HPE IMC User Access Management software

Key features

- Centralized user access management
- Support for IEEE 802.1X, MAC Authentication, BYOD and HPE Comware authentication portal
- Simplified self registration
- Advanced device profiling (fingerprinting)
- Concurrent licensing model

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 entire operation cycle.

HPE 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.
Features and benefits

Management
- User access management

Is a RADIUS server providing authentication, authorization, and accounting features. UAM provides access management services for Hewlett Packard Enterprise and third-party switches, routers, wireless, and VPN access gateways and supports 802.1X authentication protocols: PAP, CHAP, MS-CHAP, and MS-CHAPv2. UAM also leverages existing user directories such as a RADIUS proxy and works with LDAP-compliant user stores. Supports user access management for programs like BYOD

- Centralized access user and endpoint management

Offers centralized and secure authentication, authorization, and accounting services. UAM consists of a dedicated database, an embedded RADIUS server, options for a centralized or distributed UAM deployment, and support for primary and secondary UAM servers. UAM also offers a centralized Web portal for managing users and user groups, configuring user access policies, and applying policies to individual users and user groups

- User access authentication

Provides user authentication to access the network, including support for 802.1X, PAP, CHAP, EAP-MD5, EAP-PAP, EAP-TLS, EAP-PEAP-MSCHAPv2, and EAP-PEAP-MD5 authentication protocols. It also provides authentication for device users to access network devices. IMC UAM provides support to forward RADIUS authentication to third-party RADIUS servers and roaming authentication across UAM servers

- Device fingerprinting

Includes vendor, type, and OS to identify different endpoint devices. The device fingerprinting helps to manage access scenarios and perform transparent authentication on smart endpoint devices. UAM supports MAC OUI, HTTP User-Agent, DHCP options, and HPE iNode for endpoint identification

- Change-of-authorization support

UAM supports change-of-authorization attributes for a session; this feature is used to disconnect endpoints and apply new access policy

- User access authorization

Provides for authorizing users and managing network access using UAM’s user-based rights to control policy features such as IP and MAC address, NAS IP address, port, VLAN and QinQ VLAN, PC name, wireless SSID, terminal-to-domain, domain user login, and UAM's auto-learn and binding capabilities. It also assigns ACL and VLAN, user bandwidth consumption restrictions, manual IP address assignment, and limits on concurrent online users

- Portal authentication

Provides support for network authentication using portals. The methods included for portal authentication are HPE’s Comware authentication protocol or iNode client authentication

- User self-service management

Allows users to manage certain aspects of their account, network authentication and access

- Guest authentication

Allows the importing of guest accounts in batch-mode, self-registration, self-approval, approval by sponsors, guest and sponsor portal, print multiple vouchers, customized guest portal, and authentication by QR code
• Granular access control
  Allows verification of information such as access period policy, access device IP, SSID, endpoint IP, endpoint MAC, endpoint vendor, endpoint type, and endpoint OS before allowing the user to gain access to the network.

• 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 simply clicking; in a topology, administrators can clearly see the included access devices, view device information, or click to restrict device access.

• Ease of deployment
  Allows to use default configuration templates to activate authentication for guests and employees using personal or company endpoints.

• Endpoint configuration management
  Provides the quick configuration deployment functions for mobile devices; UAM deploys configurations to endpoints and activates the endpoint configurations such as wireless profile, mail settings, password policy, and VPN configuration.

• IPv6 support for portal authentication
  IMC UAM software supports the IPv6 protocol stack.

• Troubleshooting tool 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 to users who try to access the network.

• BYOD
  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.

• Enhancement of LDAP authentication
  An LDAP user can pre-register an access user account in IMC 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.

• Email support for sending guest user credentials
  When a guest user account is created, the credentials may be sent to the user by email.

• Enhanced IMC iNode client software
  Supports IPv6, and IEEE 802.1X authentication.

• Customization of client experience
  Enables user to customize portal pages and attributes of pages for smart devices; also enables the user to create custom pages for smart devices based on access scenarios, pre-registration pages and a self-service center home page.
Warranty and support

- Electronic and telephone support

Limited electronic and business-hours telephone support is available from Hewlett Packard Enterprise for the entire warranty period; to reach our support centers, refer to hpe.com/networking/contact-support; for details on the duration of support provided with your product purchase, refer to hpe.com/networking/warrantysummary

- Software releases

To find software for your product, refer to hpe.com/networking/support; for details on the software releases available with your product purchase, refer to hpe.com/networking/warrantysummary

HPE IMC User Access Management software

Specifications

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

<table>
<thead>
<tr>
<th>Minimum system requirements</th>
<th>Refer to the IMC UAM Release Notes for details about minimum system requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems requirements recommended</td>
<td>Refer to the IMC UAM Release Notes for details about system requirements recommended</td>
</tr>
<tr>
<td>Platform required</td>
<td>Server: HPE Intelligent Management Center Enterprise Software HPE Intelligent Management Center Standard Software</td>
</tr>
<tr>
<td>Browser supported</td>
<td>Refer to the IMC UAM Release Notes for details about browser supported</td>
</tr>
<tr>
<td>Notes</td>
<td>See the HPE IMC Standard or Enterprise Platform data sheet for the required software environment</td>
</tr>
<tr>
<td>Services</td>
<td>Refer to the Hewlett Packard Enterprise website at 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 Hewlett Packard Enterprise sales office</td>
</tr>
</tbody>
</table>

HPE IMC User Access Management software accessories

License

HPE IMC User Access Manager Software Module Additional 50-user E-LTU (JG753AAE)

Learn more at hpe.com/networking