr-2011	From Version 1 to 2	Changed	The QuickSpecs was completely revised. Please note the title has changed as well.



© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

To learn more, visit: <http://www.hpe.com/networking>

McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries. Microsoft and Windows Server are U.S. registered trademarks of the Microsoft group of companies. Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Citrix is a registered trademark of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

c04111575 - 13836 - Worldwide - V10 - 17-June-2016

