IMC User Access Manager v5.2 (E0401) Copyright (c) 2011-2013 Hewlett-Packard Development Company, L.P. and its licensors.

Table of Contents

- 1. What's New in this Release
- 2. Problems Fixed in this Release
- 3. UAM Software Distribution Contents
- 4. Installation Prerequisites
- 5. <u>Typical Installation</u>
- 6. Upgrade Installation
- 7. <u>Un-Installation</u>
- 8. Multi-Language Support of IMC on Windows
- 9. <u>Restrictions and Cautions</u>
- 10. Port Usage
- 11. Known Problems

What's New in this Release

You can upgrade IMC UAM 5.1 (E0301) or any of its patched version to IMC UAM 5.2 (E0401). The following lists all features released after IMC UAM 5.1 SP1 (E0301P03).

Features released in IMC UAM 5.2 (E0401)

- 1. EAP-GTC authentication. This feature is configurable under Service >> User Access Manager >> Access Rule Management >> Add Service Configuration.
- Support authentication test mode. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> System Parameters. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> System Parameters.
- 3. BYOD user authentication. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> BYOD System Settings.
- 4. Sending account expiration alerts. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> Account Expiration Warning.
- Allowing online AD users to change their passwords(For Windows only and must cooperate with iNode client), This feature is configurable under Service >> User Access Manager >> LDAP Service >> LDAP Server >> Add LDAP Server.
- Providing an AAA configuration page for access devices. This feature is configurable under Service >> User Access Manager >> Access Device Management >> Access Device >> AAA Configuration.
- Providing an 802.1X and MAC authentication configuration page for access devices. This feature is configurable under Service >> User Access Manager >> Access Device Management >> Access Device >> AAA Configuration.

- 8. Providing a portal authentication configuration page for access devices.,This feature is configurable under Service >> User Access Manager >> Portal Service >> Device.
- 9. Batch deploying configurations to access devices. This feature is configurable under Service >> User Access Manager >> Access Device Management >> Access Device.
- 10. Viewing access device configurations. This feature is configurable under Service >> User Access Manager >> Access Device Management >> Access Device.
- 11. Quickly enabling 802.1X and portal authentication on access devices for users. This feature is configurable under Service >> User Access Manager >> Service Quick Experience.

Features released in IMC UAM 5.1 SP1 (E0301P03)

- 1. Device serial number bindings for authentication. This feature is configurable under Service >> User Access Manager >> Service Configuration >> Add Service Configuration.
- Applying for services based on user groups(Only Microsoft AD). This feature is configurable under Service >> User Access Manager >> LDAP Service >> LDAP Server >> Add LDAP Server.
- 3. User group synchronization based on OUs. This feature is configurable under Service >> User Access Manager >> LDAP Service >> LDAP Server >> Add LDAP Server.
- 4. Applying for services for LDAP users based on AD group priorities. This feature is configurable under Service >> User Access Manager >> Portal Service>> IP Group >>Add IP Group.
- 5. Trial accounts. This feature is configurable under User >> All Access Users >> Add Access User.
- 6. Temporary canceling of accounts. This feature is configurable under User >> All Access Users.
- 7. Applying for trial services in batches. This feature is configurable under User >> All Access Users.
- 8. SNAC authentication. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> SNAC Settings.
- 9. Password SMS messages for guest account setup. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> SMS Settings.
- Fast authentication on smart terminals(UAM must cooperate with the H3C wireless devices) This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> System Parameters.

Features released in IMC UAM 5.1 (E0301)

- 1. Supports binding one user account to multiple VLANs. This feature is configurable under User >> User Access Manager >>Add Access User.
- 2. Supports binding user accounts to hard disk serial numbers. This feature is configurable under Service >> User Access Manager >> Access Condition>> Hard Disk Serial Number.
- 3. Supports LDAP authentication for device management users. This feature is configurable under User >> Device Management User>> LDAP User.
- 4. Supports web-based authentication for IPv6. This feature is configurable under Service >> User Access Manager >> Portal Service>> IP Group >>Add IP Group.
- LDAP authentication supports using SSL. This feature is available only in the Windows edition of IMC. This feature is configurable under Service >> User Access Manager>> LDAP Service >> LDAP Server >> Add LDAP Server.
- 6. Allows you to set one password for multiple LDAP administrators. This feature is configurable under Service >> User Access Manager >> LDAP Service >>LDAP Server.
- 7. Notifies a third-party of a user's logon and logoff. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> Authentication Notify Parameters.

- 8. Displays prompts for online users at a scheduled time. This feature is configurable under Service >> User Access Manager >> Service Parameters >> System Settings >> User Prompt List >> Add User Prompt.
- 9. Supports deploying QoS configurations to HP ProCurve devices. This feature is configurable under Service >> User Access Manager >> Service Configuration >> Add Service Configuration.
- 10. User Authentication and Accounting Log. This feature is configurable under User >> Log Management >> User Authentication and Accounting Log

Features released in IMC UAM 5.0 SP1 (E0101P03)

- 1. A user can be associated with multiple access accounts. This feature is configurable under User > User Access Manager > Add Access User.
- 2. User groups can also be imported when users are imported. This feature is configurable under User > User Access Manager > Import Accounts in Batches.
- 3. When you delete an access account, you can select whether to delete the associated platform user. This feature is configurable under User > User Access Manager > Cancel Accounts.
- 4. Sort access accounts by creation time, with the latest created account at the top. This feature is configurable under User > User Access Manager > All Access Users.
- 5. Log the login operations of the device management users. This feature is configurable under User > User Access Manager > Log Management > Device Mgmt User Auth Log.
- 6. Support configuring and assigning proprietary RADIUS attributes for access devices. This feature is configurable under Service > User Access Manager > Access Device Management.

[Table of Contents]

Problems Fixed in this Release

IMC UAM 5.2 (E0401) fixed the following problems found in IMC UAM 5.1 SP1 (E0301P03):

- 1. Export all access user accounts from UAM when Oracle is used. The total number exceeds 20000. The export results might be inconsistent with the actual accounts. Some accounts are exported twice and some accounts are missing.
- 2. Click the Service tab, and then select User Access Manager > Service Parameters > Validate from the navigation tree of iMC. The Jserver process keeps running and the menu is clicked for more than 200 times. The page cannot be displayed and iMC malfunctions. For example, the client cannot be upgraded though the operator configures a client upgrade task in iMC.
- 3. Provide a file that contains Chinese characters in the computer name field. Select the Computer Name option as the account attributes for batch account import. The import operation fails. UAM displays that the computer names are invalid.
- 4. Add an LDAP server and assign an on-demand synchronization policy to the server. The base DNs use commas as the separator, and sub-base DNs use semi-colons as the separator.UAM cannot synchronize LDAP users in the OU that belongs to a sub-base DN.
- 5. Add an LDAP server that has user groups synchronized based on OUs. Assign an on-demand synchronization policy to the LDAP server. Configure more than 50 OUs on the AD.UAM synchronizes users in the first 50 OUs to the temporary list for authentication. Other users cannot be synchronized and cannot pass authentication.
- 6. Add an LDAP server that has user groups synchronized based on OUs. The base and administrator

DNs use semi-colons as the separator.UAM cannot add the LDAP server and displays an operation error or LDAP user synchronization error.

- 7. Add an LDAP server that has user groups synchronized based on OUs. Assign an on-demand synchronization policy to the LDAP server. Configure OUs on the AD.When the LDAP users are manually or automatically synchronized, UAM generates a large number of duplicate LDAP synchronization logs.
- 8. UAM contains more than 50 SSIDs and displays the first 50 SSIDs on the SSID list. When the operator clicks the Next Page or Last Page icon, UAM cannot refresh the SSID list and displays a server error.
- 9. An LDAP user uses an account with a user prefix (domain name) for PEAP-MS-CHAPv2 authentication, and the domain control server is a Windows 2003 Server. The user cannot pass the authentication. The system prompts that the username or password is incorrect.
- 10. Set up an iMC UAM stateful failover environment. The uamauthsrv process is always restarted. In a Windows operating system, you can view the process ID of the uamauthsrv process in the task manager. In a Linux operating system, you can view the process ID of the uamauthsrv process by using a process checking command. This problem affects the user authentication.
- 11. On the iMC console, set a deployment policy for the private attributes of third-party devices.A third-party device private attribute value can be set in only one of the authentication response packet and the accounting response packet.
- 12. Manually end the running portal process. The listening ports used by the portal process can be released. However, the portal process does not stop.

IMC UAM 5.1 SP1 (E0301P03) fixed the following problems found in IMC UAM 5.1 (E0301):

- 1. Add enough portal devices and then change the number of items to be displayed per page. If the operator selects a small number to display the portal devices in more than one page, only the first screen of portal devices is displayed, and the page navigation buttons disappear. Similar problems are found on the portal IP group list page and the user log list page.
- 2. If the portal configuration file contains an invalid server IP address, the portal server process is abnormal after it is started. The iMC deployment monitoring agent keeps enabling the portal server process. As a result, many memory resources are allocated to the portal server process, whereas other processes cannot run normally.
- 3. An iMC maintainer cannot view complete data on the UAM user homepage.
- 4. LDAP synchronization policies are assigned to multiple service groups, which are configured with different operator privileges. Use a maintainer to log in to IMC. The maintainer can view all LDAP synchronization policies in any service group.
- 5. Upgrade UAM to iMC UAM 5.1 (E0301). The access MAC address control is configured in the former UAM version. In iMC UAM 5.1 (E0301), operators must manually select the iNode Client Only option on the service configuration page and then enable access MAC address control.
- 6. A large number of users access the network by using EAP-TLS authentication. After a period of time, no more users can access the network by using any authentication. UAM displays an operation error message and generates the following log "[CEapTlsAuthen::createTlsSession] Allocate room for pstTlsSession failed."

IMC UAM 5.1 (E0301) fixed the following problems found in IMC UAM 5.0 (E0101):

- 1. Apply for a service for a user, cancel the service, and apply for the service again for the user. Then you cannot cancel the service. A message tells that the user has not applied for the service or the service has already been cancelled.
- 2. From the UAM online user list, initiate a remote desktop connection to a 64-bit operating system PC that runs iNode PC client. After the user enters the correct username and password, the remote

connection fails.

- 3. IMC UAM is in the stateful failover. The UAM background authentication process (uamauthsrv) abnormally exits for multiple times, and this problem affects user authentication.
- 4. The supplementary information of a user account is null. Set the information and then clear the setting. Use the supplementary information as the query criterion in the advanced query. Then a message like "unknown error" appears and no match can be found.
- 5. If a large number of users are getting online, the policy server may not send back replies to the policy proxy server. As a result, some users cannot get online and their clients display the message that the policy server does not respond.
- 6. Configure EAP authentication on the access devices. User authentication may fail because devices of some vendors do not send user MAC addresses to IMC.

[Table of Contents]

UAM Software Distribution Contents

The UAM software contains the following files and folders:

- 1. UAM\manual\readme_uam_5.1 (E0401).html -this file
- 2. UAM\install -the UAM installation program.

Note: If only UAM is deployed, please install the client software under iNode.

[Table of Contents]

Installation Prerequisites

PC Requirements

The following are the minimum hardware and software requirements for running IMC on a PC server:

- Minimum hardware requirements
 - 4-core CPU, 2.8 GHz
 - \circ RAM \geq 8G
 - hard disk space ≥ 160G
- Operating system (Versions marked X64 are recommended):
 - 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
 - o 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
 - o 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
- VMware:
 - VMware Workstation 6.5.x
 - VMware ESX Server 4.x
- Database
 - Microsoft SQL Server 2005 Service Pack 3 (Windows only)
 - Microsoft SQL Server 2008 Service Pack 3 (Windows only)
 - Microsoft SQL Server 2008 Service Pack 3 (64-bit) (Windows 64-bit only)
 - Microsoft SQL Server 2008 R2 Service Pack 1 (Windows only)
 - Microsoft SQL Server 2008 R2 Service Pack 1 (64-bit) (Windows 64-bit only)
 - Microsoft SQL Server 2012 Service Pack 1 (Windows only)
 - Oracle 11g Release 1 (Linux only)
 - Oracle 11g Release 2 (Linux only)
 - Oracle 11g Release 2 (64-bit) (Linux only)
 - MySQL Enterprise Server 5.5 (Linux and Windows)(Up to 2000 users are supported)
- IMC Platform Compatibility
 - IMC Platform version: IMC PLAT 5.2 (E0401) or later

Note: 64-bit operating systems are recommended over 32-bit operating systems because of the larger amount of available memory for applications.

Note: Optimal hardware requirements vary with scale, other management factors, and are specific to each infrastructure. Please consult HP, or your local account teams and precise requirements can be provided.

[Table of Contents]

Typical Installation

Before installing UAM, make sure the IMC is installed correctly. To install UAM, click Install on the Monitor tab of the Intelligent Deployment Monitoring Agent, then select the components sub-directory of the upgrade package, and click OK to launch the installation wizard.

For more information about the installation instructions, see the IMC Installation Guide.

[Table of Contents]

Upgrade Installation

Follow these instructions to upgrade IMC UAM:

- 1. Back up the IMC database on the Environment tab in Intelligent Deployment Monitoring Agent.
- 2. Stop the IMC system in the Deployment Monitoring Agent.
- 3. Click **Install** in the **Monitor** tab of the Intelligent Deployment Monitoring Agent.
- 4. Select the *install/components* subdirectory of the upgrade package, and click **OK**.
- 5. After the installation is complete, the Intelligent Deployment Monitoring Agent lists the components that need to be upgraded. Click **OK** to start upgrading the components.
- 6. If this is a distributed deployment, upgrade the components deployed on the slave servers separately.
- 7. After the upgrade is complete, start all processes in the Intelligent Deployment Monitoring Agent window.

[Table of Contents]

Un-Installation

You can remove UAM component through the intelligent deployment monitoring agent. To do this, follow these steps:

- 1. In the **Intelligent Deployment Monitoring Agent** window, click **Stop IMC** on the **Monitor** tab to stop all processes of IMC.
- 2. On the **Deploy** tab, right-click the UAM component, and select **Uninstall the Component** from the shortcut menu.
- 3. When an un-installation succeeded dialog box appears, click **OK**.

[Table of Contents]

Multi-Language Support of IMC on Windows

In a non-English environment, IMC supports the same language as the operating system without any additional configuration.

If the desired non-English version of Windows is not available, strictly follow these steps to install the operating system and software so IMC can support the language:

- 1. Install an English Windows operating system.
- 2. Install the language pack.
- 3. Modify the region and language settings in the operating system.
- 4. Install an English version of SQL Server database.
- 5. Install IMC.

The following example describes how to modify the region and language settings in Windows 2008 server that has a Thai language pack.

- Select Start >> Control Panel and click Region and Language.
- Select Thai(Thailand) from the dropdown list on the Formats tab.
- Select Thailand from the dropdown list on the Location tab.
- Select Thai from the dropdown list on the Keyboards and Languages tab.
- Click Change system locale on the Administrative tab.
- Select Thai(Thailand) from the dropdown list, and click OK.
- Click Copy Settings on the Administrative tab.
- Select Welcome screen and system accounts and New user accounts, and click OK.
- Log out and re-log on to the operating system.

[Table of Contents]

Restrictions and Cautions

- To use the IPv6 feature on iMC that is upgraded from an early version, add the IPv6 address of the components to the address configuration file of iMC.
- To use the BYOD feature, deploy it on a separate server. For IMC in centralized deployment or upgraded from an early version, make sure the Web server uses port 80. Otherwise, set both the imc.http.port parameter in the \client\conf\http.properties file at the IMC installation path and the iMC Service Port in the UAM system settings to 80, restart iMC, and restart the jserver process in the Intelligent Deployment Monitoring Agent. The Self-Service Port in the UAM system settings need not be changed.
- The UAM installation disk contains the installation packages for H3C and HP IMC DHCP Agents. To support obtaining endpoint information through DHCP character, install and configure an agent on the DHCP server.
- When IMC is installed in the Oracle database, suppose IMC uses separate databases and IMC UAM and IMC PLAT are deployed in distributed mode (IMC PLAT is deployed on a host, IMC UAM on another, and the database installed on another). In this case, you should add a service naming record in the file \$ORACLE_HOME/network/admin/tnsname.ora of the database:

```
10_153_128_178 =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.153.128.178)(PORT = 1521)
)
)
(CONNECT_DATA =
(SERVICE_NAME = IMC)
)
```

Among the three bold texts, the first is the Oracle service name, which must be modified into the underline-separated address of the host where the Oracle resides; the second is the database IP address, which must be modified into the IP address of the host where the database resides; the third is the Oracle database SID, which must be modified into the actual SID of the database.

• If you modify the IP address of the IMC Platform that is deployed on a different server than UAM or EAD, execute the following scripts on the subordinate server so the server can create a database link to the IMC Platform.

Log in as the sa user, select the database "ead," and execute the following scripts: if exists (select * from master.dbo.sysservers where srvname = N'uam2platdblink')

EXEC sp_dropserver N'uam2platdblink', N'droplogins' GO EXEC sp_addlinkedserver @server=N'uam2platdblink', @srvproduct=", @provider='SQLOLEDB', @datasrc=N'\$iMC_PLAT_SERVER_IP' GO EXEC sp_addlinkedsrvlogin N'uam2platdblink', N'false', null, N'sa', N'\$SA_USER_PASSWORD'

```
GO
```

In the previous scripts, \$iMC_PLAT_SERVER_IP represents the IP address of the server on which the IMC Platform is deployed, and \$SA_USER_PASSWORD represents the password of the sa user to access the database of the IMC Platform.

[Table of Contents]

Port Usage

The following TCP/IP Ports are used.

Port	Usage
UDP 1812	Default UAM authentication port.
UDP 1813	Default UAM accounting port.
UDP 1810	UAM background port for listening to commands from the foreground.
UDP 389	Default LDAP server port.
UDP 9096	Port for monitoring the user self-service process status.
UDP 9093	Port for monitoring the Portal server process status.
UDP 9094	Port for monitoring the Portal client process status.
UDP 50100	Port for the Portal Kernel to receive Portal requests or responses sent by a device, and to receive Portal requests sent by clients.
UDP 50200	Port for the Portal proxy to receive Portal requests sent by clients.
UDP 50300	Port for the Portal proxy to receive Portal responses sent by kernel.
UDP 50600	Port for the Portal proxy to receive register requests sent by kernel.
UDP 50700	Port of the Portal Kernel for listening to commands from the Portal proxy.
UDP 50800	Port for the Portal Kernel to receive requests or responses sent by Portal proxy.
UDP	Port of the Portal Kernel for listening to commands from the foreground.

50900	
UDP 2000	Port of the Portal kernel for sending packets to devices.
UDP 8020	Port for monitoring IMC monitoring agent status when user self-service is deployed independently of UAM.

[Table of Contents]

Known Problems

Installation/Upgrade/Patch

None

Other Problems

- A lack of file resource error appears during installation of the HP DHCP Agent on 64-bit Window.Click OK in the message box. The HP DHCP Agent can be successfully installed and normally operates.
- When working with HP MSM, UAM does not automatically log off users whose endpoint information obtained through DHCP is inconsistent with the existing data in the database. The administrator can query users who have inconsistent endpoint information and manually log them off.

[Table of Contents]

Issued: Jun. 2013 Copyright (c) 2011-2013 Hewlett-Packard Development Company, L.P. and its licensors.