IMC

Endpoint Admission Defense v7.0 (E0103)

Table of Contents

What's New in this Release

IMC EAD 7.0 (E0103) can be installed directly, or you can upgrade from IMC EAD 5.1 (E0301) or later versions. The following lists all features released after IMC EAD 5.2 (E0401).

Features released in IMC EAD 7.0 (E0103)

1. The way the total number of users permitted by a license is counted is changed from by managed users to by online users.
2. Identifying endpoints based on information reported by the iNode client.
3. Applying different offline ACLs according to the ping results of specific IP addresses.
4. Informing endpoint users of disabled peripheral devices.
5. Providing the software statistics report for a specific asset and the asset statistics report for specific software products.
6. Real-time monitoring for isolated endpoints.
7. Querying assets by OS login name and including a MAC address list in asset information.
8. The Endpoint Admission Defense menu is renamed to User Security Policy and moved from the Service tab to the User tab.
9. EAD can detect weak operating system passwords based on only the iMC dictionary files.

Features released in IMC EAD 5.2 (E0402P05)

None.

Features released in IMC EAD 5.2 (E0402)

None.

Features released in IMC EAD 5.2 (E0401)

1. Configuring Internet access audit policies to audit both authenticated and unauthenticated Internet access behaviors, and access attempts to the blocked websites. In an Internet access audit policy, operators can configure whether or not to audit an Internet access behavior by destination IP address, destination port, and protocol.
2. An Internet access audit log records detailed information about a user's Internet access behaviors, including the destination IP address, source IP address, destination port, protocol number, NIC name, MAC address, and number of packets. To control the log size, EAD provides aggregation, lifetime, and maximum entries for the logs.
3. GPS, auto lock, and Bluetooth status check on Android smart terminals.
4. Providing service quick experience for portal and 802.1X users. Service quick experience enables users to complete authentication configuration, including service, user account, security policy, and access device parameters, on a single page and quickly verify the authentication result.
5. Providing APIs for querying the USB monitor logs, Internet access audit logs, and security check failures.
6. Providing advanced query for assets by service installation status (installed or not installed), service status (running or not running), and process status (running or not running).
7. Anti-virus software check for Mac OS.

[Table of Contents]

Problems Fixed in this Release

IMC EAD 7.0 (E0103) fixes the following problems, including all bugs fixed after IMC EAD 5.2 (E0401).

Resolved Problems in IMC EAD 7.0 (E0103)

1. The security log details page cannot display the complete contents of some information.
2. EAD is configured to detect weak passwords for local users. The OS login name includes domain information. EAD does not check the password for the OS login name that includes domain information.
3. Click the Desktop Asset Manager link on the Export History page for USB File Transfer. Contents on the linked page are incorrect.

Resolved Problems in IMC EAD 5.2 (E0402P05)

1. Before the upgrade, if you attempt to delete a smart terminal policy that is disassociated from a security policy, EAD prompts that the policy is being used by a security policy and cannot be deleted. The symptom persists after you upgrade IMC EAD.
2. A security policy with the URL access control function enabled is applied to a client that does not support URL access control. However, the user is not forcibly logged off after getting online.
3. A process that is configured in the Check Processes after Security Check area failed to pass the check.EAD cannot display a prompt message when a process configured in the Check Processes after Security Check area fails to pass the check.
4. A security policy that contains Internet Access Control settings is applied to an iNode client that supports the Internet access control function, but no client ACL is specified in the Internet Access Control settings. When the user gets online, the iNode client displays an incorrect message asking the user to enable the ACL function.
5. AAA configuration failed to be deployed again after a previous successful deployment.

Resolved Problems in IMC EAD 5.2 (E0402)

1. A third-party Web application URL is configured in Service > User Access Manager > Service Parameters > Unified Authentication.The third-party Web application cannot decrypt the user name and password because the iNode client uses an incorrect encryption algorithm, and the endpoint user cannot log in to the Web application system.
2. The Lock Internet Access Ability feature is enabled, and both or either of the ACL for All but Authenticated NIC field and ACL for Unauthenticated Hosts field is empty.The iNode client prompts that it cannot obtain the ACL policy and logs off the user.
3. The isolation and security ACL/VLAN setting is configured in the security policy.The endpoint user is logged off because the access device cannot identify the isolation or security ACL/VLAN setting that is deployed by the policy server.

Resolved Problems in IMC EAD 5.2 (E0401)

1. When DBMAN cold backup is used, the identity authentication and security authentication are switched to the backup server. The server will deploy the IP address and port of the cold backup server, so that iNode will report the desktop asset change information to the backup server. As a result, the desktop asset change information on the primary server is inconsistent with that on the backup server.
2. Add an administrator group. The user access module management right is not assigned to the administrator group. When an administrator in the group logs in to the console, the User tab is not displayed. However, when the administrator adds an asset, the administrator can add or select the owner.
3. EAD has recorded more than 50,000 USB monitor logs for a user over the last 12 hours. The Display Asset Monitoring Information parameter is enabled in the DAM service parameter settings. Description: EAD displays a JServer error message when you attempt to access the user's Access Account Info page by clicking the user account name.

4. In a network whicevices that partially support RADIUS, the user has logged in. When the account of a user who has logged in expires, the user is not automatically logged out.

[Table of Contents]

EAD Software Distribution Contents

The EAD software contains the following files and folders:

1. **EAD\manual\readme_ead_7.0 (E0103).html** - this file
2. **EAD\install** - the EAD installation program

[Table of Contents]

Installation Prerequisites

Server 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
  - 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 2005 Service Pack 4 (Windows only)
    - 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 7.0 (E0102) or later

- IMC UAM Component compatibility

- IMC UAM version: IMC UAM 7.0 (E0103) 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]

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. Stop the IMC system in the Deployment Monitoring Agent.
3. Click **Install** button in the **Monitor** tab of the Deployment Monitoring Agent.
4. Select the *install/components* subdirectory of the upgrade package, and click **OK**.
5. 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.
6. If this is a Distributed deployment, upgrade all components deployed on all slave servers separately.
7. After upgrade is complete, start all processes through the Intelligent Deployment Monitoring Agent.

[Table of Contents]

Un-Installation

You can remove EAD 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 EAD component, and select **Uninstall the Component** from the shortcut menu.
3. A dialog box appears, indicating that the component was successfully removed. 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.

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

[Table of Contents]

Restrictions and Cautions

1. If you configure your EAD security policy to check installation of software, be careful not to change software names or application names. If the name of a software product or application is changed, it cannot be detected due to the Microsoft Windows limitation.
2. Because the commercial software on which the HP iNode client relies cannot get the actual virus definitions of McAfee SecurityCenter 9.1.08, it is recommended that the iNode client collaborate with McAfee SecurityCenter 9.1.08 to implement the EAD solution, and that the virus definition check mode be set to auto sensing instead of a certain date.

3. Due to OPSWAT restrictions, anti-virus software detection with OPSWAT may not be able to identify versions of the virus definition files, or scan engines of anti-virus software.
4. With Asset-Access Account Binding enabled in the DAM service parameter settings (select Desktop Asset Service > Service Parameters), when a user uses an iNode client of the iNode 3.60-E6209 version or higher for authentication, the asset-access account binding function takes effect; when a user uses an iNode client of the iNode 3.60-E6208 version or lower for authentication, the asset-access account binding function does not take effect, that is, the asset can be successfully registered even if the access account does not match the asset owner.
5. To use EAD hierarchical node management, make sure that the edition and language of operating systems for parent and child IMC servers, IMC UAM, and IMC EAD are identical.

[Table of Contents]

Port Usage

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

Port	Usage
UDP 8010	Port of the EAD policy server for listening to commands
UDP 8026	Port of the EAD policy server for listening to log level update messages from the Console
UDP 9013	Port of the EAD policy server for listening to commands from the Console
UDP 9015	Port of the EAD policy server for listening to requests from the EAD agent
UDP 9017	Port of the EAD agent for listening to responses from the policy server
UDP 9019	Port of the EAD agent for listening to EAD authentication requests and responses sent by clients
UDP 9035	Port of the EAD policy server for listening to UDP requests from the UAM background
UDP 9033	Local port of the EAD policy server for Session Control packets to be sent to the access device
UDP 8015	Port of the DAM server for listening to commands
UDP 8027	Port of the DAM server for listening to log level update messages from the Console
UDP 9023	Port of the DAM server for listening to configuration commands
TCP 9025	Port of the DAM server for listening to requests from the DAM agent
TCP 9027	Port of the DAM agent for listening to responses from the DAM server
UDP 9029	Port of the DAM agent for listening to requests from clients

[Table of Contents]

Known Problems

Installation/Upgrade/Patch

- None

Other Problems

- View an Insecurity Category Statistic Report. The Insecurity Category Statistic Report does not include guest statistics.

[Table of Contents]

Issued: Sep 2013