Data sheet

HP IMC Endpoint Admission Defense Software

Key features

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

Product overview

HP 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.

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 control and management**
  Endpoint Admission Defense (EAD) Software 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; the number of licensed nodes for EAD software must match the number of UAM licensed nodes
- **Enhancement of hierarchy management**
  the root node in the hierarchy architecture can set 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**
  the Anti-X checking feature 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 support**
  EAD policy server and Desktop Asset Management (DAM) server support IPv6 communication with endpoints
- **COA support**
  EAD supports change-of-authorization attributes for a session; this feature offers a quarantine mode for devices, including other vendor devices
- **eAPI for DAM**
  the IMC Extended API suite includes APIs for DAM

Security

- **NEW Complete security evaluation**
  EAD 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**
  EAD software 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**
    using 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**
    in addition to reports, administrators can set policy based on shared data (e.g., policies or actions can be location-specific)
  - **Module correlation**
    network traffic data can be correlated to display user-specific traffic analysis
- **Integration of user management and topology management**
  on the topology map, user management operations 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 (DAM)**
  EAD software supports desktop asset management features to provide a complete inventory of endpoints; hardware specifications can be auto-discovered (e.g., CPU, memory), and software inventory can be completed to generate reports or run queries; in addition, administrators can set policies to aid in preventing data theft by controlling the computer peripherals, like USB storage; DAM also includes password and share controls and power management across endpoints

Warranty and support

- **Electronic and telephone support**
  limited electronic and business-hours telephone support is available from HP for the entire warranty period; to reach our support centers, refer to **www.hp.com/networking/contact-support**; for details on the duration of support provided with your product purchase, refer to **www.hp.com/networking/warrantysummary**
- **Software releases**
  to find software for your product, refer to **www.hp.com/networking/support**; for details on the software releases available with your product purchase, refer to **www.hp.com/networking/warrantysummary**

HP IMC Endpoint Admission Defense Software

Specifications

	HP IMC Endpoint Admission Defense Software Module 50-user E-LTU (JG754AAE)
Minimum system hardware	Different hardware will be required depending on the number of users. Intel® Pentium® 4 3.0 GHz processor 4 GB RAM memory 50 GB storage 10/100 MB NIC
Recommended system hardware	3.0 GHz Intel® Xeon® or Intel® Core™2 Duo processor or equivalent processor 4 GB RAM memory 100 GB storage 1000 MB NIC
Recommended software	Windows® Server 2003 with Service Pack 2 Windows® Server 2003 X64 with Service Pack 2 and KB942288 Windows® Server 2003 R2 with Service Pack 2 Windows® Server 2003 R2 X64 with Service Pack 2 with KB942288 Windows® Server 2008 with Service Pack 2 Windows® Server 2008 X64 with Service Pack 2 Windows® Server 2008 R2 with Service Pack 1 Windows® Server 2008 R2 X64 with Service Pack 1 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 5 X64 Red Hat Enterprise Linux 5.5 Red Hat Enterprise Linux 5.5 X64 Red Hat Enterprise Linux 6.1 X64
Browsers	Firefox 3.6 or later is recommended Internet Explorer 8.0 or later is recommended
Additional requirements	An array controller or RAID card is needed: Dual-Channel Ultra 320 SCSI card array controller or higher configuration, with a cache of 128 MB or more; supporting RAID 0, 1, 1+0, and 5
Notes	EAD and UAM are installed with 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	3-Year, 9x5 SW phone support, software updates (UV746E) 3-year, 24x7 SW phone support, software updates (UV747E) Refer to the HP website at **www.hp.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 HP sales office.

HP IMC Endpoint Admission Defense Software accessories

License

HP IMC Endpoint Admission Defense Additional 50-user E-LTU (JG755AAE)

To learn more, visit hp.com/networking

4AA3-0700ENW, Created August 2010; Updated September 2013, Rev. 5