

Overview

Models

HP IMC Smart Connect Virtual Appliance Edition E-LTU

JG766AAE

Key features

- Identity-based access, advanced device profiling, and real-time traffic quarantining
 - Converged network support with universal policies for all wired and wireless devices
 - Seamless policy enforcement based on user and/or device
 - Unified monitoring of BYOD traffic and user behavior
 - Simplified deployment and configuration
-

Product overview

Intelligent Management Center (IMC) Smart Connect Virtual Appliance Software offers a comprehensive bring your own device (BYOD) solution with easy onboarding, provisioning, and monitoring of users and clients. With this software, HP moves beyond the basic BYOD requirements of identity-based access by offering a comprehensive solution that includes single policy enforcement and converged network management across wired and wireless environments. Unified BYOD monitoring further enables administrators to plan for capacity and comply with regulatory requirements.

The HP IMC Smart Connect solution is based on HP Intelligent Management Center Standard Edition Software and includes HP IMC User Access Manager Software for user access, guest access management, device fingerprinting, and self-registration. IMC Smart Connect Virtual Appliance software is also available with wireless management for converged wired and wireless management.

IMC Smart Connect Virtual Appliance software is offered as a virtualization appliance to allow easy installation and configuration. It includes an embedded SQL database and Red Hat Linux operating system, which are delivered in an OVA file. IMC Smart Connect Virtual Appliance software comes with a license for 100 device nodes and 200 users.

Features and benefits

Management

- **Virtualization appliance**
allows easy installation and configuration; includes an embedded SQL database and Red Hat Linux operating system; comes with a license for 100 device nodes and 200 users; is delivered in an OVA file; shares server hardware with other applications, which reduces the complexity of installations and simplifies deployment as well as operational and infrastructure management
- **HP Intelligent Management Center (IMC)**
cohesively integrates fault management, element configuration, and network monitoring from a central vantage point; built-in support for third-party devices enables network administrators to centrally manage all network elements with a variety of automated tasks, including discovery, categorization, baseline configurations, and software images; the software also provides configuration comparison tools, version tracking, change alerts, and more
- **Modular architecture**
allows the addition of new modules to enrich network management capabilities; modules for user access management, VPN management, and traffic analysis can be quickly added and provide instant benefits; the architecture allows modules to share information and provide collaborative policy creation and reports
- **Virtualization management**
IMC software is one of the first management tools to integrate the management and monitoring of both virtual and physical networks; it provides insight into and management of virtual networks, and reduces migration complexity by aligning and

Overview

automating network policies with virtual images; it also supports VMware, Microsoft® Hyper-V, and KVM; IMC Virtual Network Management Software also supports automatic tracking of the network access ports of virtual machines

- **Highly flexible and scalable deployment models**

HP IMC Standard Software delivers an extensive set of capabilities for managing large heterogeneous networks and provides scalability and high availability through a flexible distributed deployment model; with its modular design, IMC software can be deployed across multiple servers to provide increased scalability and resilience

- **Rich resource management**

IMC software provides powerful network discovery and topology, including a detailed inventory of the network and highly accurate depictions of how it is configured; supported views include Layer 2 and 3, as well as VLAN topology and the ability to create custom views like a dashboard homepage; customization enables administrators to organize and control the network infrastructure based on their preferred organizational model

- **Flexible, centralized reporting**

centralized report management simplifies an organization's report administration; the software's flexible historical reports provide the information needed for network trend analysis and capacity planning, and offer predefined reports or customization options to define parameters; reports can be viewed in a number of formats, including .pdf and .xls, and can be sent automatically via email, or be set to run on a particular schedule

- **Access control list management**

IMC software simplifies the definition, deployment, and control of ACLs with effective policy-based control of network security and quality of service (QoS) across an organization's network infrastructure; ACL rule optimization helps ensure efficient use of ACL resources on devices

- **Identification and access management**

with the addition of the optional User Access Manager (UAM) module, the system implements unified and centralized access management, supporting access through authentications, including LAN, WAN, WLAN, and VPN; it supports strong authentication using smart card, certificate, and other methods, and supports various methods for endpoint access control and identity-based network services that efficiently integrate the management of user resources and services

- **Network Traffic Analyzer**

using the optional HP Network Traffic Analyzer (NTA) Software Module, the system can also collect flow information from sFlow-, nFlow-, and NetStream-capable devices; through traffic analysis, NTA software can help identify network bottlenecks, recognize anomalous traffic, and pinpoint varying levels of bandwidth traffic for different services and applications; the additional User Behavior Analysis (UBA) Module makes traffic flow correlations available

- **Compliance Center**

associates compliance policies with devices that need to be checked; the compliance check function can promptly fix configuration and security problems in the network; if incorrect configurations are found, the data for the specific device, along with the configuration error, is included in the Compliance Center report

- **HP Virtual Connect support**

IMC software supports add/remove connections for HP Virtual Connect Manager and displays the connect information from the device detail page IMC mobile application IMC software provides a new mobile application for the iPhone and Android operating systems; this provides administrators with the flexibility to monitor the network while away from their offices

- **Telnet/SSH proxy**

with the Telnet/SSH proxy, an administrator can use a browser to remotely access and manage devices through Telnet/SSH without installing a Telnet/SSH tool on the PC client used to access the device; this promotes secure and controlled access to devices while providing an audit of changes made on any device

- **Unified Task Management and IMC Wizard Center**

the IMC Wizard Center services many of the configuration wizards found within IMC software, such as quick start and the third-party device configuration wizard; new to this release is Unified Task Management, which hosts all tasks within IMC software

- **Traffic topology**

is based on the network's physical topology and enables users to view the traffic conditions of various links

- **Customized functions and third-party device support**

IMC Standard software extends device management and configuration functions; users can either extend an existing function to

Overview

support third-party devices by compiling interactive scripts and XML files, or customize a function by compiling interactive scripts, XML files, and UI configuration files

- **Performance views**

with TopN, trend analysis, summary data, and at a glance views, IMC software provides new ways to view performance data; the GUI is flexible and allows for instant viewing, switching between multiple views, and quick access to the various performance summary views

- **Security Control Center (SCC)**

can be used to define policies and enforce device settings consistently on selected devices; allows you to use policies to manage VLANs and VLAN port settings, as well as automatically apply a configuration template on newly discovered devices; you can also configure policies to send alarms when device configurations become noncompliant

- **Network data collection**

generates, packages, and sends archived information about your network, device, or IMC software to the appropriate HP Networking support or sales organizations in one simple step; this feature gathers the data you selected and then generates reports and data files containing the relevant information; it also delivers the reports to your selected destination, either by email, FTP, SFTP, or to a file location

- **Service Monitor**

can be used to monitor the availability and responsiveness of common network services via probes that you configure; the probes reside on local and remote IMC software agents and test services from servers and devices that you select when configuring the probes

- **Centralized access user management**

provides centralized policy creation to set the appropriate access rights for each type of user and device across the network; access user-related management functions are integrated into a user-friendly interface for easy operation; user management includes authentication binding policy, security policy, and access control policy; additionally, policies can be set for concurrent sessions and proxy servers

- **Centralized resource management of devices and users**

provides centralized maintenance of basic user information, such as user name, identity number, contact address, telephone number, email, and user group; this supplemental function allows user information to be customized as needed, such as student ID and grade for campus networks, or department and title for enterprise networks

- **Endpoint identity**

provides identification of all endpoints across the network with centralized access policies; the module leverages existing user directories and groups, including support for Active Directory, LDAP, and RADIUS; in addition to user name credentials, smart card and certificate authentication are also supported; an administrator can set devices/users into roles for specifying access levels; in addition, UAM administrators can be assigned to set policies only for specific roles

- **Integration of device and user management**

administrators can view users by different categories, such as location (access device), improving troubleshooting and reporting, as well as select a device and perform access operations like dropping a user; any online user can view the details (e.g., alarms, performance) of the access device, reducing help desk calls; integrating network device and user data into a common interface reduces deployment and aids both device and user management

- **Multiple access authentication modes**

UAM software supports authentication modes like IEEE 802.1X, VPN, and portal, and wireless access identity modes like PAP, CHAP, EAP-MD5, EAP-TLS, and PEAP to fit into applications with different security requirements; access users can be bound with hardware information, such as device IP address, access port, VLAN, user IP address, and user MAC address; this helps ensure secure authentication and prevents account spoofing and illegal access

- **Various rights control measures for stricter access control**

policies can be time or location specific, as well as include bandwidth limitations or a set number of concurrent user sessions; the system can be used to prevent IP spoofing and address conflicts; to prevent the spread of corporate information without permission, administrators can disable the use of multiple NICs or dial-up networks, and monitor or block access to USB or CD drives

- **Intensive user monitor**

the powerful blacklist management function helps administrators blacklist users who have made malicious login attempts, as

Overview

well as track the MAC/IP addresses of such users; administrators can monitor online users in real time and prohibit unauthorized users from having access; authentication failures are logged for analysis; in addition, administrators can send messages to online users to provide notifications of such things as pending disconnections for system updates

- **Flexible adjustment of service and environmental parameters**

the system parameter, the policy service parameter, the running parameter, the certificate authentication parameters, the user prompt, the client autorun task, and the password strategy can all be configured

- **Integrated access device management**

the access device configuration can interact with the IMC ACL manager for fast deployment of user access services; the access devices come with links to their details, including the basic information, alarms, and performance; administrators can view such information by simple clicks; in a topology, administrators can clearly see the included access devices, view their information, or click to set an access device to non-access

- **Selective deployment**

UAM software has multiple features to ease deployment and provide high scalability, including the ability to preconfigure and deploy IEEE 802.1X supplicant settings and leverage the IMC platform to configure access devices; IMC software can aid in phasing implementations by location, users, and enforcement levels, including different modes such as monitor, alert, and isolate, to allow an organization to enable access control features when appropriate

- **Enhanced user account and device administrator management**

multilanguage user accounts are now supported; Active Directory (AD) support includes on-demand synchronization of user accounts based on AD groups and user authentication against AD; UAM software provides a configuration wizard for portal authentication and PEAP authentication against AD; charts for monitoring UAM status can now be customized

- **IPv6 support for portal authentication**

UAM and EAD modules now support the IPv6 protocol stack

- **Troubleshooting tools for user authentication**

makes troubleshooting user authentication issues in the UAM module easier; it logs details of the user authentication process and displays relevant information on the Web page; with this tool, administrators can trace detailed information of users who try to access the network

- **Simple Network Access Control (SNAC) solution**

provides easy-to-use MAC-based authentication with self-registration, which requires reduced administrative overhead; users can register the MAC addresses of their devices to UAM the first instance they connect to the network; thereafter, MAC authentication will be automatically performed by the access devices

- **eAPI for UAM**

restful API for UAM module has been provided

- **Enhancement of LDAP authentication**

enables the LDAP user to log into the self-service page and preregister an access user account in UAM; the UAM user group can also be synchronized with the LDAP server and be based on the OU in the LDAP server; the service for an LDAP user can be based on the priority of OU that the administrator defines

- **SMS support for sending guest user credentials**

enables SMS to send the credential to a user who has created a guest user account

- **Enhancements of inode client**

provides support for IPv6 inode; inode client supports IEEE 802.1x authentication in a wireless setting

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

Technical Specifications

HP IMC Smart Connect Edition Virtual Appliance Software E-LTU (JG766AAE)

Minimum system hardware

Server:

Intel® Xeon® E5-2609, quad-core

12 GB RAM memory

1200 GB storage

1000 Mbps NIC

Minimum disk space of 1200 GB is to be distributed over four drives with a minimum of 300 GB each.

Services

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.

Accessories

HP IMC Smart Connect Virtual Appliance Software accessories

License	HP IMC User Access Manager Software Module Additional 50-user E-LTU	JG753AAE
	HP IMC Standard and Enterprise Additional 50-node E-LTU	JG749AAE

To learn more, visit: www.hp.com/networking

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel and Xeon are trademarks of Intel Corporation in the U.S. and other countries. Microsoft is a U.S. registered trademark of Microsoft Corporation.