Overview

Models

HP IMC User Access Manager Software Module with 50-user E-LTU	JG752AAE

Key features

- One central database of users and available services
- Advanced reporting capabilities
- Directory of network-attached devices and endpoints
- Support for IEEE 802.1X, EAP, PAP, CHAP, MS-CHAP, and MS-CHAPv2
- Access to LDAP-compliant directory services

Product overview

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 entire operation cycle.

HP IMC User Authentication Manager (UAM) software is an IMC module that supports user identity authentication based on the access policies associated with infrastructure resources, such as routers, switches, and servers. UAM software extends management to wired, wireless, and remote network users, enabling the integration, correlation, and collaboration of network device management and user management on a single unified platform.

The IMC UAM software solution provides a full-featured RADIUS server that supports centralized authentication, authorization, and accounting management of endpoints that connect and use network services. Policy management provides access control with tiered privilege levels. As a result, IMC UAM software helps reduce vulnerabilities and security breaches. IMC User Access Manager now supports a concurrent licensing model.

Features and Benefits

Management

- **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
- **NEW Centralized resource management of devices and users**
  provides centralized maintenance of basic user information, such as name, contact information, and user group; this supplemental information function allows user data to be customized as needed, such as student ID and grade for campus networks, or department and title for enterprise networks; it also supports multiple instances of HP Intelligent Management Center User Access Management (UAM) software under a single IMC platform instance
- **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
- **Device fingerprinting**
  network-agnostic device fingerprinting capabilities based on HTTP+MAC+DHCP device recognition

Overview

- **Auto-MAC registration**
  Simple Network Access Control (SNAC) enhanced with auto-MAC registration capabilities
- **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 in both device and user management
- **Multiple access authentication modes**
  UAM software supports authentication modes like 802.1X, VPN, 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 the 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 and 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 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**
  the Simple Network Access Control (SNAC) solution provides easy-to-use MAC-based authentication with self-registration, requiring minimal administrative overhead; users can register the MAC address of their devices to the UAM software the first instance they connect to the network; thereafter, MAC authentication will be automatically performed by the access devices
- **eAPI for UAM**

Overview

a "restful" API for the UAM software module has been provided

- **Enhancement of LDAP authentication**
  an LDAP user can pre-register an access user account in the UAM software; the user group could also be synchronized with the LDAP server and be based on the organizational unit (OU) in the LDAP server; the service applied to an LDAP user could then be based on the priority of OU defined by the administrator
- **SMS support for sending guest user credentials**
  when a guest user account is created, the credentials may be sent to the user by an SMS text message
- **Enhanced IMC iNode client**
  the IMC iNode client supports IPv6, and IEEE 802.1X authentication in wireless scenarios

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 User Access Manager Software Module with 50-user E-LTU (JG752AAE)

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 user 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 (UV740E) 3-year, 24x7 SW phone support, software updates (UV741E) 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 User Access Management Software accessories

License

HP IMC User Access Manager Software Module Additional 50-user E-LTU	JG753AAE

Technical Specifications

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