IMC

TACACS+ Authentication Manager 7.1 (E0302P13)

Table of Contents

1. What's New in this Release
2. Problems Fixed in this Release
3. TAM Software Distribution Contents
4. Installation Prerequisites
5. Upgrade Installation
6. Un-Installation
7. Restrictions and Cautions
8. Port Usage
9. Known Problems

What's New in this Release

IMC TAM 7.1 (E0302P13) can be upgrade from IMC TAM 7.1 (E0302), IMC TAM 7.1 (E0302P06), IMC TAM 7.1 (E0302P07), IMC TAM 7.1 (E0302P08), IMC TAM 7.1 (E0302H09) and IMC TAM 7.1 (E0302P10). The following lists all features released after IMC TAM 7.0 (E0103).

Features released in IMC TAM 7.1 (E0302P13)

None.

Features released in IMC TAM 7.1 (E0302P10)

REST APIs are added to import devices and device users to IMC TAM.

Features released in IMC TAM 7.1 (E0302H09)

Provides RESTful APIs.

Features released in IMC TAM 7.1 (E0302P08)

None.

Features released in IMC TAM 7.1 (E0302P07)

None.

Features released in IMC TAM 7.1 (E0302P06)

1. Support for FQDN and the short name attribute of devices.
2. In the self-service center, device users can send privilege-increase applications with specific expiration time to administrators for approval.
3. The username and authorization policy attributes were added to the device user list.

Features released in IMC TAM 7.1 (E0302)

None.

Features released in IMC TAM 7.1 (E0301)

None.

Features released in IMC TAM 7.0 (E0203P04)

None.

Features released in IMC TAM 7.0 (E0203P03)

None.

Features released in IMC TAM 7.0 (E0203)

None.

Features released in IMC TAM 7.0 (E0202)

1. The user self-service center is optimized to allow logins as a device management user and provides the basic information page for the device management user.
2. In command set configuration, the command name and parameter attributes are combined into one attribute named Command. Regular expressions are supported for command matching.
3. Device management user authentication uses "fixed password + RSA dynamic password" mode. By default, RSA authentication is disabled. RSA authentication parameters can be configured in system settings.
4. When IMC TAM runs on a Windows server, it can establish SSL connections with LDAP servers.
5. Different device areas can include sub-areas of the same name. Different device types can include sub-types of the same name.

Features released in IMC TAM 7.0 (E0103P02)

None.

Features released in IMC TAM 7.0 (E0103)

None.

[Table of Contents]

Problems Fixed in this Release

IMC TAM 7.1 (E0302P13) fixes the following problems, including all bugs fixed after IMC TAM 7.0 (E0103):

Resolved Problems in IMC TAM 7.1 (E0302P13)

None.

Resolved Problems in IMC TAM 7.1 (E0302P10)

None.

Resolved Problems in IMC TAM 7.1 (E0302H09)

None.

Resolved Problems in IMC TAM 7.1 (E0302P08)

The system performs certificate authentication for access users. A Denial of Service attack might be launched and causes a server memory leak by exploiting security vulnerability CVE-2015-0205, CVE-2014-3570, CVE-2015-0204, or CVE-2014-3572.

Resolved Problems in IMC TAM 7.1 (E0302P07)

The maximum string length of **Filter Condition** field on the LDAP sync policy configuration page is changed from 128 characters to 256 characters.

Resolved Problems in IMC TAM 7.1 (E0302P06)

If TAM is deployed on a Windows server and UAM is not deployed, operators cannot import certificates to the SSL-enabled LDAP servers in TAM.

Resolved Problems in IMC TAM 7.1 (E0302)

None.

Resolved Problems in IMC TAM 7.1 (E0301)

Both UAM and TAM components are deployed and the UAM license is expired. If iMC is restarted, an error page will appear at iMC login.

Resolved Problems in IMC TAM 7.0 (E0203P04)

None.

Resolved Problems in IMC TAM 7.0 (E0203P03)

1. After login, an operator can access files on the IMC server directly through the IMC TAM tamServletDownload Servlet. This poses a security threat to the IMC server.

Resolved Problems in IMC TAM 7.0 (E0203)

1. When the Oracle database is used, an operator attempts to add an LDAP server without providing the server administrator's password. The LDAP server cannot be added and an error message appears.

Resolved Problems in IMC TAM 7.0 (E0202)

1. When TAM is running on a trial iMC platform, it is shown as a trial version in the About information, whether TAM is formal or trial.

Resolved Problems in IMC TAM 7.0 (E0103P02)

1. TAM cannot synchronize LDAP users when a large number of users exist on LDAP servers.
2. A user cannot log on to the device if it is synchronized from an OpenLDAP server.

Resolved Problems in IMC TAM 7.0 (E0103)

1. The blacklist user list displays an error when an operator changes the number of entries to display per page, or when an operator pages forward or backward in the list. The log list has similar problems.
2. An error occurs if an operator clears all selected devices and reselects devices.
3. The paging function of the candidate user list might be unavailable when an operator binds a new user to an existing sync policy.
4. After the value of the **Displays Key in** parameter is changed in the system parameter settings, the system records incorrect operation logs.

[Table of Contents]

TAM Software Distribution Contents

The TAM software contains the following files and folders:

1. **TAM\manual\readme_tam_7.1 (E0302P13).html** - this file

2. **TAM\install** - the TAM installation program.

[Table of Contents]

Installation Prerequisites

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
  - RAM ≥ 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
  - 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 X64 with Service Pack 1
  - Windows Server 2012 X64 with KB2836988
  - Red Hat Enterprise Linux 5 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.5 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.5 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 6.4 X64 (Enterprise and Standard versions only)

- VMware:
  - VMware ESX Server 4.x
  - VMware ESX Server 5.x

- Hyper-V:

    - Windows Server 2008 R2 Hyper-V
    - Windows Server 2012 Hyper-V

- Database
    - Microsoft SQL Server 2008 Service Pack 3 (Windows only)
    - Microsoft SQL Server 2008 R2 Service Pack 2 (Windows only)
    - Microsoft SQL Server 2012 Service Pack 1 (Windows only)
    - Oracle 11*g* Release 1 (Linux only)
    - Oracle 11*g* Release 2 (Linux only)
    - Oracle 11*g* Release 2 (64-bit) (Linux only)
    - MySQL Enterprise Server 5.1 (Linux and Windows) (Up to 1000 devices are supported)
    - MySQL Enterprise Server 5.5 (Linux and Windows) (Up to 1000 devices are supported)
    - MySQL Enterprise Server 5.6 (Linux and Windows) (Up to 1000 devices are supported)

- IMC Platform Compatibility
    - IMC Platform version: IMC PLAT 7.1 (E0301)

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]

Upgrade Installation

Please follow these instructions for upgrading the IMC:

1. Back up the IMC database on the **Environment** tab in Deployment Monitoring Agent.
2. Manually copy the IMC installation directory to a backup path.
3. Stop the IMC system in the Deployment Monitoring Agent.
4. Click **Install** button in the **Monitor** tab of the Deployment Monitoring Agent.
5. Select the *install/components* subdirectory of the upgrade package, and click **OK**.

6. After the installation finishes, the Deployment Monitoring Agent will detect the components that need to be upgraded. Click **OK** button to start upgrading the components.
7. If this is a Distributed deployment, upgrade all components deployed on all slave servers separately.
8. After upgrade is complete, start all processes through the Intelligent Deployment Monitoring Agent.

[Table of Contents]

Un-Installation

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

1. On the Intelligent Deployment Monitoring Agent window, select the **Monitor** tab, and click **Stop IMC** to stop all processes of IMC.
2. On the **Deploy** tab, right-click the TAM component, and select **Undeploy the Component** from the shortcut menu.
3. A dialog box appears, indicating that the component was successfully removed. Click **OK**.

[Table of Contents]

Restrictions and Cautions

- During the deployment of TAM in Windows or Linux, the password set for the database user tam must not contain "&". Otherwise, the deployment does not work.
- IMC TAM does not support LDAP authentication in the scenario where the TAM and LDAP server communicate through a NAT device.
- The user password on the LDAP server cannot contain any space. Otherwise, the LDAP user will fail to be synchronized.
- Restricted for use on specific sites with TAM-LDAP communication over SSL connections.

[Table of Contents]

Port Usage

The TAM Server will BIND to and use the following TCP/IP Ports.

Component	Subcomponent	Protocol	Port	Configurable	Use	Server	Client	Notes
TAM	-	UDP	1890	No	TAM background port for listening to commands from the foreground	IMC master and subordinate servers.	IMC master and subordinate servers.	Internal use.
TAM	-	TCP	49	No	Default TAM authentication port	IMC master and subordinate servers.	Network devices.	Internal use.
TAM	-	TCP	359	No	Default LDAP server port	LDAP Servers.	IMC master and subordinate servers.	Internal use.

[Table of Contents]

Known Problems

Installation/Upgrade/Patch

None.

Other Problems

None.

[Table of Contents]

Issued: May. 2015