# IMC

## Intelligent Management Center PLAT 7.3 (E0710)



---

# Table of Contents



---

# What's New in this Release

This version can be upgraded from version IMC PLAT 7.3 (E0708) and its patches.
Warning: IMC UAM 7.3 E0623 and below versions are not compatible with IMC PLAT 7.3 E0710, please do not upgrade the IMC with UAM installed to E0710.

Warning: Do not upgrade IMC in a Server 2008 environment as it will result in the application being removed. Please migrate to a supported Operating System.

Warning: During migration, please copy the encryption keys from the old IMC to the new IMC and database servers or the new database will be corrupted:

- Before restoring the old database on the new migrated system, please copy $iMC/common/conf/ks.dat and $iMC/server/conf/imchw.conf files from the old IMC server to the corresponding directories on all IMC platform and subordinate servers, including the remote database server.
- Reboot all the servers so the encryption keys take effect.
- Restore the database.

To upgrade from versions prior to V7.3, upgrade both the IMC Platform and all the deployed service components through each released version. The upgrade path is V3.3 >> V5.0 >> V5.1 >> V5.2 >> V7.0 >> V7.1>> V7.2>> V7.3. Before you upgrade the IMC Platform, download upgrade packages for all deployed service components from HPE's website, and before you install them pay special attention to the section "Platform Compatibility" in their readme. If an upgrade package is not available for a service component, HPE recommends not upgrading the IMC Platform, or you can remove the service component before upgrading the IMC Platform. When the service component is removed, its data is lost. It is not possible to import the database taken from a previous version into V7.3.

The following lists all features released in IMC PLAT 7.2 (E0403) and later versions.

## Features released in IMC PLAT 7.3 (E0710)

- Added explanations to the online help for notifications during the alarm forwarding rule stage on the Alarm > Alarm Settings > Alarm Notification page.
- Added explanations to the online help for performance reports on the Performance Management Help > Operation Guide > Performance View > Displaying Performance View Data page.
- Added explanations to the ACL rule set function on the Service > ACL Management > ACL Resource page.
- Added Aruba OS-CX support for restapi v10.09.
- Added support for importing links on the Resource>Network Topology>right click>Link Management page.
- Added support for exporting device interface list on the Resource>Device view>A managed device information>Interface List page.
- After switching the theme, changing the browser or clearing the browser cache will not change the theme on the Theme page.
- Added the manual and auto sync functions in interface view on the System>System Configuration>System Settings page.

## Features released in IMC PLAT 7.3 (E0708P03)

- Added support for manually or automatically synchronizing port groups on the Resource > View Management > Port Group page (Run Rule Button).

## Features released in IMC PLAT 7.3 (E0708P02)

- Added deployment policy for device software deployment (in steps): Setting the running software as the backup startup software on the Service > Configuration Center > Deployment Guide > Deploy Device Software or Deploy Device Software (Step by step).
- Added deployment policy for device software deployment (in steps): ISSU support on the Service > Configuration Center > Deployment Guide > Deploy Device Software or Deploy Device Software (Step by step).
- ICC support for Nortel devices
- Added the device group and device relationship report on the Report > Report Template List page.
- Added the custom view and device relationship report on the Report > Report Template List page.
- Added device name fuzzy matching to rules for automatically joining the device group on the System > Group Management > Device Group > Add Device Group page.
- Setting the link lost color for the network topology in the advanced settings for the topology on the Resource > Network Topology > Advanced Settings > Color Settings.
- During LDAP authentication for an operator, if the user attribute is changed on the LDAP server, the login is denied on the System > Operator Management > Authentication Server.
- The device software library supports importing software of Aruba devices (6300M or later models) on the Service > Configuration Center > Software Library.
- To read the STP port table if the MSTP port table is missing to maintain the MSTP topology on the Resource > Network Topology > Custom Topology > My Network View (MSTP Instance icon).
- ICC To adding these devices to the adapter-index.xml file for Cisco, ciscoC11118P, ciscoC1111X8P, ciscoC9606RVirtualStack, ciscoC9606R, and ciscoCat9500VirtualStack.

## Features released in IMC PLAT 7.3 (E0708)

- Added support for stacking topology of Brocade devices on the Resource > Network Topology.
- Added SNMPv2 and SSH support for auto deployment plans on the Resource > Device View > Device Details. To use this feature, 1)configure adp_snmp_version=2 in the qvdm.conf file, 2)select SSH as the login type for target device.
- Windows server is enabled with TLS 1.2.
- Upgraded plink to plink0.76.
- IMC backup archive management supports path configuration. To use this feature, configure cfgArchiveDir=path in the qvdm.conf file.
- IP address conflict detection is enabled by default. You can disable the feature as needed on the System > Resource Management > IP Conflict Management page.

- If the platform version is upgraded but the component version is not upgraded and the component version is incompatible with the platform version, you can open the login page.
- Add support for JL693A 2930F.
- Add support for Aruba CX software image file.

## Features released in IMC PLAT 7.3 (E0706P11)

- 202107130001W IMC Configuration Center can display the latest software available for MSR95x on the Service > Configuration Center.
- Support for displaying information about the link between AirWave AP and a switch on the Resource > Network Topology > Converged Topology.
- Support for right-click menus for aggregate links in the topology page.
- Added the support for displaying interface rate and interface type for aggregate links in the topology page.
- Support of ICC for automatically selecting the matching plink version, such as plink0.70 and plink0.76.
- Upgraded PSFTP and PSCP version to 0.76.
- Support of ICC for Aruba7000 series devices.
- Added the **Topology Report (including aggregate subinterfaces) V2** report. The **Port** column of this report includes the member ports of aggregate interfaces.

## Features released in IMC PLAT 7.3 (E0706H08)

- None

## Features released in IMC PLAT 7.3 (E0706H07)

- None

## Features released in IMC PLAT 7.3 (E0706P06)

- Added the **Back up Running Software to Local Server** option to the Deploy Device Software and Restore Device Software pages in iCC.
- Added support of iCC for setting the **storage path** for backup configuration file on the System > Configuration Center > Options.
- Added support for backing up device configuration at the CLI for ProCurve devices in OOBM mode.
- Added compatible devices (1.3.6.1.4.1.9.1.2068) to iCC.
- iCC supports archiving backup configuration files. To use this feature, configure **create_zip_job=1** in the **qvdm.conf** file. Additionally, you can configure the archiving path through the **cfgArchiveDir** field in this file.
- Added support of ADP for deploying configuration to devices through Telnet or SSH.
- Added support for using the system ping method to detect the device response time, which can be enabled by adding the **use_system_ping = true** line to the **qvdm.conf** configuration file.
- Added plink versions plink0.74 and plink0.76. The plink0.74 and plink0.76 processes must be added to **server/bin**. To configure the plink versions that a device can use, create the **puttyVersion.cfg** file in the **$IMCROOT/server/conf** directory, and add devices in the following formats. Example:
  10.114.126.202 = plink76
  10.114.126.203 = plink74

## Features released in IMC PLAT 7.3 (E0706)

- Support for bulk deleting operator groups was added.
- Support for exporting SMC event data was added on the System > System Configuration > Data Export page.
- Support for configuring the Report Retention Period (Days) option was added.
- The Network Interface Usage Statistics template was added on the Report > Report Template List page.
- The Custom View-Specific Interface Report template was added on the Report > Report Template List page.
- The Device Interfaces Report V2 template was added on the Report > Report Template List page.
- Support for SSH (plink) was added on the Resource > Device View page in the Windows operating system.

1) Click Download SSH (Plink) File in the right action pane to download the SSH (Plink) file to your local client.
2) Decompress the downloaded SSH (Plink) file to the C:\localssh directory.
3) Double-click registry file localssh_reg.reg in the C:\localssh\ directory to import it, and restart the browser and log in again.
4) On the details page for a device, click the SSH (Plink) link to remotely log in to the device.

- Support for checking the max server memory was added for SQL Server installation.
- The Serial Number and Software Version columns were added on the Resource > Device View page.
- Support for comparing a device ACL with the ACL template was added
- Support for QoS Resource List was added on the Service > ACL Management > Assistant page.
- Support for ACL MAC Address Authentication was added on the Service > ACL Management > Assistant page.
- Support for enabling and disabling a trap filter rule were added on the Alarm > Trap Management > Filtering Trap page.
- Support for bulk deleting trap definitions was added on the Alarm > Trap Management > Trap Definition page.
- Support for modifying email addresses was added on the Alarm > Alarm Settings > Alarm Notification > Modify Mail Notification page.
- Support for viewing alarm repeat times was added on the Alarm > Alarm Browse > All Alarms > Alarm Details page.
- Support for backing up configurations for Cisco ASR1006-X routers with SYSOID 1.3.6.1.4.1.9.1.2143 was added on ICC.
- Support for synchronizing the System Name field was added when the system was checking the device state periodically.
- Support for the Oracle 19c(64 bit) and SQL Server 2019 Enterprise (64 bit) databases was added to IMC.
- The default password for the administrator changes to Pwd@12345 when you install IMC.
- The name of the Interface Report changes to Device-Specific Interface Report.
- The devId parameter becomes optional for the /perf/summaryData query. If the parameter is not configured, IMC queries the performance of all devices.
- By default, IMC uses plink to establish sessions when SSHing to devices. To disable this feature, delete the putty07 file in the server/conf directory.
- The Enable NetEdit option was added on the System > System Configuration > System Settings page. To open the NetEdit page for a device after enabling this feature, access the Resource > Network Assets page, click the Device Label link, and then click the Serial Number link on the Network Assets tab.
- The Password Strategy-Compliance Check parameter was added on the System > System Configuration > System Settings page.

## Features released in IMC PLAT 7.3 (E0705P12)

- Support for Aruba 6300 JL658A was added.
- Support for Aruba 6100 JL677A JL678A JL679A was added.
- The website certificates are updated.
- Support for Aruba 8360 JL717A JL718A JL720A JL722A was added.

## Features released in IMC PLAT 7.3 (E0705P11)

- Support for deleting expired data was added in the performance component.
- Support for deleting expired configuration files was added in ICC.
- Support for Cisco Catalyst 9000 devices was added in ICC.

## Features released in IMC PLAT 7.3 (E0705P10)

- IMC topology show the topology of a VSX pair of devices.
- Added compatibility with HPE 2530-8-PoEP(OID:1.3.6.1.4.1.11.2.3.7.11.173) devices.

## Features released in IMC PLAT 7.3 (E0705P07)

- Added support for importing user groups.
- Added access parameter template type RESTful API.

- Added report type Interfaces Report.
- "Memory utilization (%) - top5","CPU utilization (%) - top5" and "device unreachable ratio (%) - top5" are added to the "custom view" option.
- Support for link agg and stacking of Alcatel-Lucent Enterprise and Brocade.
- SCP for Cisco Nexus devcies.
- Report Tracking support showing MAC to IP for VXLAN.
- ACL support for Aruba OS-CX.
- Vlan support for Aruba OS-CX.
- ICC support for Aruba OS-CX.
- Support for enabling allowlist for EL expressions by default.
- "Location" column added for "Device Asset Report V2" and "Device Asset Report(Concise) V2".
- Added support for SSHv2 hmac-sha2-256 and hmac-sha2-512.

## Features released in IMC PLAT 7.3 (E0705P06)

- The function of exporting users was added on the User > All Users page.
- The default for the Complexity parameter was modified to Must Contain Uppercase Letters, Lowercase Letters, Numbers, and Special Characters on the Password Strategy page.
- The Include Devices of Subviews parameter was added in the Setting dialog box for the Device State Overview widget.
- No error message is displayed when an SNMP write test fails.
- The F5 Load Balancer adapter for ICC is updated.
- When adding the Device Unreachability (%) - Top 5 widget to the home page, you can select a custom view for the widget in the Setting dialog box.
- Support for sorting the performance views by Name, Creator, and Creation Time field was added on the Resource > Performance View page.
- From this release, the system management module will receive syslog messages from all devices when no syslog filter rules exist.
- Support for HPE 2915-8G-POE devices was added.
- The max-repetitions can be configured for SNMP GETBULK requests.

## Features released in IMC PLAT 7.3 (E0705P04)

- Support for configuring a step-by-step device software deployment task was added on the Service > Deployment Guide. In the task, you can set the time points for these sequential steps: uploading the software file, setting the uploaded file as the startup file, and restarting the devices.
- Support for configuring the alarm sound settings (such as the repeated alarm sound times) for the following occasions were added on the Alarm Sound Setting: When uncovered alarms exist, when unrecovered alarms are not acknowledged.
- Support for exporting trap definitions was added on the Alarm > Trap Management > Trap Definition.
- Support for displaying all files that a trap definition MIB file depends on when the MIB file is imported was added on the Alarm > Trap Management > Trap Definition.
- Support for the Real-Time Location function in VXLAN environments was added on the Resource > Terminal Access > Real-Time Location.
- Support of SSH for putty0.7 was added.

## Features released in IMC PLAT 7.3 (E0705P02)

- Supports disabling TLS 1.0.
- Added support of the TLS 1.1 and TLS 1.2 protocol for the MS SQL server database.
  In order to configure the IMC environment to use TLS 1.2, perform the following steps after applying patch 7.3 E0705P02:
  1) Ensure your MS SQL version supports TLS 1.2 and it's patched, following https://support.microsoft.com/en-sg/help/3135244/tls-1-2-support-for-microsoft-sql-server.
  2) On all IMC and database servers, install the OLE DB patch available from https://www.microsoft.com/en-

us/download/details.aspx?id=56730.
3) Disable both TLS 1.0 and TLS 1.1 in the registry, following https://support.microsoft.com/en-us/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat.
4) Add usetls=true at the top of server/conf/qvdm.conf file.

- Support for configuring the storage path for device backup files was added on the Service > Configuration Center > Options page.
- Support for importing and exporting device configuration parameters was added to the device configuration deployment function on the Service > Configuration Center > Deploy Device Configuration page.
- Support for querying traps by severity was added on the Browse Trap page Alarm> Trap Management> Trap Definition.
- Support for exporting real-time alarms to.csv files was added on the Alarm> Alarm Browse>Real-Time Alarms page.
- The Delete All button was added on the Browse Syslog page Alarm>Syslog Management>Browse Syslog.

## Features released in IMC PLAT 7.3 (E0705)

- Supports generating an alarm when the RSM module becomes unavailable.
- Supports user group import was added on the User > User Management > Import Users page.
- Supports exporting selected history access log records was added on the Resource > Terminal Access > History Access Log page.
- Supports modifying the vendor ID of an operator matching rule was added on the advanced RADIUS server configuration page.
- Supports batch device topology diagnosis was added. You can select one or more devices on the topology, and then select Topology Diagnosis from the right-click menu to diagnose the devices in batches.
- If an SMS message contains more than 500 characters, the message content will be displayed as the first 497 characters appended with an ellipsis (¡).
- The Joined Device Groups field was added to the device details page to identify the device groups to which the device belongs.
- The Export Excel and Delete All options were added on the System > SMSC Settings > Sending Records page, allowing you to export selected or delete all SMS sending records.
- Supports assigning auto backup plans to operator groups for privilege control.
- Task scheduling parameters were added to the RESTful API-based configuration tables POST /icc/deploy/confFileTask and GET /icc/deploy/confFileTask/{taskId}.
- Supports using "${}" to represent dynamic parameters in the match pattern of a basic compliance policy rule was added.
- The Device Category and Device Model columns were added to the alarm list on the Alarm > Alarm Browse > All Alarms page.
- When configuring alarm forwarding through WeChat messages, you can query the followers of the official account to select the desired message recipients.
- The Play option was added on the Alarm Sound Setting > Upload Voice File page. You can use the option to play an uploaded voice file.
- Supports importing and exporting device severity settings for trap definitions was added on the trap definition list page.
- The index type configuration for adding a custom index was optimized.
- Supports integrating multiple AirWave systems.
- VRM supports Windows Hyper-V Server 2016 and SCVMM 2016.
- Added support of the platform for the Cisco C6807-XL devices.

## Features released in IMC PLAT 7.3 (E0703H01)

- None

## Features released in IMC PLAT 7.3 (E0703)

- The auto backup plan supports configuring mail notifications based on the backup results on the Service > Configuration Center > Auto Backup Plan > Add Auto Backup Plan page.
- The compliance check reports can be exported, and mail notifications can be configured based on the compliance

check results on the Service > Compliance Center > Check Task page.
- The repeated devices are filtered when you configure devices for the realtime alarm widget on the homepage, and the configuration page width is increased appropriately.
- The alarm contents can be customized in the mail notifications for alarms on the Alarm > Alarm Notification page.
- The physical server name can be modified on the physical server details page on the Resource > Virtual Resource Management > Virtual Neteork View page.
- In the Resource > Virtual Resource Management > Virtual Neteork View page, after the server status details icon is clicked, the server alarm information page is opened.
- VRM supports the RESTful API for querying all VMs.
- VRM supports cutting the KVM VM operations.
- On the Resource > Virtual Resource Management > Virtual Neteork View page, the VM performance data columns (including CPU, memory, and disk I/O) are added and can be customized.
- The version of putty in IMC is upgraded from 0.61 to 0.70.
- IMC runs in an OpenJDK environment from this software version.

## Features released in IMC PLAT 7.3 (E0702)

- The front panel and rear panel alignment mode can be switched for the device panel on the Resource > Device view > Detail > Open Device Panel page.
- The device panel supports the HP J8694A yl X2/CX4 10-GbE Module on the Resource > Device view > Detail > Open Device Panel page.
- The alarms can be forwarded to a third-party workflow system besides H3C ITSM on the Alarm > Alarm Settings > Alarm Notification > Add Alarm Forwarding page.
- In the Service > Configuration Center > Configuration Templates > Add Configuration Template page, the template type TCL script is added, which supports deploying device configuration through TCL scripts. The rest APIs POST /icc/deploy/confFileTask and GET /icc/deploy/confFileTask/{taskId} are synchronously modified.
- The ICC configuration templates support embedding (referencing other configuration templates through parameters) on the Service > Configuration Center > Configuration Templates page.
- The device information can be modified for the scheduled compliance check tasks on the Service > Compliance Center > Check Task page.

## Features released in IMC PLAT 7.3 (E0701)

- None

## Features released in IMC PLAT 7.3 (E0605H09)

- None

## Features released in IMC PLAT 7.3 (E0605H08)

- None

## Features released in IMC PLAT 7.3 (E0605H07)

- None

## Features released in IMC PLAT 7.3 (E0605P06)

- The history access logs can be exported.
- The **Physical Network Asset Statistics widget** is added on the homepage.
- The REST API **/perf/topNData/deviceLevelData** is added to obtain the TopN devices by CPU usage.
- The line thickness can be set for the performance widget in the dashboard.
- The original traps of devices can be stored.

Devices in the **Unmanaged** state are filtered when devices are automatically backed up.
- Two parameters are added to the configuration file qvdm.conf. One parameter is used to configure the number of background task threads. The other parameter is used to specify whether to use only the TCL script for configuration backup.
- You can specify a device group for devices automatically discovered during auto discovery.
- The **Location** and **Contact** columns are added for customizing columns for a device view.
- Maintainers can import and export devices.
- The **Reboot Device** task in batch operations can be modified and copied.
- The devices can be filtered by device view in the **Device Asset Report V2** and **Device Asset Report (Concise) V2**.
- For a compliance policy, you can use a formula to configure the relationship between rules as AND or OR. The device view can list compliant interfaces and supports exporting the interface check information. In the strategy view, compliance polices can be filtered based on the policy check results.
- Query conditions **Task Name** and **Creator** are added for deployment tasks.
- The **fault_oid_sour** field was added to the alarm view **nme_fault_v_trap** to represent the original OID information of alarms.
- The **Persisted for** column is added when are alarms are exported in CSV format. The REST API **/fault/alarm** adds a new query condition **Persisted for**.
- The devices can be filtered by custom view on the **CPU Utilization (%)-Top5** and **Memory Utilization (%)-Top5** widgets on the homepage.
- You can specify different TFTP server addresses for different devices when backing up device configurations.
- The mail sender name can be customized in the alarm mail forwarding configuration.
- Message notifications can be batch enabled and disabled for alarms.

## Features released in IMC PLAT 7.3 (E0605H05)

- The audit information for the device configuration baselines can be filtered based on the audit result.
- The batch baseline device configuration can be queried based on the time range.

## Features released in IMC PLAT 7.3 (E0605P04)

- The following columns were added to a user-defined report: serial number, hardware version, software version, and product number on the Report > Custom Reports > Add Custom Report page.
- A RESTful interface was added to modify the device additional information.
- Batch deploying VXLANs, which enables you to create a VXLAN on multiple devices at the same time on the Service > VXLAN Management > Devices page.
- Exporting backup history records on the Service > Configuration Center > Backup History Report > Detailed Information page.
- Merging of CLI scripts and identification and alert for highly risky commands during device configuration deployment on the Service > Configuration Center > Deployment Guide > Deploy Device Configuration page.
- RESTful interfaces used to search for the device configuration, obtain device backup configuration files, back up device software images, and set file transfer protocols were added. The RESTful interface for device configuration was also made open.
- Using configurations that trigger the following types of alarms as the baseline configurations: Running Configuration differs from baseline and Startup Configuration differs from baseline on the Alarm > Alarm Browse > All Alarms > Alarm Details page.
- Exporting device backup configuration files based on device name, IP address, or device model on General Search page.
- Changing the rule for a compliance policy on the Service > Compliance Center > Compliance Policy > Modify Compliance Policy page.
- Multiple levels of thresholds on the Resource > Global Index Settings page.
- Monitoring by group on the Resource > Monitoring Settings Depend On Group page.
- Configuring a platform alarm forwarding rule for APM alarm forwarding on the Alarm > Alarm Settings > Alarm Notification page.
- Changing alarm level settings on the Alarm > Alarm Settings > Alarm Level Configuration page.
- Policy-based alarm level escalation on the Alarm > Alarm Settings > Alarm Level Configuration page.

Configuring alarm distribution processors by group on the Alarm > Alarms Browse> All Alarms page.
- An option was added to the widget to display the duration or alarm time on the Home Widget.
- Filtering and displaying the syslog list by view ID on the Alarm >Syslog Management > Browse Syslog page.
- Advanced syslog search based on a combination of descriptions on the Alarm >Syslog Management > Browse Syslog page.
- The Performance Index Config tab was moved to the Performance Option menu on the Resource > Performance Option page.
- The RESTful interface for alarm registration was modified. The UUID parameter is now optional.
- The Batch Set button is added for specifying different display indexes for different devices on the Performance Option > Display Index page on the Resource > Performance Option > Display Index page.
- The software products that already exist in the software library will not be downloaded again from devices.
- During auto discovery, you can specify a device group for auto-discovered devices on the Resource > Auto Discovery page.
- You can filter the check results of check tasks by the check result on the Service > Compliance Center > Task History > Compliance Policy Check Results page.
- You can specify an operator group with the access right when creating a deployment task on the Service > Configuration Center > Deployment Guide > Deploy Device Configuration page.
- The legend cannot be displayed on the CPU Utilization widget.

## Features released in IMC PLAT 7.3 (E0605H02)

- None

## Features released in IMC PLAT 7.3 (E0605)

- The embedded database was upgraded to SQL Server 2016 Express.
- Support for QoS hardware statistic index (Queue Datagram Hardware Statistics).
- You can start or stop processes on the **System > System Configuration > Server page.**

## Features released in IMC PLAT 7.3 (E0506P09)

- Supports selecting interfaces by port group.
- Supports specifying the port group when an alarm notification rule is added on the Alarm > Alarm Settings > Alarm Notification page.
- Supports viewing the interface status and the status update time in the stack topology on the Resource > Network Topology page.
- Supports synchronously modifying the database administrator password in DBman after the database administrator password is modified on Intelligent Deployment Monitoring Agent.
- Supports filtering devices by model when iCC batch makes device software as the baseline on the Service > Configuration Center > Software Library > Make Baseline page .
- Supports saving the selected device conditions on the realtime alarm widget.
- After you open the VLAN view panel and then click the link for querying port information on the Service > VLAN Management > VLAN Topology page, you can query port information by the combination of VLAN ID, interface type, and device IP.
- Supports disabling the function of using NetBIOS to detect host names on the System > System Configuration > System Settings page.
- Supports customizing SNMP ports on the System > System Configuration > System Settings page.
- Supports customizing Telnet ports on the System > System Configuration > System Settings page.
- Supports monitoring CPU and memory for ZTE devices on the Resource > Performance Management > Monitoring Settings page.
- Supports upgrading patches for Comware devices on the Service > Configuration Center > Deployment Guide > Deploy Device Software page.
- Supports selecting port groups for filtering rules of the up/down trap group on the Alarm > Trap Management > Filtering Trap page.
- Adds the Syslog parameter as the criterion for checking whether alarms escalated from Syslogs are repeated on the

Alarm > Trap Management > Trap To Alarm page.
- Whether interface up/down events generate intermittent traps conforms to the interface up/down trap configuration on the Alarm > Trap Management > Filtering Trap > Intermittent Trap Analyze page.
- Adjusts the automatic alarm recovery time to 5:30 am.

## Features released in IMC PLAT 7.3 (E0506P07)

- Automatically repairing orphaned users of databases.
- Allowing operators to select to enter the automatic discovery page or the getting started page upon the first login.
- Making the files backed up in one backup task as the baseline on the Service > Configuration Center > Backup History Report page.
- Support of VRM for checking the VRM version and agent version consistency.
- Interface performance monitoring for Brocade switches.
- Specifying the levels of alarms to be reported in hierarchical NMS on the Alarm > Alarm Settings > Hierarchical System Alarming page.
- Monitoring and alarming memory leaks for devices.
- Support for trap definitions of Aruba wireless devices.
- Configuring aggregation times for repeated alarms on the Alarm > Trap Management > Filtering Trap > Duplicate Trap Filter Configuration page.
- Displaying stack physical interface status in the stack topology.
- Trap-based quick synchronization for stack devices.
- DHCP-plug service used to manage DHCP-plugs.
- Software and patch upgrade for H3C Comware 7 devices.
- Distributed database backup and recovery for APM.
- Sorting the list by using the maximum value, minimum value, or average value by clicking the corresponding column heading on the Resource > Performance View > Monitoring Data Statistics page.
- Support for H3C OneStore management.
- After you click the link for one ACL resource and then add or modify one rule set on the Service > ACL Management > ACL Resource page, you can define ACL rules with user-defined rule numbers, and move a rule to the specified position when sorting rules.
- Support Arista devices in VLAN and ACL.

## Features released in IMC PLAT 7.3 (E0506P03)

- The speed of opening the device panel improved.
- The DBMan automatic backup recovery function can detect the remaining disk space and trigger an alarm.
- Added support for batch configuration of device type in device view on the Resource > Batch Operation > Configure Device Type page.
- Added support for querying devices by system description on the Advanced Query page.
- Added batch configuration of NETCONF parameters on the Resource > Batch Operation > Netconf Settings page.
- Multiple SNMP parameter templates can be specified for auto discovery in advanced mode.
- Added support for NTP clock monitoring and alarm triggering on H3C network devices.
- Added support for the port display and performance monitoring on Brocade switches.
- Added support for the Inspect function on the Resource > Network Topology > Data Center Topology > System Settings page.
- Added support for inputting the length on the Resource > Network Topology > Data Center Topology page.
- Added support for displaying the history data for the temperature and humidity data on the Resource > Network Topology > Data Center Topology page.
- Added support for adjusting the order of views on the dashboard on the Dashboard page.
- Added the environment and power widget on the Dashboard page.
- Added the environment and power widget on the Homepage.
- Added support for generating a connection between clouds in a topology.
- Added support for custom icons on the topology maps.
- Added support for custom icons on the topology subviews.
- Added support of the topology for the circular layout.

The topology cloud supports modifying the associated topology.
- The topology supports setting permissions for the hand icon function.
- On an opened VLAN view panel on the topology, the VLAN list is displayed in ascending order of VLAN ID by default.
- Added the configuration template contents of the configuration template library to the general search.
- The report component automatically detects and repairs isolated user problems.
- Sending periodical reports in mails supports retries after a failure.
- Added the HTTPS Access Settings option on the System > System Configuration > HTTPS Access Settings page.
- When you delete a matching rule in the advanced LDAP server configuration of the authentication server configuration, the operator created by the matching rule is deleted synchronously on the System > Operator Management > Authentication Server page.
- Added the Lock Duration for Three Continuous Login Failures option to system parameters.
- Added the Enable Web Proxy option to opening Web-based NMS configuration in system parameters.
- Added the General Configuration Access option to Other SMS Sender on the System > System Configuration > SMSC Settings page.
- Added the REST interfaces related to the deployment monitoring agent.
- Added the REST interface for querying the syslog parsing template library.
- Added the REST interface for querying VLAN devices.
- Added the REST interface for globally querying the members of a VLAN according to the VLAN ID.
- Added the backup configuration file size check. Backup fails if the file size is less than 200 bytes.
- If SSHv2 failed to access some Huawei devices, you can add the device IPs to the server\conf\ssh_v1_devices.cfg file, and use SSHv1 to access the devices.
- The subgroup information is added to the returned information from the REST interface for querying user groups.
- Additional user information is added to the returned information from the REST interface for querying users.
- Support for the IP Routing Table feature was added to the Resource Management module. The feature allows you to view and query the routing tables of managed devices on the Resource > Resource Management > Device Routes page.
- Predefined trap definitions for Aruba devices were added to the Trap Management module.
- The Maintenance Experience field was added on trap definition management pages in the Trap Management module. You can view and edit maintenance experiences for a trap definition.
- The Device Panel is available for ProCurve 2620 devices and HPE 1810 devices.

## Features released in IMC PLAT 7.3 (E0506)

- IMC can be installed in SQL Server with the model database smaller than 256M.

## Features released in IMC PLAT 7.3 (E0504P04)

- Parameters support * fuzzy matching when you set device severity levels for trap definitions on the **Alarm > Trap Management > Trap Definition** page.
- Improves the Real-Time Location efficiency on the **Resource > Terminal Access > Real-Time Location** page.
- Adds the HTTPS access configuration feature, which allows users to upload their own HTTPS certificate files.
- Supports setting the auto layout offset value for nodes in the topology on the **Resource > Network Topology** page.
- Adds the interface tx/rx rate index on the **Resource > Network Topology > Custom Topology > My Network View > Traffic Topology** page. Adds the function that the traffic topology configuration page is not replaced if you click another button after you click the traffic topology button.
- The **Resource > Performance Management > Performance View** page supports baseline threshold display.
- The **Resource > Performance Management > Global Index Settings** page supports configuring different thresholds based on interface bandwidths.
- The **Resource > Network Topology** page supports link display for Avaya devices.
- The **System > System Settings** page supports setting the CPU, memory, and disk usage thresholds of the IMC server.
- The **Resource > Network Topology** page supports topology baseline comparison.
- The dashboard view supports sorting.
- The rack topology of the 3D room supports setting descriptions of virtual device objects.
- The operator group permission configuration supports setting dashboard permissions.
- The **Resource > Network Topology** page supports changing icons of the topology cloud.

The **Alarm > Alarm Browse > All Alarms** page supports displaying traffic values of traffic alarms in the performance monitoring in the optimum measurement.
- The **Alarm > Alarm Browse > All Alarms** page supports displaying the alarm sources of blinking alarms.
- Upgrading the OpenSSL version to 1.0.2k.
- Support for specifying devices to be checked by custom views when adding compliance check tasks in iCC.
- Support for importing parameters when deploying configuration to a device in iCC.
- Support for adding match rules based on Group CN on the **Authentication Server > LDAP Server > Advanced Settings** page.

## Features released in IMC PLAT 7.3 (E0504P02)

- Support for receiving KVM events.
- RESTful interfaces used for querying the lower-level NMS list.
- NETCONF supports UNIS devices.
- RESTful interface: Time-Division Alarm Statistics.
- APM alarms contain the alarm source column that displays the applications and device IP addresses.
- The alarm sources of APM alarms can be redirected to the APM application pages.
- IP column on the All Alarms page.
- Support for accessing the lower-level NMS alarm view through the upper-level NMS by using the URL method.
- Selecting devices for realtime alarms on the IMC home page.
- The alarm statistics feature supports statistics by trap group.
- Periodic test feature for the GSM modem.
- CDMA type for the GSM Modem sending method in the SMSC settings.
- The trap filtering parameter settings support regular expressions.
- RESTful interface: Query Root Alarm Interface.
- Alarm query by alarm time range on the All Alarms page
- Alarm acknowledgement on the Real-time Alarms page.
- AC traffic monitoring in the VXLAN module.
- The power environment equipments in the 3D room support the i9000 socket data source, including the entrance guard devices, information used for unlocking the control door of the entrance guard system, and the door unlocking operations.
- The map component in the big-screen area of the dashboard supports level-2 drilldown feature.
- The dashboard supports displaying the overall topology.
- The iCC module supports Arista devices.
- After stack member devices are automatically deployed and are stacked, IMC automatically deletes the redundant stack member devices from the system.
- The syslog-to-alarm escalation feature supports the interface alias.
- The trap-to-alarm escalation feature provides the Reduced Scenario mode, which can reduce the number of alarms.
- The trap filtering feature supports matching by regular expression.
- The stack topology supports the Cisco FEX feature.
- Supports configuring auto forwarding recovered alarms to users on the **System > System Configuration > System Settings** page.

## Features released in IMC PLAT 7.3 (E0504)

- None

## Features released in IMC PLAT 7.3 (E0503)

- Updates the star theme.
- Changes the page frame to support partial refresh.
- Supports navigating to the AC and AP details pages in resource view.
- Supports displaying AirWave APs in the converged topology.
- IMC can be deployed to VMs created on VMware ESXi Server 6.0.
- The **Resource > Device View > Device Details** page supports displaying the VDC feature of Cisco devices.

- The **Alarm > Alarm Browse > All Alarms** page supports merging duplicate alarms into one alarm.
- The **Alarm > Alarm Browse > All Alarms** page supports viewing child alarms from root alarms.
- The REST API supports querying the IPv6 address of VLAN interfaces.
- The REST API supports obtaining device routing information.
- The **Service > Configuration Center** page supports configuration backup and recovery for Brocade devices.
- The **Service > Configuration Center** page supports configuration backup and recovery for ZTE devices.
- The **Service > Configuration Center** page supports software upgrade for Ruijie 6200 and 2900 series devices.
- The **System > System Configuration > Data Collection** page supports collecting Layer 2 topology memory information.
- The **Resource > Network Topology** page supports enabling LLDP for ZTE devices so that IMC can draw the links to the devices.
- The **Resource > Device View > Device Details > Interface List** page supports interface IP addresses in the VRF of ZTE devices.
- The **Resource > Performance Management > Monitoring Settings** page supports automatically using the device threshold as the temperature threshold for H3C devices.
- The **Alarm > Syslog Management > Syslog Template** page supports specifying regular expression for upgrading the alarm rules.
- The **Alarm > Syslog Management > Syslog to Alarm** page supports modifying the template content for upgrading the alarm rules.
- The HAC license expiration time is consistent with IMC.
- The **System > System Configuration > System Settings** page supports customizing alarm message format.
- The **Alarm > Alarm Browse > All Alarms** page displays the alarm source for APM alarms.
- In iMC/server/conf/qvdm.conf, you can customize for how long to save the performance monitoring data.
- The **Resource > Network Topology** page supports enabling LLDP for the ESXi server so that IMC can draw the links between the switches and the ESXi server.
- When the primary and secondary IMC servers use different versions, DBMan periodically sends alarms.
- The **System > System Configuration > Performance Index Configuration** page supports dynamic thresholds.
- The DBA privileges are not assigned to IMC users using the Oracle database.
- The **Alarm > Alarm Browse > All Alarms** page does not generate grouped alarms, unmanaged device alarms, and unknown traps.
- On the **System > System Configuration > System Settings** page, disabling the DismanPing function deletes NQA configuration from the device.
- The **Alarm > Trap Management > Trap Definition** page displays trap definition in SNMPv2 format and displays the received original trap OID.
- The export of IMC NMS Trap conforms to the SNMP v2c MIB standard.
- The **System > Resource Management > Access Parameter Template** page supports duplicate user names in the SNMPv3 template.
- Version update for OpenSSL to 1.0.2h.
- Supports exporting data to an Excel sheet in device view.
- Adds batch undeployment in Intelligent Deployment Monitoring Agent.
- Adds database connection usage information in Intelligent Deployment Monitoring Agent.
- Adds the import/export device appended information function.
- Adds the operator group-related REST API.
- Supports selecting tablespace in Oracle environment.
- Adds performance data to the virtualized topology node tooltip for VRM.
- Adds VM tooltip to the 3D equipment room topology for VRM.
- Adds the device reboot REST API for iCC.
- Adds the REST API for saving the running configuration to the startup configuration for iCC.
- The J# column is added to the Device Asset report (Concise) report, and an entry for inputting J# is provided.
- A report can be sent through email to multiple email addresses. The function of testing whether these destination email addresses are valid is added.
- Custom View Data Summary Report, more advanced device choice on which to report on.
- Supports OneView 3.0 integration.
- Resource management can recognize Arista devices.

## Features released in IMC PLAT 7.2 (E0403P10)

- The Instance column was added to the Table page accessed by using the Table View mode in the MIB management tool.
- The Alarm > Alarm Settings > Alarm Notification page supports auto sending of recovery alarms.
- On the Alarm > Trap Management page, the Oracle or SQLServer version supports traps with the trap OID not exceeding 500 characters, and the MySQL version supports traps with the trap OID not exceeding 250 characters.
- VRM supports ESX6.0.

## Features released in IMC PLAT 7.2 (E0403L09)

- Adds support for the HPE Aruba 2930F VSF series on the Resource > Network Topology > Stack Topology page.
- Supports configuring the device synchronization time on the System > Automatic Device Sync Time page.
- Supports Cisco devices whose banners contain the pound signs (#) on the Service > Configuration Center page.
- Supports configuring permitted VLANs for trunk ports of a device that has aggregate interfaces on the Resource > Network Topology > Device > Add to Current VLAN page.
- Supports Cisco Nexus switches on the Service > Configuration Center page.
- Supports displaying interface aliases in performance alarms on the Alarm > Alarm Browse > All Alarms page.
- Supports viewing the CPU and memory recovery alarms of the IMC server on the Alarm > Alarm Browse > All Alarms page.
- Supports configuring whether to escalate alarms for devices with the maintenance tag on the System > System Configuration > System Settings page.
- Supports setting the lifetime for the collected original performance data in the iMC/server/conf/qvdm.conf file.
- Supports configuring whether to send recovery alarms for alarm notifications and forwarding in the iMC/server/conf/qvdm.conf file.
- H3C devices support configuring MACsec links.
- More detailed logs are needed for importing traps through MIB files. For example, the total number of MIB files processed and the total number of MIB files parsed successfully.
- The IMC topology supports displaying and managing server clusters.
- The IMC platform supports customizing the function framework in the UCD by functional point.
- The Real-Time Location page supports adding tags to devices.
- The 3D topology supports selecting the number of switches and the environment & power facility type when you configure environment & power facilities through a right-click.
- The data center topology map supports CAD files.
- Adds the rack height (U) field to the .csv file for the automatical building function of the 3D topology.
- Adds the memory monitoring index for the single device monitor in the IMC dashboard.
- The IMC dashboard supports automatically fitting the custom topology to the screen size.
- The network topology supports setting the font size and color for device labels (the settings take effect only on the current view).
- Adds the loop legend description to the topology.
- The topology link management function supports exporting links to an excel file.
- The elements on the dashboard need the corresponding labels and the object names must be displayed on the labels.

## Features released in IMC PLAT 7.2 (E0403P06)

- None

## Features released in IMC PLAT 7.2 (E0403P04)

- The **Resource > Network Topology** page supports the tree layout.
- The **Resource > Network Topology > Custom View** page provides multiple levels of custom views. This feature implements hierarchical display of custom views in the topology. The hierarchy is consistent with Resource > Custom View and the left navigation tree of the network topology. From this release, all views under the custom view will be displayed hierarchically in the topology according the existing hierarchical relationship.
- The **Resource > Network Topology** page supports the stack topology of HPE Aruba 5400R series devices.
- The **Resource > Network Topology > Data Center** page supports monitoring Cointech hygrothermographs.

- The **Resource > Network Topology > Data Center** page supports recording user operations performed on racks (for example, clicks and browses) and the pauses in the 3D room.
- The 3D room provides RESTful APIs for obtaining rack information and the rack and room locations for a device.
- RESTful APIs for obtaining device MIB tables.
- The **Device Detail > Interface List** page supports displaying an interface alias that contains more than 64 characters.
- The **Service > Network Devices > Device Details** page supports adding VXLANs in the EVPN mode.
- The **Service > VXLANs Traffic Information** page provides the VXLAN monitoring feature.
- The **Service > Network Devices > Device Details** page supports configuring ACs.
- The **Service > Network Devices > Device Details** page supports adding L3VNI interfaces in distributed networks.
- The **Service > Network Devices > Device Details** page supports binding VPN instances to DHCP relay IP addresses in distributed networks.
- The **Service > Network Devices > Device Details** page supports adding VSI interface MAC addresses and secondary IP addresses.

## Features released in IMC PLAT 7.2 (E0403P03)

- The Dashboard page provides a toolbar on the topology.
- The Dashboard page provides automatic switch between views.
- The Dashboard page supports component-based filtering for widgets to be added.
- The **Resource > Network Topology** page provides subview alignment in the right-click menu of the topology.
- The **Resource > Network Topology** page provides the Add Monitor option in the right-click menu of topology links in performance management.
- The **Resource > Network Topology** page provides the vertical distance configuration between the device icon and the device label.
- The **Resource > Network Topology** page displays the status of connections in link aggregation by expanding the stack topology.
- The **Alarm > Alarm Settings > Alarm Notification** page supports the asterisk (*) wildcard character in parameter settings.
- The **System > Operator Management > Authentication Server** page supports RADIUS server and TACACS server configuration.
- The **System > Operator Management > Authentication Server** page allows you to define the accessible user groups, device groups, and custom views by OU in advanced settings.
- The **Service > Configuration Center** page provides software update for Cisco 800, 2651, 2800 series devices.
- The **Service > Configuration Center** page provides configuration backup and restoration and software update for Aruba 3810 series, 7000 series, and IAP series wireless devices.
- Support for integration with DCN, identifying the VSC and VRS roles, and displaying connection relationships between the roles in the topology.
- VRM supports Windows Hyper-V Server 2012 R2 and SCVMM 2012 R2.
- VRM supports obtaining storage information from VMware hosts.

## Features released in IMC PLAT 7.2 (E0403L02)

- Open data sources of iCC for reports, including deployment tasks, backup history reports, device configuration backup, and device software update.
- Backup and restoration of i-Ware configuration on security products.
- Obtaining information about the VMware NTP server, network card speed, and duplex mode in VRM.
- Configuring whether to assign all trunk and hybrid ports to a device VLAN when you add it through the RESTful interface.
- SCOM supports the HTTPS protocol.
- Adding custom templates for performance indexes.
- Displaying custom TopN indexes in the device view, interface view, custom view, IP view, and query result page.
- DBman can back up configuration files that include realtime performance monitoring and traffic topology settings.
- The Lower-Level NMS Performance View widget was added to Dashboard to provide monitoring data of the lower-level NMS.
- The procedure of modifying NMS parameters for devices that failed access parameter verification was added to batch

operations.
- The Download Logs feature in Log Configuration supports automatically downloading the software version information.
- Netconf log management in Log Configuration.
- Basic query and advanced query on the operator management page.
- Trap group management was added to the trap management page for trap filtering.
- The Alarm Notification feature supports displaying user information in the destination mail address.
- Using a public IP address as the lower-level NMS address in Hierarchical IMC Alarming settings.
- Using the custom view to filter alarms in Dashboard.
- The Alarm Notification feature supports adding relationships among alarm parameters for alarm configuration.
- Configuring the number of hierarchical alarms to be displayed in Hierarchical IMC Alarming settings.
- Backing up FW, IPS, ACG, and LB data of the H3C i-Ware platform.
- The ACL, VLAN, and iCC features in the Service module support Cisco Nexus series switches.

## Features released in IMC PLAT 7.2 (E0403L01)

- RESTful API for querying global VLANs.
- Optimized menus in the More and Operation columns in the device list.
- The Deploy Software option was added to the right-click menu of devices on the topology.
- The fabric topology does not display loop links.
- Displaying PE-PE links of IRF fabric devices.
- When unrecovered alarms are not acknowledged option was added to the Alarm Sound Settings page.
- V2 report of unused interfaces.
- Quick service process view.
- Viewers were assigned the privilege of modifying the collection interval on the realtime performance monitoring page.
- On the Resource >> Network Topology page, the fabric topology does not display the loop links.
- Modifying ports in the DBMan configuration file.
- The Resource >> Network Topology page displays PE-PE links of IRF fabric devices.
- DBMan allows you to modify ports in the dbman.conf file in the /dbman/etc directory of the IMC installation path.

## Features released in IMC PLAT 7.2 (E0403)

- Supports OneView integration.
- Supports VXLAN.
- Custom views support upper-level views by using the API POST plat/res/view/custom
- Supports the following new operating system: RHEL 7.x.
- Supports Oracle 12c Release 1
- Adding the Perspective QSP template.
- Adding system integration with AirWave
- Integration with Aruba ClearPass and Aruba AirWave trap definitions in trap management of the alarm module.
- Reporting alarms to upper-level IMC administrators for processing when the grace days for alarm acknowledgement expires on the Alarm Notification page of the alarm module.
- The tools directory provides iMC-MIB-Download_Windows.zip or iMC-MIB-Download_Linux.zip to import IMC trap definitions to MIB files
- Set the autocfg_exec_mode parameter to 1 in the file /server/conf/qvdm.conf of the IMC installation path, and then restart the imciccdm program to support serial execution of auto deployment plans.
- Backup function for HPE PROCURE 2520 device configurations on the Service > Configuration Center page.
- Using the device model as the display name in the topology.
- Custom report feature.
- Custom view eAPI and upper-level views.
- Starting and stopping a single process by using command lines in Linux.
- Access to interface lists of interface views by clicking icons on the Interface View TopN widget on the home page.
- Displays route relationships among devices on a route topology based on device routing tables.
- In Intelligent Policy Center, Action Management supports the Restart VM operation.
- On the device query page, the advanced query provides the Device Alarms field.

On the all alarms page, the advanced query provides the logical combination of NO.
- Supports custom interfaces for third-party mails servers.
- The performance view provides the Modify the Upper-Level Folder feature.
- The configuration template library supports access control by operator group.
- Configuration template deployment supports exporting parameters from CSV files.
- The VRM component supports detecting unmanaged hosts under a managed vManager.
- Device and interface (link) maintenance tagging.
- Displaying or hiding interface aliases in interface-related alarms.
- Sending alarm notification in long SMS messages.
- A Test button is provided to test the SMS modem.
- Scenario-based trap-to-alarm rule configuration.
- Displaying the STP root bridge in the MSTP topology.
- Topology diagnosis.
- Managing Extreme x460 series devices by using Resource Management.
- The default setting for DismanPing is FALSE in the global configuration.
- Configuring a rule to automatically add interfaces of new devices to an interface view.
- Email alarm notifications provide a link for users to confirm the alarms.
- A REST API for obtaining trap definitions is provided.

**[ Table of Contents ]**

---

# Problems Fixed in this Release

IMC PLAT 7.3 (E0710) fixes the following problems, including all bugs fixed in IMC PLAT 7.2 (E0403) and later versions.

## Resolved Problems in IMC PLAT 7.3 (E0710)

1. CMS case 0929123: Added tips information to performance threshold configuration.
2. CMS case 0928785: Modified the history record export format to xlsx.
3. CMS case 0929106: IMC cannot open deployment task after IMC upgrade.
4. CMS case 0929132: Gray out the upgrade strategy Back up the running software to local server for Aruba OS-CX.
5. CMS case 0928970: iMC E0706P11 syslog facility sporadically stops working.
6. CMS case 0929115: Upgrade via TFTP fails for 2530 device because password error cannot be verified in log.
7. CMS case 0928909: Supports the parsing and display of applicable devices for the software name ArubaOS-CX_xxxx-yyyy_version.
8. CMS case 0928924: iMC Oracle DB deadlock detected.
9. CMS case 0928892: REST API script fails on E0708, and works just fine on E0706P11.
10. CMS case 0928941: iMC software deployment fails for Aruba 2930M using SCP.
11. CMS case 0929075: E0708P02-device configuration backup for 2920 stacked switches not supported after upgrade to E0708P02.
12. CMS case 0928950: iMC-cx upgrade fails with a server busy error.
13. CMS case 0928943: E0708 software deployment failed for old Procurve switches 2500 (2900) series if SFTP is used.
14. CMS case 0929131: Aruba OS-CX upgrade failed to transfer file but iMC claimed it successful.
15. CMS case 0929133: SFTP server plaintext password contains text vulnerability.
16. CMS case 0928699: Software Deployment takes too long.
17. CMS case 0929000: Unable to use CLI Templates to perform any kind of command that needs a "y" as response.
18. CMS case 0929130: CX error snmp write error during upgrade in 708P03.

## Resolved Problems in IMC PLAT 7.3 (E0708P03)

1. CMS case 0928761: The topology report (including aggregate subinterfaces) V2 gives wrong results.
2. CMS case 0928978: Operator login (LDAP) doesn't work after the upgrade to E0708P02.
3. CMS case 0928759: CWE-693: Vulnerability - The HTTP security header is not detected.

4. CMS case 0928870: In version E0706P11, new devices cannot be added to IMC.
5. CMS case 0928847: Manual backup of Huawei devices fails.
6. CMS case 0928749: Auto backup plans do not work.
7. CMS case 0928908: Cisco devices show incorrect temperatures.
8. CMS case 0928932: Cisco 2960 and 1000 switches fail software upgrade via IMC with the error that the device software cannot be deleted.
9. CMS case 0928938: In IMC PLAT E0708, CX 6000 devices failed to copy the current primary images to the secondary partition.
10. CMS case 0928826: IMC is expected to allow selecting instances in global indexes.
11. Fixed the log4j security vulnerability.
12. SNMP errors are not removed during Aruba OS-CX device upgrade.
13. ArubaOS-CX software upgrade initializes tasks abnormally.
14. If you click to add a performance instance profile in the performance instance profile widget on the homepage, the page is navigated incorrectly.
15. If you select the outbound direction when you deploy an ACL for global packet filtering, the ACL takes effect in the inbound direction actually.

## Resolved Problems in IMC PLAT 7.3 (E0708P02)

1. If the newly added subview has not been saved in disabled mode, the device location in the subview is incorrect.
2. CMS case 0928775: CVE-2022-42889 : Apache Commons Text Vulnerability.
3. CMS case 0928762 : Cisco router compliance check failed.
4. CMS case 0928591: After applying VLAN patch to add VLAN to port group, VLAN assignment to port on an Aruba CX 6100 is broken.
5. CMS case 0928770: Aruba CX VLAN information disappears when VLAN name is changed.
6. CMS case 0928806: Custom topology doesn't show saved state.
7. CMS case 0928808: Issues with trap definition: 1.3.6.1.4.1.11.2.14.12.4.0.1
8. CMS case 0928826: IMC is required to allow selecting instance in global index for Aruba CX temperature.
9. CMS case 0928429: Username and password for SSH session in clear text in Task Mgr.
10. CMS case 0928522: Unable to back up switch cisco Nexus9000 C92160YC-X.
11. CMS case 0928655: Software version of VSF stack switches not displayed in the device view.
12. CVE-2022-42889 - Apache Commons Text Vulnerability.

## Resolved Problems in IMC PLAT 7.3 (E0708)

1. CMS case 0928240: The advanced query function is unavailable.
2. CMS case 0928367: The live update function is unavailable.
3. CMS case 0928134: The RESTful API test succeeds even if the password is incorrect.
4. CMS case 0928417: Version update for log4j.
5. CMS case 0928396: Added support for exporting version software from Aruba OS-CX to IMC.
6. CMS case 0928190: After Aruba device software import, the compatible device models cannot be automatically identified.
7. CMS case 0928472: In the device and interface configuration guide, after you select the Aruba device, no operation options are available for selection.
8. CMS case 0928134: The VLAN process generates dump files.
9. CMS case 0928197: An Aruba OS-CX update issue exists. Upon version file upload, the primary version is not changed.
10. CMS case 0928184: Auto backup never ends and configuration link on device page does not work.
11. CMS case 0928157: An error occurs in the Procurve Stack Script during deployment of new device software.
12. CMS case 0928375: CX upgrade fails on Linux because the SFTP server is not running.
13. CMS case 0928231: The CIST region is displayed in gray.
14. CMS case 0928327: IMC E0706P06 upgrade via SFTP fails on the HPE 5130 switch.
15. CMS case 0928424: After upgrade to PLATE0706P11, the interface list configured in the alarm filtering rules cannot be displayed.
16. CMS case 0928099: Backup is displayed as succeeded but no device has actually been backed up.

17. CMS case 0928384: Unable to change the VLAN for interfaces on InstantOn 1930.
18. CMS case 0928100: Failed to import the ADP configuration template to a non-default folder.
19. CMS case 0928109: Backup failure for the ADP task does not affect incorporating devices upon coming online.
20. CMS case 0928575: snregen.bat is not working.
21. CMS case 0928518: E0706p11 after IMC upgarde can not backup switches config.
22. CMS case 0928563: IMC 5510 and 5530 software upgrade fails after upgrade to E0706P11.
23. CMS case 0928485: IMC not querying MIB tables for terminal location and user tracking report.
24. CMS case 0928316: Aruba device software upgrade fails.
25. CMS case 0928464: Configuration backup fails for the HP 2610 and HP 5401 devices.
26. CMS case 0928404: Upon receiving a device polling message, the ACL component polls device ACL information. As a result, a lot of login logs are generated on the devices.
27. CMS case 0928591: VLAN assignment to port on a Aruba CX is failed.
28. CMS case 0928734: Cannot import cx software, max file size exceeded.
29. CMS case 0928171: Repeated alerts on monitored memory instances.
30. CMS case 0928619: IMC 7.3 E0706p11 Unable to backup switch cisco catalyst 9000.
31. CMS case 0927943: duplicate IP address alarm storm for loopback 127.0.0.1.
32. CMS case 0928522: e0706p11 Unable to backup switch cisco Nexus9000 C92160YC-X chassis.

## Resolved Problems in IMC PLAT 7.3 (E0706P11)

1. CMS case 0927788: IMC ACL is unable to read EIGRP(88) rules.
2. CMS case 0928038: A message is displayed that "device does not exist" when you specify the file transfer mode for a device.
3. CMS case 0927856: No English help file is available on the authentication server configuration page.
4. CMS case 0927938: The IP address allocation menu is not displayed.
5. CMS case 0928037: The version contains the log4j1.2.17.jar file.
6. CMS case 0927940: With a proxy used, the liveupdate function is used to report Java error.
7. CMS case 0928023: Failed to save the topology because the Layer 3 device location information is not saved.
8. CMS case 0927977: Optimized the time consumption for loading important device widgets on the homepage. To set the number of important devices, open \client\conf\commonCfg.properties in the iMC installation directory, and edit the value of maxImportantDevNumber.
9. CMS case 0927204: In the imc_config.tbl_universal_job_dev_step table, history data are not periodically deleted. The table contains large amount of data, resulting in slow startup of the job process. Change the data retention period to 180 days.
10. CMS case 0927309: Backup script meaningful error required. If both the startup and running configuration backup fail, no reason is displayed for the running configuration backup failure.
11. CMS case 0927750: E0706P06 version script error that results in Aruba 6200/6300 upgrade failure.
12. CMS case 0927797: IMC 0706 DBMan cannot restore config_db.
13. CMS 928086/927788 IMC ACL is not reading some lines from Cisco device.
14. CMS case 0927936: Since upgrade to version E0705 customer has causes issues on topology issues, Aruba OS-CX aggregate links are not displayed.
15. CMS case 0928109: After the ADP task is complete, the file transfer mode is set to SFTP in ICC option for the incorporated device.
16. CMS case 0927943: IP address conflict detection must be disabled by default. You can enable the feature as needed.
17. Duplicate archive for device configuration backup files. After version upgrade, the archive feature is disabled by default. Due to original errors, large numbers of duplicate backup files exist and require manual deletion. To delete the files, access the IMCROOT/server/data/cfgbak directory, and delete the files and folders other than those with the *.cfg suffix.
18. CMS case 0928131: After importing the Aruba os-cx device software, device models cannot be automatically recognized. You need to manually select compatible device models.
19. CMS case 0928181: After the ADP task is complete, a message is displayed that "fail to send message to other process" in the result.
20. CMS case 0928018/0927998: After version upgrade to E0706H07, performance optimization related with custom rules for the alarm component results in alarm process startup failure.
21. CMS case 0928200: The VLAN management tab is not available for 6200F Aruba OS CX.

## Resolved Problems in IMC PLAT 7.3 (E0706H08)

1. CVE-2021-44832 - Apache Log4j2 is vulnerable to a remote code execution (RCE) attack via JDBC Appender when an attacker controls configuration.
2. Sub-components such as iMC-Portal, iMC-UAM-BYOD, and iMC-UAM-SSV cannot be deployed.

## Resolved Problems in IMC PLAT 7.3 (E0706H07)

1. CVE-2021-45105 - Apache Log4j2 does not always protect from infinite recursion in lookup evaluation.
2. CVE-2021-45046 - Apache Log4j2 Thread Context Lookup Pattern vulnerable to remote code execution in certain non-default configurations.
3. CVE-2021-44228 - Log4j's JNDI support has not restricted what names could be resolved. Some protocols are unsafe or can allow remote code execution.

## Resolved Problems in IMC PLAT 7.3 (E0706P06)

1. CMS case 927569:When the state of a device in a subview on a topology changes, the location of the subview changes.
2. CMS case 0927705:If you select LDAP Server Requires Secure Connection (SSL) in the LDAP server area on the authentication server configuration page, an operator fails the LDAP authentication.
3. CMS case 0727341:Euplat/seplat does not support TLS1.2.
4. CMS case 0927449:When ArubaOS-CX devices are upgraded, the device space is not checked, and the version parsing function is supported.
5. CMS case 0927132:After a client is migrated to IMC, the advanced rules are out of order and the compliance check tasks are slow.
6. CMS case 0927232:F5 device backup times out.
7. CMS case 0927344:The Aruba interface startup time is incorrect.
8. CMS case 0927346/0927747:Duplicate monitored instances are generated in performance monitoring. To resolve this issue, add the **perf_delete_duplicate_instance=true** line to the **qvdm.conf** file and restart the **imcperfdm** process.
9. CMS case 0927561/0927688:Scheduled auto backup tasks might not be executed. To resolve this issue, add the **reset_frequency = 1** line to the **qvdm.conf** configuration file.
10. CMS case 0927661:IMC backup core dumps every few minutes.
11. CMS case 0927699:When commands are issued to a Cisco device through the RESTful API, no echo is returned.
12. CMS case 0927753:Database errors occur in iCC configuration backup and no records exist in history backup report.
13. CMS case 0927280:DBMAN backup failed because the DB file size computed by DBMAN is incorrect.

## Resolved Problems in IMC PLAT 7.3 (E0706)

1. Multiple EAD component reports cannot be opened after the IMC PLAT is upgraded to version E0705P10.
2. CMS case 0926638:Advanced rules of a compliance policy were detected out of order on the Service > Compliance Center > Add Compliance Policy page.
3. CMS case 0926888:The memory leaks when a large number of syslog messages are imported.
4. CMS case 0926918:ICC support for backing up Palo Alto device configurations was added.
5. CMS case 0927026:Device backup archive files are zipped repeatedly.
6. CMS case 0926567:IMC fails to obtain software versions for F5 Load-balancers.
7. CMS case 0926914:IMC sends ping packets to unknown IP addresses after discovering devices. To resolve this problem, set the Enable Forged Ping Packets and Enable DismanPing parameters to No in the Layer 2 Topology Configuration area on the System > System Configuration > System Settings page.
8. CMS case 0927154:IMC 7.3 E0705P10 "DB connection error" while generating Asset report.
9. CMS case 0927014:IMC 7.3 E0705P10 RTLS issue - IP location not working "No match found".

## Resolved Problems in IMC PLAT 7.3 (E0705P12)

1. The sysUpTime column of the unused interfaces report fails to display the correct system up time for the listed interfaces.
2. Certificate configuration on the HTTPS Access Settings page fails.

3. imcacldm.exe crashes when putty07 file created in IMCROOT/server/conf directory, and dump files will be created under IMCROOT/server/conf/log/dump

## Resolved Problems in IMC PLAT 7.3 (E0705P11)

1. ICC Configuration Center cannot not display the latest available software image for MSR95x devices.
2. CMS case 0926756: iMC sends the y character twice during login. As a result, the user cannot log in to H3C 5500 devices for ICC operations.
3. CMS case 0926610: F5 device configuration backup failed.
4. CMS case 0926848: Upgraded the plink process to 0.74.
5. CMS case 926759: Liveupdate fails on 2930M or 2930F switches.
6. CMS case 926891: When the time zone is set to BRT (UTC-3) for the IMC server, the last hour performance data cannot be displayed.

## Resolved Problems in IMC PLAT 7.3 (E0705P10)

1. Failure to back up device configuration because the configuration file storage path is incorrect.
2. Failure to back up configuration of Aruba OS-CX devices, which is caused by TFTP.
3. Failure to configure VLANs on Aruba OS-CX devices when the RESTful API access privilege is set to read-only.
4. CMS case 926581, S3/P3 IMC 7.3 E0705P06 Configuration Center is not displaying Latest software available for MSR95x.

## Resolved Problems in IMC PLAT 7.3 (E0705P07)

1. Add VLAN to Links occasionally fails.
2. Compliance Policy Basic Match Rules "Variable" feature missing in E0705P04.
3. "Performance view all summary report V2", "performance view summary report V2" export is missing the "device IP" column.
4. IP address missing from CSV Export File- Performance Summary Reports.
5. VLANs added on the device doesn't show up in iMC.
6. Linux.10 sysoid identified as Sangfor_AF Series.
7. Cisco ASA backup change script request.
8. IMC device does not respond to ping alarm for IMC server itself.
9. Devices cannot be added via SNMPv3 and IPv6.
10. Update $iMCROOT/server/conf/adapters/ICC/Aruba Networks/Aruba205/enter_exec.tcl.
11. Real-Time Location failed because the dot1d node was not queried.
12. DBman did not restore the backup files when restoring the backup data.
13. IMC sends continous SSH requests to Aruba OS-CX version 10.5 devices.
14. Imcfaultdm process restarts frequently.
15. CVE-2020-24647 - AccessMgrServlet className Input Validation Code Execution Vulnerability.
16. CVE-2020-24648 - ZDI-CAN-8928 AccessMgrServlet className Deserialization of Untrusted Data Remote Code Execution.
17. CVE-2020-24649 - "ByteMessageResource transformEntity" Input Validation Code Execution Vulnerability.
18. CVE-2020-24650 - ZDI-CAN-8963 legend Expression Language Injection Remote Code Execution.
19. CVE-2020-24651 - ZDI-CAN-8964 SyslogTempletSelectWin Expression Language Injection Remote Code Execution.
20. CVE-2020-24652 - ZDI-CAN-8967 addVsiInterfaceInfo Expression Language Injection Remote Code Execution.
21. CVE-2020-7141 - ZDI-CAN-8968 addDeviceToView Expression Language Injection Remote Code Execution.
22. CVE-2020-7142 - ZDI-CAN-8971 eventInfo_content Expression Language Injection Remote Code Execution.
23. CVE-2020-7143 - ZDI-CAN-8970 faultDevParasSet Expression Language Injection Remote Code Execution.
24. CVE-2020-7144 - ZDI-CAN-8966 compareFilesResult Expression Language Injection Remote Code Execution.
25. CVE-2020-7145 - ZDI-CAN-8957 choosePerfView Expression Language Injection Remote Code Execution.
26. CVE-2020-7146 - ZDI-CAN-8960 devGroupSelect Expression Language Injection Remote Code Execution.
27. CVE-2020-7147 - ZDI-CAN-8961 deploySelectBootrom Expression Language Injection Remote Code Execution.
28. CVE-2020-7148 - ZDI-CAN-8962 deploySelectSoftware Expression Language Injection Remote Code Execution.

29. CVE-2020-7149 - ZDI-CAN-8981 ictExpertCSVDownload Expression Language Injection Remote Code Execution.
30. CVE-2020-7150 - ZDI-CAN-8987 faultStatChooseFaultType Expression Language Injection Remote Code Execution.
31. CVE-2020-7151 - ZDI-CAN-8988 faultTrapGroupSelect Expression Language Injection Remote Code Execution.
32. CVE-2020-7152 - ZDI-CAN-8985 faultParasSet Expression Language Injection Remote Code Execution.
33. CVE-2020-7153 - ZDI-CAN-8980 iccSelectDevType Expression Language Injection Remote Code Execution.
34. CVE-2020-7154 - ZDI-CAN-8982 ifViewSelectPage Expression Language Injection Remote Code Execution.
35. CVE-2020-7155 - ZDI-CAN-8989 select Expression Language Injection Remote Code Execution.
36. CVE-2020-7156 - ZDI-CAN-8986 faultInfo_content Expression Language Injection Remote Code Execution.
37. CVE-2020-7157 - ZDI-CAN-8991 selViewNavContent Expression Language Injection Remote Code Execution.
38. CVE-2020-7158 - ZDI-CAN-8996 perfSelectTask Expression Language Injection Remote Code Execution.
39. CVE-2020-7159 - ZDI-CAN-8959 customTemplateSelect Expression Language Injection Remote Code Execution.
40. CVE-2020-7160 - ZDI-CAN-8978 iccSelectDeviceSeries Expression Language Injection Remote Code Execution.
41. CVE-2020-7161 - ZDI-CAN-9002 reportTaskSelect Expression Language Injection Remote Code Execution.
42. CVE-2020-7162 - ZDI-CAN-8992 operatorGroupSelectContent Expression Language Injection Remote Code Execution.
43. CVE-2020-7163 - ZDI-CAN-8998 navigationTo Expression Language Injection Remote Code Execution.
44. CVE-2020-7164 - ZDI-CAN-9003 operationSelect Expression Language Injection Remote Code Execution.
45. CVE-2020-7165 - ZDI-CAN-8979 iccSelectCommand Expression Language Injection Remote Code Execution.
46. CVE-2020-7166 - ZDI-CAN-8993 operatorGroupTreeSelectContent Expression Language Injection Remote Code Execution.
47. CVE-2020-7167 - ZDI-CAN-8999 quickTemplateSelect Expression Language Injection Remote Code Execution.
48. CVE-2020-7168 - ZDI-CAN-9004 selectUserGroup Expression Language Injection Remote Code Execution.
49. CVE-2020-7169 - ZDI-CAN-8994 ictExpertCSVDownload Expression Language Injection Remote Code Execution.
50. CVE-2020-7170 - ZDI-CAN-8990 select Expression Language Injection Remote Code Execution.
51. CVE-2020-7171 - ZDI-CAN-8995 guiDataDetail Expression Language Injection Remote Code Execution.
52. CVE-2020-7172 - ZDI-CAN-9000 templateSelect Expression Language Injection Remote Code Execution.
53. CVE-2020-7173 - ZDI-CAN-8958 actionSelectContent Expression Language Injection Remote Code Execution.
54. CVE-2020-7174 - ZDI-CAN-9001 soapConfigContent Expression Language Injection Remote Code Execution.
55. CVE-2020-7175 - ZDI-CAN-8977 iccSelectDymicParam Expression Language Injection Remote Code Execution.
56. CVE-2020-7176 - ZDI-CAN-9015 viewTaskResultDetailFact Expression Language Injection Remote Code Execution.
57. CVE-2020-7177 - ZDI-CAN-9012 wmiConfigContent Expression Language Injection Remote Code Execution.
58. CVE-2020-7178 - ZDI-CAN-8984 mediaForAction Expression Language Injection Remote Code Execution.
59. CVE-2020-7179 - ZDI-CAN-9007 thirdPartyPerfSelectTask Expression Language Injection Remote Code Execution.
60. CVE-2020-7180 - ZDI-CAN-8983 ictExpertDownload Expression Language Injection Remote Code Execution.
61. CVE-2020-7181 - ZDI-CAN-9008 smsRulesDownload Expression Language Injection Remote Code Execution.
62. CVE-2020-7182 - ZDI-CAN-9006 sshConfig Expression Language Injection Remote Code Execution.
63. CVE-2020-7183 - ZDI-CAN-9011 forwardredirect Expression Language Injection Remote Code Execution.
64. CVE-2020-7184 - ZDI-CAN-9010 viewBatchTaskResultDetailFact Expression Language Injection Remote Code Execution.
65. CVE-2020-7185 - ZDI-CAN-9014 tvxlanLegend Expression Language Injection Remote Code Execution.
66. CVE-2020-7186 - ZDI-CAN-9009 powershellConfigContent Expression Language Injection Remote Code Execution.
67. CVE-2020-7187 - ZDI-CAN-8997 reportpage index Expression Language Injection Remote Code Execution.
68. CVE-2020-7188 - ZDI-CAN-9013 userSelectPagingContent Expression Language Injection Remote Code Execution.
69. CVE-2020-7189 - ZDI-CAN-8974 faultFlashEventSelectFact Expression Language Injection Remote Code Execution.
70. CVE-2020-7190 - ZDI-CAN-8973 deviceSelect Expression Language Injection Remote Code Execution.
71. CVE-2020-7191 - ZDI-CAN-8972 devSoftSel Expression Language Injection Remote Code Execution.
72. CVE-2020-7192 - ZDI-CAN-8969 deviceThresholdConfig Expression Language Injection Remote Code Execution.
73. CVE-2020-7193 - ZDI-CAN-8976 ictExpertCSVDownload Expression Language Injection Remote Code Execution.
74. CVE-2020-7194 - ZDI-CAN-9005 perfAddorModDeviceMonitor Expression Language Injection Remote Code Execution.
75. CVE-2020-7195 - ZDI-CAN-8975 iccSelectRules Expression Language Injection Remote Code Execution.
76. CVE-2010-1632 Apache Axis2 Vulnerability.

## Resolved Problems in IMC PLAT 7.3 (E0705P06)

1. The system displays the login page after the user clicks Save Configuration on the 3D device panel page of a device.

2. Telnet/SSH Proxy menu disappeared.
3. Optimization of automatic discovery for multiple subnets.
4. When the user attempts to view the details of a backup task or deployment task, the system displays an error that the task is not yet executed or has been deleted.
5. Fails to connect to SQL Server.

## Resolved Problems in IMC PLAT 7.3 (E0705P04)

1. The system failed to correctly open the VLAN topology page as requested by the user who accesses the system by using IE11.
2. The syslog RESTful API imcrs/syslog/log returns error code 500 in response to the API call that has the query parameter content set.
3. The system displays an error page after the user attempts to go back to a previous page by clicking a link in the breadcrumb navigation path on the Resource > Global Index Settings > Add Custom Index > Test Customized Index page.
4. The system displays an error page when deleting a group-based monitor entry whose associated custom view has already been deleted.
5. The system reports an error when an IE user attempts to add selected devices to a custom performance view.
6. Automatic alarm distribution failed when the username of the processor specified in the alarm distribution rule contains hyphens (-).
7. It takes a long time to open the IMC home page for an HTTPS user.
8. The JSON-formatted RESTful API response contains incorrect content.
9. The live update function is not available.
10. The $(FaultDuration) parameter is missing in the alarm forwarding email.

## Resolved Problems in IMC PLAT 7.3 (E0705P02)

1. CVE-2020-24629 IMC UrlAccessController Authentication Bypass Vulnerability.
2. CVE-2020-24630 IMC operatorOnlineList_content Privilege Escalation Vulnerability.
3. CVE-2020-24646 Hewlett Packard Enterprise Intelligent Management Center tftpserver Stack-based Buffer Overflow Remote Code Execution Vulnerability.
4. PSRT111053 IMC Expression Language Injection Remote Code Execution Vulnerability.
5. PSRT110958 IMC Expression Language Injection Remote Code Execution Vulnerability.
6. V-w3zer9hvd5 IMC "ByteMessageResource transformEntity" Input Validation Code Execution Vulnerability.
7. Data collection fails in distributed environment.
8. IMC's CPU has reached 100% on imcnetresdm randomply.
9. Alarm email not received for NEW devices until imcfaultdm process is restarted.
10. Configuration Center CLI Script Deployment Feature "Import Parameters" missing since 7.3 E0703.
11. Support for displaying a confirmation dialog box was added when the operator attempted to remove a monitor index from the set of default monitoring indexes.
12. Continues sending mail notifications after Alarm Notification was deleted.
13. Telnet/SSH operation logs display the super password in plain text.

## Resolved Problems in IMC PLAT 7.3 (E0705)

1. The alarm notification mail content format configuration field FaultDuration is changed to Duration.
2. A user who is only authorized to view a report template can delete and modify the report template.
3. In a non-English Windows operating system, if the administrator group name is not Administrators, you must manually execute command to start jserver process.
4. The Customize Column page of Virtual Resource Management has Chineses characters.
5. Updated the cacert of LiveUpdate.
6. Updated the IMC iHATool tool to resolve the problem that the IMC service cannot be started because iHA does not use the new service name when starting the IMC service.
7. The links in the VLAN topology do not support the break point feature.
8. The Read-Write Community String or Read-Only Community String field displays the default value on the page for

viewing or modifying an SNMP template, although the field was left empty when the SNMP template was created.
9. If you select multiple devices when deploying device configuration, the devices are not completely displayed (only the first 50 devices are displayed) on the configuration parameter page.
10. The exported syslog file cannot be deleted when the file expires.
11. LDAP authentication problem caused by too short a limit on the server name.
12. Real-Time Location timed out.
13. The running configuration of Huawei devices cannot be backed up through the SFTP protocol.
14. PSRT110973 IMC Expression Language Injection Remote Code Execution Vulnerability.
15. PSRT110974 IMC Expression Language Injection Remote Code Execution Vulnerability.
16. PSRT110975 IMC Expression Language Injection Remote Code Execution Vulnerability.
17. PSRT110976 IMC Expression Language Injection Remote Code Execution Vulnerability.
18. PSRT110977 IMC Expression Language Injection Remote Code Execution Vulnerability.
19. PSRT110978 IMC Expression Language Injection Remote Code Execution Vulnerability.
20. CVE-2019-5390 IMC dbman command 10018 (hostRoleSwitch) injection vulnerability.
21. CVE-2019-5391 IMC dbman command 10018 (hostRoleSwitch) Remote Stack Buffer Overflow.

## Resolved Problems in IMC PLAT 7.3 (E0703H01)

1. When a large number of compliance check tasks exist, it takes a long time to open the compliance check task list page.
2. When using the Deployment Guide-Deploy File function, an error occurs when you select devices that fail to be pinged or devices with unknown status.
3. The Operation column for the compliance check task list uses incorrect words.
4. When a compliance policy has an advanced rule with multiple lines of contents, the check result is incorrect.
5. When you deploy software for Cisco devices, the upload process takes a long time.

## Resolved Problems in IMC PLAT 7.3 (E0703)

1. The converged topology fails to be exported into Visio if ESX nodes exist in the converged topology.
2. Unused Interfaces Report V2 fails to be exported in PDF format.
3. Real-Time Location times out.
4. When you open the interface configuration wizard of batch operations and perform the **Add Ports to VLAN** operation, VLAN data cannot be queried on the page if the HTTPS access setting is configured to enable only HTTPS access.
5. For a virtualization performance monitoring index, no data item is displayed or multiple data items are displayed at the same time point.
6. CVE-2019-5392 IMC dbman Opcode 10001 Information Disclosure.
7. CVE-2018-7121 IMC JMX Insecure Config Unauth RCE.
8. CVE-2018-7122 IMC JMX Insecure Configuration Remote Unauthenticated Information Disclosure.
9. CVE-2018-7123 IMC dbman Opcode 10014 Unauthenticated 'kill' DoS.
10. CVE-2019-11941 IMC iccSelectDevType expression language injection remote code execution.
11. CVE-2019-11942 IMC TopoMsgServlet Expression Language Injection Remote Code Execution Vulnerability.
12. CVE-2019-11943 IMC soapConfigContent Expression Language Injection Remote Code Execution Vulnerability.
13. CVE-2019-11944 IMC AMF3 Externalizable Deserialization of Untrusted Data Remote Code Execution Vulnerability.
14. CVE-2019-11945 IMC AccessMgrServlet className Deserialization of Untrusted Data Remote Code Execution Vulnerability.
15. CVE-2019-11946 IMC ImcLoginMgrImpl Hard-coded Cryptographic Key Credentials Disclosure Vulnerability.
16. CVE-2019-11947 IMC dbman Use of Hard-coded Credentials Remote Code Execution Vulnerability.
17. CVE-2019-11948 IMC ifViewSelectPage Expression Language Injection Remote Code Execution.
18. CVE-2019-5370 IMC ictExpertCSVDownload Expression Language Injection Remote Code Execution Vulnerability.
19. CVE-2019-11949 IMC powershellConfigContent Expression Language Injection Remote Code Execution Vulnerability.
20. CVE-2019-11950 IMC WebSocket Shape3DWebSocketServlet Expression Language Injection Remote Code Execution Vulnerability.
21. CVE-2019-11951 IMC faultEventSelectFact Expression Language Injection Remote Code Execution Vulnerability.
22. CVE-2019-11952 IMC faultTrapGroupSelect Expression Language Injection Remote Code Execution Vulnerability.
23. CVE-2019-11953 IMC smsRulesDownload Expression Language Injection Remote Code Execution Vulnerability.

24. CVE-2019-11954 IMC operationSelect Expression Language Injection Remote Code Execution Vulnerability.
25. CVE-2019-11955 IMC devSoftSel Expression Language Injection Remote Code Execution Vulnerability.
26. CVE-2019-11956 IMC ByteMessageResource transformEntity Deserialization of Untrusted Data Remote Code Execution Vulnerability.
27. CVE-2019-5355 IMC dbman Opcode 10003 'Filename' Denial of Service.
28. CVE-2019-11967 IMC PLAT "ConfFileResource renameFile" Input Validation Code Execution Vulnerability.
29. CVE-2019-11968 IMC PLAT "ConfFileResource" Input Validation Code Execution Vulnerability.
30. CVE-2019-11969 IMC PLAT "ForwardRedirect" Expression Language Injection Code Execution Vulnerability.
31. CVE-2019-11970 IMC PLAT "ImcplatResServiceSkeleton" SQL Injection Code Execution Vulnerability.
32. CVE-2019-11971 IMC PLAT "isAccountBindingWithOperator" SQL Injection Code Execution Vulnerability.
33. CVE-2019-11972 IMC PLAT "OperatorMgrImpl" SQL Injection Code Execution Vulnerability.
34. CVE-2019-11973 IMC PLAT "queryDataBySQL" SQL Injection Code Execution Vulnerability.
35. CVE-2019-11974 IMC PLAT "queryIpAllocateInfoBySubnetIp" SQL Injection Code Execution Vulnerability.
36. CVE-2019-11975 IMC PLAT "queryOptionInfosByIp" SQL Injection Code Execution Vulnerability.
37. CVE-2019-11976 IMC PLAT "queryServerByIp" SQL Injection Code Execution Vulnerability.
38. CVE-2019-11977 IMC PLAT "readListBySql" SQL Injection Code Execution Vulnerability.
39. CVE-2019-11978 IMC PLAT "SmscCfgDaoImpl" SQL Injection Code Execution Vulnerability.
40. CVE-2019-11979 IMC PLAT "S-queryIpAllocateInfoByServerIp" SQL Injection Code Execution Vulnerability.
41. CVE-2019-11980 IMC PLAT "SSHParameterResource" InputValidation Code Execution Vulnerability.
42. CVE-2019-11981 IMC PLAT "updateEmailSuffix" SQL Injection Code Execution Vulnerability.

## Resolved Problems in IMC PLAT 7.3 (E0702)

1. The MIB node searching function on the MIB management interface is not available.
2. On the device details page, the MIB management menu privilege set by MIB management for an operator group does not take effect.
3. A card of an Aruba 8400 device is displayed in an incorrect slot on the device panel.
4. IMC cannot process the condition that the max VLAN node value is set to -1 on Cisco devices.
5. Cisco NX7000 configuration fails.
6. The sysoid range is modified to 1.3.6.1.4.1.9.12.3.1.3.* for Cisco Nexus devices.
7. When VLANs are being deployed to a device, if IMC logs in to the device through SSH, you will be prompted whether to save the password, and normal IMC login to the device is blocked.
8. The software upgrade causes errors to multiple levels of thresholds in the performance component.
9. The Real-Time Location positioning function is optimized.
10. The privilege of the viewer operator group might be lost randomly, which affects the normal login and access of operators in the group.
11. IMC cannot back up the Juniper Switches Ex4200.
12. The AirWave APs added to the converged topology cannot be displayed properly.
13. The IMC page crashes after the VXLAN component is installed.
14. IMC issues the commit command when polling the Juniper device configuration.
15. IMC cannot back up the Nortel ERS switches.
16. CVE-2019-5393 IMC dbman Opcode 10002 Arbitrary Backup.
17. CVE-2018-7124 IMC iccSelectCommand Expression Language Injection Remote Code Execution Vulnerability.
18. CVE-2018-7125 IMC PrimeFaces Expression Language Injection Remote Code Execution Vulnerabity.
19. CVE-2019-5338 IMC addVsiInterfaceInfo Expression Language Injection Remote Code Execution Vulnerability.
20. CVE-2019-5339 IMC devGroupSelect Expression Language Injection Remote Code Execution Vulnerability.
21. CVE-2019-5340 IMC actionSelectContent Expression Language Injection Remote Code Execution Vulnerability.
22. CVE-2019-5341 IMC SyslogTempletSelectWin Expression Language Injection Remote Code Execution Vulnerability.
23. CVE-2019-5342 IMC legend Expression Language Injection Remote Code Execution Vulnerability.
24. CVE-2019-5343 IMC compareFilesResult Expression Language Injection Remote Code Execution Vulnerability.
25. CVE-2019-5344 IMC faultDevParasSet Expression Language Injection Remote Code Execution.
26. CVE-2019-5345 IMC eventInfo_content Expression Language Injection Remote Code Execution.
27. CVE-2019-5346 IMC faultInfo_content Expression Language Injection Remote Code Execution.
28. CVE-2019-5347 IMC UrlAccessController Authentication Bypass Vulnerability.
29. CVE-2019-5348 IMC GWT deviceservice queryCustomCondition Expression Language Injection Remote Code Execution Vulnerability.

30. CVE-2019-5349 IMC TopoDebugServlet Expression Language Injection Remote Code Execution Vulnerability.
31. CVE-2019-5350 IMC TopoDebugServlet Deserialization of Untrusted Data Remote Code Execution Vulnerability.
32. CVE-2019-5351 IMC GWT deviceservice saveSelectedInterfaces Expression Language Injection Remote Code Execution Vulnerability.
33. CVE-2019-5352 IMC GWT perfAddFormServer getAddFormBean Expression Language Injection Remote Code Execution Vulnerability.
34. CVE-2019-5353 IMC reportpage index Expression Language Injection Remote Code Execution Vulnerability.
35. CVE-2019-5354 IMC GWT perfInsListServer getInsListBean Expression Language Injection Remote Code Execution Vulnerability.
36. CVE-2019-5355 IMC GWT perfAddFormServer getAddFormBean Expression Language Injection Remote Code Execution Vulnerability.
37. CVE-2019-5356 IMC CommonUtils unzip Directory Traversal Remote Code Execution Vulnerability.
38. CVE-2019-5357 IMC FileUploadServlet Unrestricted File Upload Remote Code Execution Vulnerability.
39. CVE-2019-5358 IMC viewTaskResultDetailFact Expression Language Injection Remote Code Execution Vulnerability.
40. CVE-2019-5359 IMC select Expression Language Injection Remote Code Execution Vulnerability.
41. CVE-2019-5360 IMC perfAddorModDeviceMonitor Expression Language Injection Remote Code Execution Vulnerability.
42. CVE-2019-5361 IMC faultParasSet Expression Language Injection Remote Code Execution Vulnerability.
43. CVE-2019-5362 IMC TopoDebugServlet Expression Language Injection Remote Code Execution Vulnerability.
44. CVE-2019-5363 IMC GWT deviceservice saveSelectedDevices Expression Language Injection Remote Code Execution Vulnerability.
45. CVE-2019-5364 IMC quickTemplateSelect Expression Language Injection Remote Code Execution Vulnerability.
46. CVE-2019-5365 IMC deviceSelect Expression Language Injection Remote Code Execution Vulnerability.
47. CVE-2019-5366 IMC guiDataDetail Expression Language Injection Remote Code Execution Vulnerability.
48. CVE-2019-5367 IMC MyFaces Static Key ViewState Use of Default Credentials Remote Code Execution Vulnerability.
49. CVE-2019-5368 IMC reportTaskSelect Expression Language Injection Remote Code Execution Vulnerability.
50. CVE-2019-5369 IMC tvxlanLegend Expression Language Injection Remote Code Execution Vulnerability.
51. CVE-2019-5370 IMC ictExpertCSVDownload Expression Language Injection Remote Code Execution Vulnerability.
52. CVE-2019-5371 IMC addDeviceToView Expression Language Injection Remote Code Execution Vulnerability.
53. CVE-2019-5372 IMC iccSelectRules Expression Language Injection Remote Code Execution Vulnerability.
54. CVE-2019-5373 IMC customTemplateSelect Expression Language Injection Remote Code Execution Vulnerability.
55. CVE-2019-5374 IMC operatorGroupTreeSelectContent Expression Language Injection Remote Code Execution Vulnerability.
56. CVE-2019-5376 IMC TopoMsgServlet Java Reflection Remote Code Execution Vulnerability.
57. CVE-2019-5377 IMC sshConfig Expression Language Injection Remote Code Execution Vulnerability.
58. CVE-2019-5378 IMC userSelectPagingContent Expression Language Injection Remote Code Execution Vulnerability.
59. CVE-2019-5379 IMC deploySelectSoftware Expression Language Injection Remote Code Execution Vulnerability.
60. CVE-2019-5380 IMC selViewNavContent Expression Language Injection Remote Code Execution Vulnerability.
61. CVE-2019-5381 IMC faultStatChooseFaultType Expression Language Injection Remote Code Execution Vulnerability.
62. CVE-2019-5382 IMC faultFlashEventSelectFact Expression Language Injection Remote Code Execution Vulnerability.
63. CVE-2019-5383 IMC wmiConfigContent Expression Language Injection Remote Code Execution Vulnerability.
64. CVE-2019-5384 IMC iccSelectDymicParam Expression Language Injection Remote Code Execution Vulnerability.
65. CVE-2019-5385 IMC perfSelectTask Expression Language Injection Remote Code Execution Vulnerability.
66. CVE-2019-5386 IMC viewBatchTaskResultDetailFact Expression Language Injection Remote Code Execution Vulnerability.
67. CVE-2019-5387 IMC navigationTo Expression Language Injection Remote Code Execution Vulnerability.
68. CVE-2019-5388 IMC Expression Language Injection Remote Code Execution Vulnerability.
69. CVE-2019-5389 IMC Expression Language Injection Remote Code Execution Vulnerability.
70. CVE-2019-11957 IMC dbman decryptMsgAes Stack-based Buffer Overflow Remote Code Execution Vulnerability.
71. CVE-2019-11958 IMC operatorGroupSelectContent Expression Language Injection Remote Code Execution Vulnerability.
72. CVE-2019-11959 IMC thirdPartyPerfSelectTask Expression Language Injection Remote Code Execution

Vulnerability.
73. CVE-2019-11960 IMC select Expression Language Injection Remote Code Execution Vulnerability.
74. CVE-2019-11961 IMC templateSelect Expression Language Injection Remote Code Execution Vulnerability.
75. CVE-2019-11962 IMC selectUserGroup Expression Language Injection Remote Code Execution Vulnerability.
76. CVE-2019-11963 IMC deploySelectBootrom Expression Language Injection Remote Code Execution Vulnerability.
77. CVE-2019-11964 IMC iccSelectDeviceSeries Expression Language Injection Remote Code Execution Vulnerability.
78. CVE-2019-11965 IMC deviceThresholdConfig Expression Language Injection Remote Code Execution Vulnerability.
79. CVE-2019-11966 IMC operatorOnlineList_contentOnly Cleartext Storage of Sensitive Information Privilege Escalation Vulnerability.
80. CVE-2018-7115 IMC buffer overflow in dbman.exe opcode 10001 on windows.

## Resolved Problems in IMC PLAT 7.3 (E0701)

1. None

## Resolved Problems in IMC PLAT 7.3 (E0605H09)

1. If a checkbox is selected and cleared multiple times, the operation speed becomes slow as the operation times increase.
2. Querying the specified gateways by IP might fail if the querying operation in the background takes more than 60 seconds.
3. Some history access logs that are not exported might be deleted.

## Resolved Problems in IMC PLAT 7.3 (E0605H08)

1. When multiple operators operate the autodiscovery page at the same time, they will affect each other.
2. An error occurs when you enter the device details page if the VXLAN component is installed and the number of VXLAN devices exceeds 2100.

## Resolved Problems in IMC PLAT 7.3 (E0605H07)

1. The **Real-Time Location** function be optimized.

## Resolved Problems in IMC PLAT 7.3 (E0605P06)

1. The mails sent are encoded in GBK.
2. The IMC platform has security vulnerabilities PSRT110696, PSRT110724,and PSRT110731.
3. An error occurs on the page when a port aggregation group is added or modified.
4. When configuration is being backed up for some devices, the CPU usage of the imccfgbakdm.exe process reaches 90%.
5. The mails of scheduled reports are sent twice.
6. The configuration backup and restoration function of DBMAN cannot be used if the password for the user named **sa** is modified in the Windows + separated distributed SQL Server database environment.
7. After the password for the user named **sys** is modified in the Linux+Oracle environment, the system fails to connect to the database.
8. An operator that has privilege to part of the user groups can view all users on the **All Users** page.
9. The **Device Asset Report V2** fails to be opened if assets with empty names exist.
10. Acknowledging alarms in alarm mails fails.
11. If the configuration to be deployed contains data that do not conform to the specifications of the device, the deployment task is shown as successful, but the configuration fails to be executed on the device.
12. The page for modifying indexes crashes if the threshold level is switched on the page.
13. When you select Other SMS Sender and configure General Configuration Access, SMS messages containing URLs with spaces fail to be sent.
14. When the MIB nodes of a Brocade device do not have interface physical address information, repeated device alarms might be generated.
15. The traffic topology window is not completely displayed and cannot zoom in or out properly.

16. In a distributed environment, the local-address field value in the server-addr.xml file becomes incorrect. As a result, the ITSM and BIMS components cannot work properly.
17. SNMP settings are not imported from .csv file to use with Auto Deployment.
18. IMC fails to upgrade 3600 series switches.
19. IMC Operator unable to log in after update.

## Resolved Problems in IMC PLAT 7.3 (E0605H05)

1. The alarm background process is continuously restarted.
2. Unit conversion is not performed for the dynamic threshold curve.
3. An error page opens if you use an operator that does not exist to log in.
4. An error page opens if you click Import Users.
5. An error page opens if you click Batch User Operations.
6. The device append information exported is empty if you export a custom view.
7. The capacity report cannot be properly exported in the .csv format.
8. An error page opens when you click Modify SubGroup Icon for an empty subview.
9. The website certificates are updated.
10. The menu for opening the Web manager is missing on the device view and device details pages.
11. On the All Users page, an operator that has the privilege only to part of the user groups can view all users.

## Resolved Problems in IMC PLAT 7.3 (E0605P04)

1. The status of a custom view is incorrect in the topology if the custom view contains multiple levels of subviews.
2. The compressed file downloaded is empty if the subordinate server process logs are downloaded on the Log Configuration page.
3. The exported topology file in visio format cannot be opened if IMC is installed in the Linux environment.
4. The dashboard cannot be displayed correctly.
5. The custom view topology is opened slowly if the custom view contains clouds.
6. The Page display style items configuration change does not take effect on the Configuration Templates page.
7. The page displays only the differences rather than all contents if you switch to Show Difference Only and then switch back to Show All on the Configuration Compare page.
8. The check task related pages are loaded slowly if a large number of check tasks exist.
9. An error page opens when you click Add Display Index if you enter the Display Index page through Auto Discovery > Set Default Monitor Indices > Monitor Option > Display Index.
10. The Traffic Topology does not display data if the same topology is opened on multiple clients and then one of these clients is closed.
11. The page crashes if you select Yes for Allow breaks in performance trend graphs on the Performance Option page.
12. The number of alarms on the alarm panel is different from the actual number of alarms if the following operations are performed: 1) Install the APM component in IMC. APM alarm A exists. 2) Add device B with alarm A to IMC for management. 3) Add the Important Devices widget to the Home page, and add device B to the widget. 4) Alarms are generated on device B.
13. On the Relationship Graph page for Root Alarm Display, the page does not respond when you select View Details or View CI Relationship from the shortcut menu of a device.
14. The number of alarms queried is incorrect in Hierarchical System Alarming.
15. The RESTful interface /imcrs/syslog/log queries data incorrectly.
16. In the converged topology, the cloud positions are not saved if the background of the converged topology is configured as the GIS map.
17. On the 5412 device panel, cards in slot A and slot I are not displayed.
18. A device cannot be added to a rack if virtual devices exist on the rack.
19. The custom topology is opened slowly if the topology has clouds.
20. Auto backup fails if multiple auto backup plans have the same device.
21. The alarm emails are encoded by using GBK.
22. The topology links for Cisco devices are missing if the CDP information of Cisco devices is incorrect.
23. The imcjobmgrdm process crashes if you select a custom view without devices when creating an auto backup plan.
24. The IMC platform components are exposed to Jackson security vulnerabilities CVE-2017-7525, CVE-2017-17485,

CVE-2018-5968, CVE-2018-7489, CVE-2017-9096.
25. The IMC platform components are exposed to security vulnerabilities ZDI-CAN-5749.
26. The IMC platform components are exposed to SLF4J security vulnerabilities CVE-2018-8088.
27. The IMC platform components are exposed to security vulnerabilities PSRT110694.

## Resolved Problems in IMC PLAT 7.3 (E0605H02)

1. HTTPS access to IMC is denied if the IMC version is upgraded from a version earlier than 7.3.

## Resolved Problems in IMC PLAT 7.3 (E0605)

1. The card positions are displayed incorrectly on the device panel if IMC PLAT is upgraded from an earlier version to IMC PLAT 7.3 (E0506L08) or later.
2. After related alarms are recovered, the number of alarms on the alarm panel is different from that on the alarm list.
3. In the IMC version leveraging the Oracle database, the trap list is empty.
4. The alarm source is displayed as NMS for APM application alarms if APM application alarms are forwarded through a method (for example, email).
5. Exporting the backup device summary report to a .pdf file failed.
6. The jdk certificate file shipped with IMC is incorrect.
7. In a Window environment, the DHCP Client and Windows Event Log services interfere with javaservice.exe, which might cause IMC upgrade failure.
8. After some Windows updates are installed, the TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA cipher suites are introduced, which might cause IMC upgrade failure.
9. The overlay information of a 6520XE device is slowly synchronized if the 6520XE device is fully configured with VSIs and then the VSI information is synchronized to IMC.
10. A device is repeatedly added if two operators add the same device to the same rack at the same time.
11. The **imcjobmgr** process restarts unexpectedly when all devices in the auto backup plan are deleted from IMC.
12. IMC installation or upgrade fails because of cipher suites.
13. IMC upgrade fails because file javaservice.exe is being used.
14. An error page opens when you display details about the Backup History Report if the number of devices in an Auto Backup Plan is greater than 1000.
15. LiveUpdate is unavailable for HPE 5406R zl2 Switch.
16. The auto database recovery succeeds, but a DBMan log message shows that the recovery fails because the ZIP file is greater than 2 GB.
17. VPN instances are not available for configuration backup on Cisco IOS devices that do not support VPN instances.
18. The system displays an operation timeout error if a user selects the Add VLAN to all Trunk and Hybrid ports option when adding VLANs for multiple devices in a topology.
19. The performance page does not respond if IMC has been running for around a week.
20. The imcfaultdm process automatically starts if filtering parameters are specified for a single device in an alarm filtering rule in a version earlier than IMC PLAT 7.3 (E0506P06) and then IMC is upgraded to version IMC PLAT 7.3 (E0506P06) or later.
21. In a HAC scenario, configuration template files cannot be synchronized to standby severs.

## Resolved Problems in IMC PLAT 7.3 (E0506P09)

1. The iHA client waits for a long period of time before a server group is successfully added if the server group is firstly added by the iHA client.
2. The IMC Sync server fails to start if two IMC servers are added to the same group, and the active server is switched.
3. The GSM modem test fails if you switch the GSM modem type and test the GSM modem.
4. The CPU and memory threshold alarms for the IMC server are inaccurate if the database service is started more slowly than the IMC service when the IMC server is restarted.
5. The backup time does not take effect though the system prompts that it is successfully modified if the backup time is modified during the DBMan backup process.
6. The global filtering conditions do not take effect if the filtering conditions are separately set for a device in the trap filtering rule.

7. The ICC device capability set shows that servers and storage devices are supported.
8. DBMan automatic backup fails and the process is restarted if the backup server is unreachable in a DBMan dual-server cold backup scenario.
9. Redundant monitor instances exist for the server storage space usage index monitoring.
10. The alarms on the upper-level IMC are not recovered if the lower-level IMC is configured to report recovered alarms to the upper-level IMC.
11. The IMC server disk space is fully occupied if a large number of core dump files appear on the IMC server in the Linux environment.
12. The alarm page does not respond if the device sends a large number of interface UP/DOWN alarms and the related interfaces do not exist on the device interface list page.
13. "/fault/alarm" On the REST interface, the returned data is incorrect when the data of the last page is queried.
14. "/fault/alarm" On the REST interface, the description of the orderBy parameter is incorrect.
15. "/fault/alarm" On the REST interface, the processing for the desc parameter is incorrect.
16. The IMC platform components are exposed to security vulnerabilities CVE-2018-1835.
17. On an English operating system, an alarm component upgrade might fail.
18. A device software upgrade might fail.
19. When the storage space on a device is greater than 4 GB, a storage space optimization fails.
20. The third parameter in an alarm that notifies the existence of a duplicate device cannot be resolved.
21. Maintainers cannot see a configuration template folder that they themselves created.
22. In the compliance check report, information that is expected to be displayed in a line of the compliance check report is displayed in two or more lines.
23. The LiveUpdate feature cannot upgrade an HPE 3800 or 2920 IRF fabric.

## Resolved Problems in IMC PLAT 7.3 (E0506P07)

1. When devices with invalid masks exist, the left resource tree cannot be displayed.
2. If IMC uses the MySQL database, the operation of deleting alarms is slow.
3. A compliance check task for devices in custom views is created. When you view details about the task, the information shows that the task checks all devices.
4. When you create a compliance check task by copying a compliance check task for the devices in a custom view, the operation fails.
5. When you click a search result of General Search, you cannot be navigated to the corresponding device information page.
6. An error occurs if you first set custom view parameters and then set traps when adding a filtering rule on the Alarm > Trap Management > Filtering Trap page.
7. After a compliance check task is executed, the check result column is empty if the compliance check task is created for devices in a custom view.
8. It takes a long time to query history access logs.
9. Access switches cannot be located in Real-Time VM IP Location.
10. The alarm information is inaccurate in the following conditions:
    - The device memory usage gradually increases.
    - Device Memory Trend Alarm is enabled in IMC.
11. The IMC platform components are exposed to security vulnerability CVE-2017-3735.
12. When IMC PLAT 7.3 (E0506) is installed and deployed, processes of the WSM component cannot start.
13. When an interface goes down, an alarm is generated. After the operator enables alarms for disconnected links, the alarm cannot be recovered when the interface comes up.
14. The IMC platform components are exposed to security vulnerability ZDI-CAN-5120.
15. The configuration backup fails on a Nortel BayStack device.
16. An HPE Stack device cannot restart after the software upgrade.
17. After the APM application alarm recovery, the number of alarms on the alarm list is different from the number of alarms on the alarm board.
18. The configuration backup fails on an HPE device.
19. When IMC is installed in a Linux environment, the database backup might fail.
20. The syslog resolution is incorrect when a syslog template with the Use Regular Expression option selected is added.
21. IMC cannot be added with devices that have duplicate IP addresses and interfaces in MIBs.
22. After the related alarms are recovered, the number of alarms on the alarm list is different from the number of alarms on

the alarm board.

23. The two interfaces of a link are displayed on the topology, but Idle Interface is displayed for these interfaces on the device interface list page.
24. The device-specific page cannot be opened when the operator queries devices through a general search and then clicks the query result.
25. WSM cannot be upgraded to IMC WSM 7.3 (E0506).
26. The IMC platform components are exposed to security vulnerability ZDI-CAN-5120.
27. The IMC platform components are exposed to security vulnerability CVE-2004-2761.
28. The IMC platform components are exposed to security vulnerability CVE-2017-3735.
29. The IMC platform components are exposed to security vulnerability ZDI-CAN-4067.
30. When IMC is upgraded to IMC PLAT 7.3 (E0506P03), the configuration template folder created by a user is not available.
31. A server error is prompted when the operator performs an SNMP operation in the MIB management window in the following conditions:
    - IMC is deployed with an Oracle database.
    - The operator has cleared the Read-Write Community String field on the device details page. Device Memory Trend Alarm is enabled in IMC.
32. Special characters cannot be used when you modify the username of an SNMP template.
33. When incorrect device SNMP parameters are added, the prompt has spelling errors.
34. After you move a combined subview in the topology, save the topology, and reload the topology, the location of the combined subview might drift if the subview contains a large number of devices.
35. The service monitors cannot be displayed if IMC is upgraded from an earlier version to a version later than IMC PLAT 7.3 (E0504P04).
36. The performance management component fails to be upgraded if the Windows system files are hidden.
37. The operator group privilege cannot be correctly configured for a performance view if an operator in a maintainer group adds the performance view.
38. After you click Performance Index Config on the System page, you cannot enter the performance index configuration page.
39. It takes more than 1 hour for the imcnetresdm process to start when IMC is started.
40. The imcl2topodm process is restarted if the Network Asset Management component is not installed.
41. An HPE stack device fails to be restarted if software is upgraded for the HPE stack device.
42. On the IP/MAC learning query page, the query result is empty for Cisco devices if SNMPv3 is configured to access Cisco devices.
43. The alarm component might fail to be upgraded if IMC PLAT is upgraded from version IMC PLAT 7.3 (E0504) to the patch version of IMC PLAT 7.3 (E0504).
44. The data on the alarm dashboard is incorrect if related alarms are recovered.
45. Configuration backup fails if you back up the configuration for Nortel BayStack devices.
46. An error message appears if the login method SSH and the transfer protocol TFTP are selected for configuring an HPE ProCurve device.
47. Down event alarms are periodically generated for an aggregate subinterface if the aggregate subinterface is down.
48. The link between a server and a switch is not displayed if the server has multiple IP addresses and supports forwarding packets.
49. Failed to log in to an HPE ProCurve 2510G device if SFTP is used to back up the configuration for an HPE ProCurve 2510G device.
50. The alarm statistics are incorrect if application alarms are deleted in APM.
51. The color of an aggregate link in the topology does not change when an aggregate subinterface of the link is down and generates alarms.
52. An error page appears when you delete a trap filtering rule or view the trap filtering rule details.
53. The IMC platform components are exposed to security vulnerabilities CVE-2017-12617, CVE-2017-8958, ZDI-CAN-5093, ZDI-CAN-4757 and ZDI-CAN-4905.
54. The IMC platform components are exposed to security vulnerabilities ZDI-CAN-4367, ZDI-CAN-4372, ZDI-CAN-4386, ZDI-CAN-4387, ZDI-CAN-4368 , ZDI-CAN-4373 , ZDI-CAN-4379 , ZDI-CAN-4377 and ZDI-CAN-4378.
55. The IMC platform components are exposed to security vulnerabilities ZDI-CAN-4896.

## Resolved Problems in IMC PLAT 7.3 (E0506P03)

1. The horizontal axis of the report on the performance view is too dense when the interval between the begin time and the end time is too long.
2. The alarm statistics on the fault board does not match the actual number of alarms when a user deletes devices.
3. IMC upgrade fails when a user has started a deployment task, which causes the imcscripttool and plink processes to be running.
4. Device configuration backup fails by chance.
5. The name of the default SNMP access parameter template can be modified through the REST interface.
6. The alarm statistics on the fault board does not match the actual number of alarms when the APM component is deployed.
7. VRM's REST interface for querying virtual machine information returns data without hard disk information.
8. Importing SNMPv3 devices fails.
9. A device fails to be added through the REST interface when the global SSH template is used.
10. The alarm escalation rule for traps is not updated when a user modifies a self-defined trap and deletes the parameter information.
11. Device synchronization might fail when a user configures the device login mode as Telnet in IMC and synchronizes the device on the ACL device list page.
12. The device information is not updated when a user synchronizes a device after the physical device is replaced.
13. MAC addresses of the Other type are not displayed when a user clicks IP/MAC Learning Query on device details page.
14. The IMC DHCP Plug service might fail to be started when a user restarts the DHCP server.
15. Device software backup might fail when a user backs up device software through TFTP.
16. The displayed device model is incorrect when a user adds an Aruba Stack 2930M device to IMC.
17. The displayed dynamic performance threshold is incorrect when a user adds the device for performance monitoring.
18. The device status changes to Unknown when a user modifies the SNMP parameter to a wrong value on the device details page and synchronizes the device.
19. DBMan fails to recover automatically when the IP address of the subordinate server is configured as a host name.
20. The configuration backup fails when a user backs up the configuration file of a Cisco Catalyst 2924C-XL-V device.
21. A widget has no data when a user adds the TopN widget on the homepage and an unreachable device exists.
22. The device space check timed out when a user upgrades the software for a Cisco stacking device.
23. The alarm fails to recover automatically when IMC receives an auto-recovered alarm.
24. The system prompts "Failed to connect the database server. Please manually input the database file path, which must exist on the database server." when the subordinate server is deployed with only the NTA component and the user clicks Configure on the Environment tab in the intelligent deployment monitoring agent.
25. If the SQL Express embedded database is used, the current database capacity includes the log file size when an alarm appears indicating that the database capacity is close to the upper limit.
26. In an IMC system that contains over 500 PCs, the system prompts a timeout error when some pages are accessed.
27. The imcfaultdm process is restarted if IMC receives alarms reporting interface down events for a link.
28. The imcsyslogdm process is restarted if syslog-to-alarm rules containing regular expressions are configured in IMC.
29. The system displays incorrect dynamic threshold statistics if IMC failed to collect threshold data at certain time points as intended.
30. The device details page of a ZTE device does not contain software version information.
31. The alarm panel displays incorrect alarm statistics if APM alarm sources are added to IMC.
32. The imcnetresdm process failed to start.
33. If the LLDP neighbor information on a port does not match the interface information displayed in IMC, the topology falsely displays two links while actually only one link exists.
34. After the operator configures the Automatic Device Sync Time setting and then restarts the imcnetresdm process, the Automatic Device Sync Time setting does not take effect.
35. An auto backup plan is no longer executed if a database connection error occurs during the execution of the plan.
36. Traps received from SNMP-incapable devices are not displayed on the Browse Trap page.
37. The system failed to back up the configurations of Cisco ASR9001 and ASR9904 devices.
38. The MIB management tool failed to record the complete MIB tree (the specified range of MIB OIDs) as intended if the MIB tree contains invalid MIB OIDs.
39. The Inventory Report contains an empty MAC Address column.
40. The operator cannot log in to IMC by using a password that contains over 15 characters.
41. The password in the SNMP template configured through REST API is displayed in ciphertext.
42. The device information file exported from the device view contains an empty Rack column.
43. The batch operation plan list on the Batch Operation Plan page contains a Modify column but modification for batch

operation plans is not supported.
44. The imcfaultdm process might restart if IMC receives traps from devices.
45. A space is appended to the label of the background area of a custom topology each time the operator clicks Save to exit the background editing mode.
46. Denial of service vulnerabilities ZDI-CAN-4808/ZDI-CAN-4809 occurs in the MIB management component.
47. Deserialization of untrusted data remote code execution vulnerabilities ZDI-CAN-4759/ZDI-CAN-4760/ZDI-CAN-4761 occur in the NE management component.
48. Deserialization of untrusted data remote code execution vulnerabilities ZDI-CAN-4810/ZDI-CAN-4811/ZDI-CAN-4812/ZDI-CAN-4813/ZDI-CAN-4814/ZDI-CAN-4815 occur in the resource management component.
49. Remote code execution vulnerability ZDI-CAN-4758 occur in the resource management component.
50. Remote code execution Vulnerability occurs in the DBMAN module.

## Resolved Problems in IMC PLAT 7.3 (E0506)

1. When device synchronization is performed on the ACL device page, the imcacldm process is restarted.
2. If IMC PLAT is upgraded to version 7.3 (E0504), the DBMan process fails to start.
3. After the device is replaced with another device with the same IP address, device synchronization fails.
4. If a user configures IMC to send alarms in SMS messages through the modem, SMS message sending fails.
5. If IMC PLAT 7.3 (E0504) is upgraded to any of its patch versions, the alarm component might fail to be upgraded.
6. ACL device synchronization might fail.
7. When a user opens the device panel of a third-party device, right-clicks a port of the device, and selects Interface Management > Port Properties or other items from the shortcut menu, the device details page prompts that the selected port doesn't support this operation.
8. If the ACL application configured on a device is associated with an inexistent ACL definition, a page error occurs when a user synchronizes the device and clicks the Advanced Query button on ACL device page.
9. When a user clicks the VLAN topology link in the navigation bar, selects a topology, and clicks OK, the VLAN topology page does not open.
10. When a user opens the Web manager through the right-click shortcut menu of the device in the topology, a blank page appears.
11. When a user modifies the instance layout for the performance view of the Gather Data type and clicks this performance view, an error occurs.
12. When a user modifies the default monitor indexes for performance and saves the modification, the default monitor indexes are all removed.
13. Auto backup succeeds, but the administrator receives no notification emails.
14. Chinese characters appear in the English version of IMC.
15. If IMC PLAT is upgraded to version 7.2 (E0403P10), The VLAN Management tab for 3Com switches is lost.
16. When execute actions in sequence is selected as the action execution type in the SCC policy, The execution result of actions displays failure even if the actions are successfully executed.
17. The port status is not displayed when a user views the device panel of some devices.
18. If IMC PLAT is deployed in distributed mode in the Windows environment, IMC PLAT fails to be upgraded to version 7.3 (E0504) on the subordinate hosts.
19. Most IMC processes in the Intelligent Deployment Monitoring Agent might disappear with a low probability if the IMC server is restarted after IMC PLAT is upgraded to version 7.3 (E0504) or its patch version.
20. Some items are not displayed if the number of items on the Remove Baseline page is more than the number of items that can be displayed per page.
21. IMC Plat has addressed multiple remote code execution injection vulnerabilities in this release. These include multiple vulnerabilities in the Java Server Faces (JSF) expression language, directory traversal, denial of service, and deserialization.

## Resolved Problems in IMC PLAT 7.3 (E0504P04)

1. The status of ports is incorrectly displayed when you view the HPE 2530-48G or HPE 2530-24G device panel in IMC.
2. The IMC DHCP Plug service fails to be started when the DHCP server or the IMC DHCP Plug service is restarted.
3. Security vulnerability exists if the database is backed up or restored in Intelligent Deployment Monitoring Agent.
4. The links connected to a router are not drawn in the topology.

5. The alarms of a device are not deleted completely 10 minutes after the device is removed from IMC.
6. The status of a task is displayed as Disabled after the auto backup plan runs for a period of time.
7. The H3C Comware V3 stack device configuration file fails to be backed up.
8. The imcupgdm process restarts unexpectedly if H3C Comware V7 software is upgraded and the Set the Current Running Software as Backup Startup Software option is selected.
9. ACL synchronization and deployment fail if ACLs of the name type exist on a Cisco device.
10. Part of the fields of alarms received through SMS or mail notifications are empty if stage forward is enabled for alarm notification rules.
11. The alarm description is different from the contents in the alarm parameters if IMC receives repeated alarms.
12. Some trap definitions with trap OID as 0 exist after IMC PLAT is upgraded to version 7.3.
13. The alarm notification rules do not take effect if stage forward is enabled for them.
14. The recovery time of a recovered trap changes if the system generates self-recovered traps.
15. The imcfaultdm process restarts unexpectedly if you modify the trap definition but do not modify the trap to alarm rule.
16. The Cisco ASR9010 configuration fails to be backed up.
17. When the CMDB CI attribute that contains a back slash (/) is saved and then read, the back slash (/) in the attribute is lost.
18. The Enable Web Proxy option in System Settings is displayed as Chinese characters in IMC in English.
19. The memory usage of the IMC service keeps increasing if IMC PLAT is upgraded to IMC PLAT 7.3 (E0504P02).
20. The expected prompt message does not appear when you enter special characters for the auto layout offset field in the advanced settings for the topology.
21. Only the IP address label is displayed for devices if IMC PLAT 7.3 (E0504P02) is directly installed, multiple labels (including Show IP) are selected for the topology, the configuration is saved, and the topology is reloaded.
22. The legend description for a Loopback-link device is literally inaccurate.
23. After the topology is reloaded, the position of a node in the topology is not the same as that when the topology is saved after the GIS map is configured as the background for the converged topology and the node is dragged to a certain position.
24. The links cannot be viewed conveniently if there are a lot of links after you select Compare with Baseline from the right-click shortcut menu in a blank area in the topology to view the comparison result.
25. The changed items are not prompted or highlighted and cannot be viewed conveniently if you select Compare with Baseline from the right-click shortcut menu in a blank area in the topology to view the comparison result.
26. The ProvinceRegional Map and Flow Center widgets appear when you switch to the platform from the dashboard configuration page.
27. If the administrator assigned views option is selected on the dashboard configuration page and several views are assigned to the group to which the operator belongs, all views are displayed on the same page when the dashboard views are opened.
28. The page crashes if you add a camera to a 3D room, right-click it, and select Data Source Type from the shortcut menu to configure the URL.
29. The rack view page does not respond if you click Modify Area on the rack view page.
30. IMC fails to receive SNMPv3 traps.
31. If a user selects the SNMPv3 template when configuring SNMP parameters for devices, the SNMP parameter test times out.
32. If IMC is upgraded to IMC PLAT 7.3 (E0504), DBMan fails to be started.
33. When a physical device is synchronized after it is replaced, the device asset information in IMC is not updated.
34. HPE1920 device configuration backup fails in IMC.
35. An HPE Aruba 2930M VSF switch is incorrectly identified in IMC.
36. If a greater value is entered when a user modifies the performance threshold, the displayed value is rounded and is different from the entered one.
37. When memory monitoring is added for CheckPoint2600, the performance view displays 100% for the memory usage.
38. When a user adds an operator group, adds an operator to the operator group, and then selects and clears the SNMP, SSH, and Telnet permission of the operator group repeatedly, the parameter template page does not display SNMP, SSH, or Telnet templates.
39. When IMC is upgraded to IMC PLAT 7.3 (E0504P02) and runs for a period of time, the CI list page does not display the CI list.
40. When Syslog data of the same day is queried on the Syslog page, the jserver process crashes.
41. The task name parameter is not parsed and is displayed as $1 on the details page of the trap named Device config is not

according to the rules of check task.
42. When the backup directories of the master and subordinate servers are inconsistent and DBMan is used to manually restore the database, database restoration on the subordinate server fails.
43. When the IMC PLAT 7.2 patch version is upgraded to 7.3, DBMan fails to be started.
44. The Service Monitoring page does not display service monitors that are successfully added.
45. The Task History page does not display the View Task Execution Report and View and Get Report links.
46. If IMC is upgraded to IMC PLAT 7.3 (E0504P02), a user is not navigated to the device details page when the user clicks a device label on the custom view page.
47. A user is navigated to the home page each time the user clicks a link in My Favorites.
48. After IMC is started, the login page might display the following message: Failed to load components during the system start up: Component name: iMC-Report.

## Resolved Problems in IMC PLAT 7.3 (E0504P02)

1. When the route topology feature is enabled and the outgoing interface of the directed route is a loopback interface or MP interface, the IP topology displays a large number of nonexistent links.
2. When all trunk ports (including aggregate interface member ports) are assigned to VLANs, an aggregate interface is disaggregated.
3. When the type of the SNMP template is modified to SNMPv3 Priv-Des Auth-Md5, the SNMP parameter test times out.
4. When the size of the .zip files in the backup data file of the Deployment Monitoring Agent exceeds 2 GB, database restoration fails.
5. The interface bandwidth usage index has no data after a device restart.
6. When IMC is installed in the French language, compliance check tasks cannot be created successfully.
7. When IMC uses the Oracle database, after an operator enters a value in a required field and clicks OK on the page for adding a compliance check task, the page does not respond.
8. When the user is an operator of a custom operator group, custom views cannot be selected when a user creates auto backup tasks.
9. The IMC HAC global configuration is lost after a primary/standby switchover.
10. When IMC PLAT 7.2 (E0403) is upgraded with the P06 patch, a license expiration message is displayed after IMC is started.
11. With the Use Regular Expression option selected for a syslog parsing template, an error occurs when an operator views, modifies, or copies the syslog parsing template.
12. When syslog export is performed, the immediate export has no export time or export data.
13. After an IMC upgrade, an error occurs when an operator views the trap filtering rules that are created before the IMC upgrade
14. When an operator views the trap definition list and the trap definition details, the trap OID information in the trap definition list is inconsistent with the trap OID information in the trap definition details, and Trap OIDV1 and Trap OIDV2 cannot be displayed.
15. When operators are added and device groups and manageable custom views are customized, privilege errors occur for modules of the IMC platform.
16. When the time range used for data statistics monitoring is switched, a page error occurs.
17. When an operator clicks the global index settings in the performance management module to configure the left navigation settings, the right side of the page is not redirected.
18. On the All Alarms > Advanced Query page, when an operator selects the Alarm Time Range for the Alarm at field, specifies the date and time, and then performs a query, an error occurs.
19. When an operator queries alarms by the time range of 00:00-24:00 or 23:59-24:00, an error occurs.
20. The background alarm process goes down and the System Settings page cannot open if a large number of traps from non-IMC-managed devices are received.
21. IMC is installed in an operating system that uses a comma (,) as a decimal point (for example, a German operating system) and the global threshold for a performance monitoring index contains a decimal fraction. After the threshold is successfully set, the fractional part of the value is displayed as 0s.
22. The configuration of an HPE VC 10Gb module fails to be backed up.
23. IMC auto backup fails if the auto backup time is set to 00:00 in the intelligent deployment monitoring agent.
24. The device configuration backup fails if SFTP is used to back up configuration for an H3C device and the display startup commands shows that the configuration file format is startup.cfg(*).

25. The CPU usage of the IMC server is high in an iHA scenario.
26. If dbman is used to implement auto backup and recovery in an iHA scenario, the master IP address of the standby host is switched to the heartbeat address after the standby host becomes the active host.
27. The background syslog process goes down if Syslogs in incorrect format are sent to IMC.
28. When the software is upgraded for HPE switches, two different software versions are identified as the same if the two software image file names end with letters.
29. Failed to modify NETCONF parameters for devices.
30. On the page for adding or modifying a configuration template, the non-default operator groups are not displayed.
31. The plat module has the security vulnerability of ZDI-CAN-4067/ZDI-CAN-4053/ZDI-CAN-4054/ZDI-CAN-4055/ZDI-CAN-4056.
32. In the device details for 5130EI series devices, the device management menu does not have the RADIUS Server Configuration and Interface 802.1X Configuration items.
33. After upgrading to IMC PLAT 7.3 (E0504), it's failed to synchronize the device with SNMP V3.

## Resolved Problems in IMC PLAT 7.3 (E0504)

1. None

## Resolved Problems in IMC PLAT 7.3 (E0503)

1. When more than 246 KB update packages are installed on the IMC server running Windows, the sysinfo tool fails to collect information about all KB update packages.
2. The report module has the security vulnerability of apache commons CVE-2016-4372.
3. When a large number of custom views exist, the Select Device page is slow to load on the resource homepage and all of the alarm pages.
4. The CPU usage is high in the HAC environment.
5. DBMan fails to recover from a backup file if the .zip file backed up by using DBMan exceeds 2G.
6. The configuration file backed up by iCC has incorrect contents if the echo display contains the greater than signs (>) when you log in to an HPE device.
7. IMC prompts the device software fails to be upgraded if the software upgrade process has been running for more than 1 hour for Cisco stack devices.
8. IMC fails to be upgraded from 7.2 to 7.3 if you try to upgrade IMC from 7.2 to 7.3 in an environment using the Thai language.
9. If the HPE Procurve device deploys startup configuration through SFTP, the deployment fails.
10. If the Cisco device deploys startup configuration through SCP, the deployment fails.
11. If the H3C Comware V7 device attempts to recover the device software, a timeout message is displayed.
12. If performance monitor is added in the MySQL environment, the performance monitoring data is unavailable occasionally.
13. The plat module has the security vulnerability of SQL Server CVE-2015-1761.

## Resolved Problems in IMC PLAT 7.2 (E0403P10)

1. When an operator modifies an ACL in IMC, the ACL rule numbers of the ACL change.
2. When an operator modifies an ACL in IMC, the ACL name of the ACL is deleted.
3. When a larger number of syslog to alarm rules are configured and the rules contain views, upgrading syslogs to alarms takes a long time.
4. When staged alarm notification is configured, the recipients of recovery alarms are not identical to the recipients of alarms.
5. When multiple devices are selected to execute access parameters checking, an error occurs when accessing the IMC home page and the log information indicates that the system is busy.
6. When no data is returned during the interaction of some GSM modems, SMS message test fails.
7. If the Telnet service is disabled on HPE ProCurve devices, configuration backup fails.
8. When alarms are forwarded through SMS messages, the SMS messages support including alarm generation time.
9. An operator fails to access the operator page after clicking Add Operator or Modify Operator.
10. The expiration date of the VXLAN module is not identical to the expiration date of the IMC platform on the About

page.
11. An operator fails to access the next page when the number of performance views exceeds the selected maximum display number of 50. When the maximum display number is set to 8, no page navigation icons are displayed.
12. IMC server throws Java exception when trying to TEST SNMP parameters in Batch operations SSH settings page.
13. Deprecate the REST interface /imcrs/vrm/host/templete for VRM.
14. After Java 8 is installed, a dialog box displaying " Block potentially unsafe components from being run " appears when you click SSH on device Action list.

## Resolved Problems in IMC PLAT 7.2 (E0403L09)

1. The device software library does not display the HPE 5900AF-5920AF_7.10.R2418P06-B software downloaded from LiveUpdate.
2. The AP monitoring data becomes abnormal when the AP is rebooted.
3. Failure to back up the configuration for HPE PROCURVE 26/28 series devices.
4. The VRM plugin cannot work properly because there is a line feed between the IP address and the port number in the VRM plugin configuration file.
5. On the IMC operator group management page, the Access Lower-Level NMS privilege (the privilege is added by default) is added to the viewer group to control the viewers' access to the snapshot of lower-level NMS view on the IMC resource page.
6. The IP addresses of online accounts are not correct on the access log history page.
7. You will receive the same Email twice if you configure two email addresses on the alarm notification page.
8. The system fails to upgrade the IMC inventory component when other database users are used.
9. After debugging is enabled, the IMC web page is unusable.
10. When you click Add or Modify on the System > Operators page, the page might hang or be busy.
11. If a transceiver module is plugged or unplugged, the transceiver module change is not displayed after the asset synchronization interval.

## Resolved Problems in IMC PLAT 7.2 (E0403P06)

1. When two cloud views point to each other's parent custom view, page errors occur.
2. VRM does not support Windows Server 2012 R2.
3. When an operator logs in to the backup IMC of an IMC system that has the primary and backup IMC licenses registered, the following message appears: Invalid license.
4. The statuses of subviews of a custom view are not counted in determining the status of the custom view.
5. The widgets on the dashboard cannot be refreshed.
6. Sometimes the mail sending feature for auto backup plans is unavailable and users cannot receive mails.

## Resolved Problems in IMC PLAT 7.2 (E0403P04)

1. When device synchronization is performed for multiple times, database access errors occur.
2. After Syslog events are occurred for a monitor index, an operator increases the threshold and reduces the repeat times value to be smaller than the occurrence times. Then, the performance module reports alarms even when the threshold is not exceeded.
3. Devices cannot be added to IMC by using SNMPv3 templates.
4. If IMC polls immediately after devices are restarted, the year in the generation time of interface down alarms might be 1970.
5. When IMC is upgraded to IMC PLAT 7.2 (E0403), IMC PLAT 7.2 (E0403L01), IMC PLAT 7.2 (E0403L02), or IMC PLAT 7.2 (E0403P03), alarm forwarding mails does not support the plaintext format.
6. When an operator attempts to delete a custom trap filter rule, a "system busy" message appears.
7. When an MP link recovers from the down state, the status of the MP link is not displayed correctly.
8. When services do not respond for a short time, service down alarms are generated in service monitoring.
9. VXLAN traffic information is generated based only on a single index.
10. Licenses for the IMC platform do not include the VXLAN license.
11. The ACL device list does not display HPE OEM devices of the H3C brand.
12. Aggregate interfaces cannot be added for devices running Comware V7.

13. When IMC is upgraded from versions earlier than IMC PLAT 5.1 (E0202) to IMC PLAT 7.2 (E0403L02) or IMC PLAT 7.2 (E0403P03), the Access Parameter Template page might display SNMP, Telnet, or SSH parameters as SNMP, Telnet, or SSH templates.
14. On the MSTI list page, VLANs mapped to MSTIs are incorrect for HPE devices.

## Resolved Problems in IMC PLAT 7.2 (E0403P03)

1. When the custom view contains multiple levels of cloud views in the custom topology, the status of a custom view or cloud view is incorrect in a custom topology.
2. The IMC platform components are exposed to OpenSSL security vulnerabilities CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, and CVE-2015-1794.
3. When the alarm matches two mail notification rules, an alarm mail is sent twice.
4. When idle interfaces are used as an interface filter criterion in port group view, subinterfaces of an aggregated link are displayed.

## Resolved Problems in IMC PLAT 7.2 (E0403L02)

1. When the WSM component is deployed, an operator can successfully change the theme of a dashboard through the theme menu, but the theme menu displays each theme name as undefined.
2. The operator can successfully delete a report on the My Reports page but fails to delete another report without refreshing the page.
3. When an operator logs in to IMC as a maintainer or viewer and attempts to access the realtime performance monitoring page, a page error occurs.
4. When a large number of performance monitor instances exist on a device, the At a Glance page of the device is loading and cannot display data.
5. When an operator logs in to the standard platform of IMC, the Resource tab does not display the Maintenance Task option.
6. When the screen resolution is set to 1280 and the IMC Web page theme is set to ash black, the basic management view page displays contents in the navigation bar at the top of the page in separate lines.
7. When an operator accesses the System Settings page, the System Settings page does not display the Task History Lifetime field.
8. When the alarm module is deployed, the tip information of each device in racks in the 3D room does not contain the alarm information.
9. The software products downloaded from LiveUpdate cannot be displayed in the software library of iCC.
10. The resource background fails to be started if you install SSM, create a virtual firewall, delete the firewall, and then restart the resource background.
11. A Syslog of more than 1024 bytes cannot be displayed correctly in IMC.
12. After an AP is rebooted, traffic statistics for the AP are displayed incorrectly.
13. If an alarm matches two rules in the alarm notification settings, alarm notification mails are repeatedly received for the alarm.
14. When a new rule is to be added to a compliance policy, in the device series selection window, the selected entries are cleared after entries are paged forward or backward.

## Resolved Problems in IMC PLAT 7.2 (E0403L01)

1. VLAN topologies are inaccessible in QSP view.
2. When a virtual machine on a host is cloned, the system displays a page for fixing the operation failure.
3. In QSP view, menus under Deploying Firmware are incorrect.
4. Customized columns on the network asset page are not displayed when the operator who customized them relogs in to IMC.
5. When interfaces on Comware devices are bound with VPN instances, the interface list for Comware devices does not display interface address information.
6. When a member port of an aggregate interface comes up again, the interface-down alarm for the port is not recovered.
7. IMC cannot display the CPU usage of each processor for a Linux server that has multiple processors.
8. Alarms sometimes are not triggered for services monitored on the Device Details page.

9. Direct link status does not change when the interface status in the route topology is changed.
10. When a new sFlow probe instance is added for a device, existing instances for sFlow probes are overridden.
11. VMs cannot be deleted from a host that runs CAS.
12. The sending time in SMS message delivery records is in 12-hour format for SMS messages delivered through the IMC SMS sender, third-party SMS sender, or mail-to-SMS conversion function.
13. In the RSM edition, the page crashes when an interface view is added.
14. Security holes #576313:Security holes exist when Apache Commons Collections Java library insecurely deserializes data.
15. Query criteria are invalid in the alarm query view after the IMC PLAT is upgraded to a version later than IMC PLAT 7.1 (E0303P13).
16. An error page appears when the parameter setting page of the custom report function is opened in a service component.
17. On the custom topology, device labels are modified to Korean character strings, and they become illegible after the topology is reloaded.
18. Device alarm event configuration entries cannot be added.
19. Lower-level IMC does not have the left navigation tree when it is accessed from the upper-level IMC system.

## Resolved Problems in IMC PLAT 7.2 (E0403)

1. This symptom occurs when a user views the dashboard that contains the per-level alarm trend chart. The dashboard displays data incorrectly.
2. This symptom occurs when a user adds the per-level alarm trend chart (the alarm class is all alarms) and the per-class statistics trend chart (the alarm class is configuration alarms) to the dashboard and monitors alarms for some time. Curves of the per-level alarm trend chart fall at irregular intervals.
3. This symptom occurs when a user selects a device on the Applet network topology, right-clicks the device, and then selects Open Device Panel from the shortcut menu. A page error occurs when a user accesses the device panel.
4. This symptom occurs when Enable Mail Notification is selected in license expiration mail notification settings on the system settings page. The mail content is incorrect and the mail format requires optimization.
5. This symptom occurs when a user accesses the system settings page with the alarm module not installed. Accessing the system settings page takes a long time.
6. This symptom occurs when a user clicks Add Link on the link management page for a custom topology. An error for the Add Link page occurs.
7. This symptom occurs when a maintainer logs in to IMC and double-clicks a cloud in the converged topology. A maintainer fails to open the topology for a cloud.
8. This symptom occurs when a user clicks the Add Link icon on the converged topology, or right-clicks the converged topology and selects Add Link from the shortcut menu. An error for the Link Management page occurs.
9. This symptom occurs when a user clicks Save in the toolbar on the converged topology. The note and the background area cannot be saved.
10. This symptom occurs when a uses accesses a REST API. The associated model schema for a REST API does not exist.
11. This symptom occurs after the WSM component is installed. The REST APIs of license management are unavailable and the response codes are 404.
12. This symptom occurs when a maintainer who has no management rights to self-service accounts modifies a user. A page error occurs when a maintainer attempts to modify a user.
13. This symptom occurs when IMC had ever been started before it was upgraded to IMC PLAT 7.1 (E0303P13). The Device Asset Report(Concise) cannot be obtained after IMC was upgraded to IMC PLAT 7.1 (E0303P13).
14. This symptom occurs when a user exports the Device Asset Report(Concise). The summary report at the end of the Device Asset Report(Concise) is displayed incorrectly after the Device Asset Report(Concise) is exported to an EXCEL file.
15. This symptom occurs when the performance management module is installed and monitoring objects are added in IMC that runs in Linux and uses an Oracle database. The performance background process restarts sometimes.
16. This symptom occurs when a user deploys the alarm management module of the IMC PLAT 7.1 (E0303P13) version, undeploys and removes the module, and then deploys the module again. An error occurs during the deployment of the alarm management module of the IMC PLAT 7.1 (E0303P13) version.
17. This symptom occurs when the sending alarm SMS message feature is enabled in IMC that runs in Linux. Alarm SMS messages cannot be received.
18. IMC runs on Linux and uses the Oracle database. An error page appears after an operator clicks Refresh on the server details page that contains an empty server name field.

19. The disk space of the IMC server is full after DBMan automatic backup runs for a long period of time in distributed, standalone, or primary/backup IMC deployment.
20. An operator disables the route topology feature and then synchronizes devices. The custom topology still contains links added by the route topology feature.
21. The topology page displays an incorrect link state after an operator performs the following procedure:
    a. On the topology page, changes the link interface for a device whose state has changed from reachable to unreachable.
    b. Views the link status.
22. The SNMP parameters test displays a Failure message after an operator performs the following procedure:
    a. Clicks MIB Management in the Action section of a device's Device Details page, and then opens the SNMP parameter configuration page.
    b. Configures the read-only community string in the Read-Only Community String field, and leaves the Read-Write Community String field empty.
    c. Clicks Test.
23. An operator configures an SMS messaging alarm notification rule with a plus sign (+) preceding the country code. The cellphone cannot receive alarm notification SMS messages.
24. The following error message appears after an operator deletes a trap definition from the trap definition list: Operation failed with error code 4002. Please contact your administrator.
25. An error page appears after an operator configures the alarm reporting feature for the first time on the hierarchical IMC alarming configuration page.
26. When an operator modifies index settings on the Add Monitor page and attempts to select the Global Index Settings option, a page error appears.
27. Monitor data loss occurs on the realtime performance monitoring page after a performance management module upgrade.
28. SMS messages cannot be sent by using the Convert Mail into SMS sending method after the reboot of IMC.
29. When a single mail notification rule on the Alarm Notification page contains more than one recipient address, sending of alarm notification mails fails.
30. A page error might occur when an operator clicks the ACL Configuration icon for a device on the ACL device list page of the ACL management module.
31. If a .csv file contains SNMPv3 parameters, it cannot be imported to auto deployment plans.
32. When the report module is deployed after the IMC platform with a remote database is upgraded to IMC PLAT 7.2 (E0403), the following message appears: Invalid object name 'TBL_RPTVIEWER_INSTALL_UPDATE'.
33. Database files backed up by running DBMan commands cannot be restored through DBMan.
34. After a device that includes aggregation interfaces is added to IMC, the VLAN device list does not display the device.
35. When the log level of the alarm module is set to Debug, CoreDump sometimes occurs in the background process of the alarm module.
36. If an online endpoint uses an IP address different than the endpoint IP/MAC address binding in the terminal access module, IMC generates IP/MAC address inconsistency alarms for the endpoint multiple times.
37. CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-2015-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015-6678, CVE-2015-6682, CVE-2015-5572, CVE-2015-5576, CVE-2015-6679, CVE-2015-5571.
38. All configuration template files in iCC will be cleared if you update an early version to IMC PLAT 7.1 (E0303P16) or later.

[ Table of Contents ]

---

# IMC Software Distribution Contents

The IMC PLAT 7.3 (E0710) distribution list contains the following files and folders:

1. **manual\readme_plat_7.3 (E0710).html** - This file
2. **windows\install** - IMC installation program
3. **linux\install** - IMC installation program for Red Hat Enterprise Linux

# Installation Prerequisites

## Server Requirements

The following are the minimum hardware requirements and supported software programs to run IMC platform, for additional resource requirements please check IMC components readme files:

- Minimum hardware requirements
  - Pentium 4 3.0 GHz processor
  - 12 GB of RAM
  - 100 GB hard disk space

- Operating system:
  - Windows Server 2012 X64 with KB2836988 (only iMC upgrade supported)
  - Windows Server 2012 R2 X64 (only iMC upgrade supported)
  - Windows Server 2016 X64
  - Windows Server 2019 X64 with KB5005112 KB5022840 KB5026362
  - Windows Server 2022 X64
  - Red Hat Enterprise Linux 7.3 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 7.4 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 7.5 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 7.6 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 7.9 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 8.1 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 8.2 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 8.3 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 8.4 X64 (Enterprise and Standard versions only)
  - CentOS 7.3 64bit (only iMC upgrade supported)
  - CentOS 7.4 64bit (only iMC upgrade supported)
  - CentOS 7.5 64bit (only iMC upgrade supported)
  - CentOS 7.6 64bit (only iMC upgrade supported)
  - CentOS 7.8 64bit (only iMC upgrade supported)
  - CentOS 7.9 64bit (only iMC upgrade supported)

- VMware:
  - VMware Workstation 6.5.x
  - VMware Workstation 9.0.x
  - VMware ESXi Server 5.5
  - VMware ESXi Server 6.0
  - VMware ESXi Server 6.5
  - VMware ESXi Server 6.7
  - VMware ESXi Server 7.0

- Hyper-V:
  - Windows Server 2012 Hyper-V
  - Windows Server 2012R2 Hyper-V
  - Windows Server 2016 Hyper-V
  - Windows Server 2019 Hyper-V

- Database
  - Microsoft SQL Server 2012 Express, Standard and Enterprise SP4 (Windows only)
  - Microsoft SQL Server 2014 Express, Standard and Enterprise SP3 (Windows only)

    - Microsoft SQL Server 2016 Express, Standard and Enterprise SP2 (Windows only)
    - Microsoft SQL Server 2017 Express, Standard and Enterprise (Windows only)
    - Microsoft SQL Server 2019 Express, Standard and Enterprise (Windows only)
    - Microsoft SQL Server 2022 Express, Standard and Enterprise (Windows only)
    - Oracle 11*g* Release 1 (Linux only)
    - Oracle 11*g* Release 2 (Linux only)
    - Oracle 12*c* Release 1 (Linux only)
    - Oracle 12*c* Release 2 (Linux only)
    - Oracle 18*c*(Linux only)
    - Oracle 19*c*(Linux only)
    - MySQL Community and Enterprise Server 5.5 (Linux and Windows) (Up to 1000 devices are supported)
    - MySQL Community and Enterprise Server 5.6 (Linux and Windows) (Up to 1000 devices are supported)
    - MySQL Community and Enterprise Server 5.7 (Linux and Windows) (Up to 1000 devices are supported)
    - MySQL Community and Enterprise Server 8.0 (Linux and Windows) (Up to 1000 devices are supported)

Note:An operating system marked with only iMC upgrade supported means that you can upgrade an existing iMC version but cannot install a new iMC version on the operating system. The maintenance services of such operating systems have ended or are about to end. As a best practice, do not use these operating systems in new sites.

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

Note: If an embedded database is used, you must install the **.net framework4.6** or **.net framework4.7.**

### GSM modem (optional)

A GSM modem is required for forwarding alarm messages. The following models have been tested to work with IMC. For more information about a specific GSM modem, see its product manual.

- WaveCom M2306B
- WaveCom TS-WGC1 (Q2403A)
- Wanxiang serial port GSM modem (DG-C1A)
- Wanxiang USB GSM modem (DG-U1A)
- Wanxiang USB min GSM modem (DG-MINI)
- WaveCom M1206B GSM modem (chip: 24PL)
- WaveCom USB M1206B GSM modem (chip: Q24PL, Q2403A)

[ Table of Contents ]

---

# Client Prerequisites

### PC Requirements

- Minimum hardware requirements
    - 2.0 GHz processor
    - 4096 MB of RAM
    - 50 GB hard disk space

- Operating system
    - Windows XP SP3 or later (except the tablet mode and touch mode)

- Browser
  - Firefox 50 or later is recommended.
  - Chrome 64 or later is recommended.
  - Turn off the pop-up blocking settings in the browser.
  - Add the IMC website to the trusted sites of the browser.
  - The recommended resolution width is 1280.
  - JRE 1.7.0_update76 or later is recommended. If a client has no JRE, IMC prompts the user to install JRE for the client.
  - After IMC is upgraded, clear the cache of the browser to get the optimal access experience.

[ Table of Contents ]

---

# Installing and Upgrading IMC

To install IMC on Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022, first modify the user account control settings:

1. Open the Control Panel from the Start menu and click **System and Security**.
2. In the **Action Center**, click the **Change User Account Control Settings** link.
3. In the **User Account Control Settings** window, set the **Choose when to be notified about changes to your computer** to **Never notify**.

To upgrade IMC:

1. Back up the IMC database on the **Environment** tab in the Deployment Monitoring Agent.
2. Manually copy the IMC installation directory to a backup path.
3. Stop IMC in the Deployment Monitoring Agent.
4. Restart IMC server.
5. Click **Install** on the **Monitor** tab of the Deployment Monitoring Agent
6. Select the **windows/install/components** directory in the upgrade package and click **OK**.
7. Click **OK** in the popup message dialog box.
8. Click **Start** in the **Upgrade Common Components** dialog box to upgrade common components.
9. After common components are upgraded, click **Close**.
10. In distributed deployment mode, stop the Deployment Monitoring Agent on the master server and restart the Deployment Monitoring Agent on every subordinate server. Click **Yes** in the popup message dialog box to upgrade common components on every subordinate server.
11. The Deployment Monitoring Agent displays all components that need to be upgraded. Click **OK** to start upgrading.
12. In distributed deployment mode, upgrade all components deployed on every subordinate server.
13. After all components are updated, start all processes in the Deployment Monitoring Agent.

For more information about installation and upgrade procedures, see *IMC Getting Started Guide* and IMC deployment guides.

Important:

1. *Before you upgrade the IMC Platform, download upgrade packages for all deployed service components from HPE's website, and before you install them pay special attention to the section "Platform Compatibility" in their readme. If an upgrade package is not available for a service component, HPE recommends not upgrading the IMC Platform, or you can remove the service component before upgrading the IMC Platform. When the service component is removed, its data is lost.*
2. *If the Deployment Monitoring Agent displays a list of components incompatible with the new version of the IMC Platform, you must download upgrade packages for these components before you can continue the upgrade process.*
3. *All service components must use v7.2 or higher to work with IMC PLAT 7.2. After the IMC Platform is upgraded, upgrade the deployed service components, such as WSM, UAM, EAD, NTA/UBA, APM, and SOM. Before installing or*

*upgrading a service component on this platform software, please verify the section "Platform Compatibility" in the service component's readme. Otherwise, IMC might not be started. For the compatibility matrix, see readme files of the service components.*

4. *If you receive the message "Upgrade JVM failed..." during the upgrade process, restart server and delete the folder in the* ***\common\jre*** *directory of the IMC installation path and continue to upgrade.*
5. *For data integrity, HPE recommends backing up database on the* ***Environment*** *tab of the Deployment Monitoring Agent, and copying the IMC installation directory to a secure location after the upgrade.*
6. *For an operating system that is not supported, please install IMC of the same version in a supported operating system, use DBMan to restore the data to the newly installed IMC, and them upgrade the newly installed IMC.*
7. *When the MySQL 5.X database is used, if IMC fails to connect to the database after version iMC PLAT 7.3 (E0703) or later is installed or IMC is upgraded to version iMC PLAT 7.3 (E0703) or later, modify the MySQL configuration file (my.ini in the Windows environment or my.cnf in the Linux environment) as follows: add default-time-zone = time zone of the operation system to [mysqld]. For example, if the time zone of the operating system is in China, add default-time-zone = '+8:00'. After modifying the configuration file, restart the database. In the Windows environment, perform the following tasks: 1) Select Start > All Programs > Administrative Tools > Services. The Services window opens. 2) Right-click the MySQL service name in the Windows operating system. From the shortcut menu, click Restart to restart the MySQL database. In the Linux environment, execute the service mysql restart command (for MySQL 5.5/5.6) or the systemctl restart mysqld.service command for MySQL 5.7 to restart the database.*

[ Table of Contents ]

---

# Removing IMC

To remove IMC on Windows, run the uninstallation wizard by selecting **All Programs > Intelligent Management Center > Uninstall IMC** from the Start menu, or you can remove the Intelligent Management Center in the **Add or Remove Programs** window of the Control Panel.

To remove IMC on Linux, enter the **deploy** directory of the IMC installation path by using the **cd** command, and then execute **uninstall.sh**. IMC is typically installed in the **/opt/iMC** directory.

Follow the directions in the uninstallation wizard, and manually delete all files in the IMC directory when the process is complete.

[ Table of Contents ]

---

# Running the Deployment Monitoring Agent

The Deployment Monitoring Agent is a GUI program to manage the deployment of the IMC modules and monitor the performance and the state of processes of the IMC server. After the installation finished, the Deployment Monitoring Agent is automatically started to guide the user through deployment.

On Windows, run the Deployment Monitoring Agent by selecting **All Programs > Intelligent Management Center > Deployment Monitoring Agent** from the Start menu. On Linux, run the Deployment Monitoring Agent by executing **dma.sh** in the **deploy** directory of the IMC installation path.

If Deployment Monitoring Agent cannot start, make sure the HPE IMC Server service is running. This service is automatically started along with the OS and runs as a daemon/background process. On Windows, you can start the service in Windows Services. On Linux, you can start the service with the **service imcdmsd start** command.

IMC must be started from the Deployment Monitoring Agent.

[ Table of Contents ]

# Starting IMC

To start IMC, click **Start IMC** on the **Monitor** tab of the Deployment Monitoring Agent.

[ Table of Contents ]

---

# Logging in to IMC through a Web Browser

Once the server is running, you can access the IMC user interface using a Web browser. Enter the following address in the Address Bar of a browser:

```
http://hostname:port/imc
```

Where *hostname* is the host name or IP address of the IMC server (the default is localhost if you launch the Web browser on the IMC server machine), and *port* is the Web server port (the default is 8080) used by IMC.

You can also access the IMC user interface with Web browser through HTTPS. Enter the following address in the address bar of a browser:

```
https://hostname:port/imc
```

Where *hostname* is the host name or IP address of the IMC server (the default is localhost if you launch the Web browser on the IMC server machine), and *port* is the Web server port for HTTPS (the default is 8443) used by IMC.

When the IMC login page appears, use the username "admin" and password "Pwd@12345" to log into IMC.

Refer to the IMC Online Help for details on how to add operators, and add your devices to IMC.

The default security level in the IE properties is High. If you try to log in to IMC with this default, the system will prompt "Content from the Web site listed below is being blocked by the Internet Explorer Enhanced Security Configuration." Click Add to add the IMC website to the trusted sites. If you do not add the IMC website to the trusted sites and determine not to display the prompt any more, you may fail to log in to IMC. To solve the problem, use either of the following methods:

1. Set the security level to **Medium**.
    - Start IE and select **Tools > Internet Options**.
    - Select the **Security** tab, and then click **Custom Level**.
    - In the popup dialog box, set the security level to **Medium**.
2. Add the website of the IMC server to the trusted sites.
    - Start IE and select **Tools > Internet Options**.
    - Select the **Security** tab, Select **Trusted sites**, and the click **Sites**.
    - Add the website of the IMC server in the popup dialog box.

On your first access to **Resource > Network Topology**, the browser prompts "The application's digital signature cannot be verified. Do you want to run the application?" Below the prompt are the name "topo", and the publisher "IMC Development Team". Select the "**Always trust content from this publisher**" checkbox, and click **Run**.

**Note:** *In centralized deployment, when the "User Access Manager - User SelfService" component is deployed, you will enter the Self-Service login page rather than the IMC login page if you enter **http://hostname:port/** in the address bar. To enter the IMC login page, change the string following **window.location.href=** into **'/imc/login.jsf';** in the index.html file in directory **\client\web\apps\ROOT**.*

[ Table of Contents ]

---

# Monitoring the Server

On the **Monitor** tab of the Deployment Monitoring Agent, you can see the Disk Usage, CPU Usage, and Physical Memory Usage of the IMC server. On the **Process** tab of the Deployment Monitoring Agent, you can see all IMC processes and their running status. On the **Environment** tab of the Deployment Monitoring Agent, you can see the OS information and database usage.

You can see the monitoring data of the IMC server only when IMC is started. For information about starting IMC, see "Starting IMC".

[ Table of Contents ]

---

# Distributed Deployment

The IMC components can be installed on more than one server to meet specific performance requirements. A distributed IMC system typically has one master server with IMC Platform deployed and multiple subordinate servers with service components deployed.

To install IMC on a subordinate server, execute the **installslave.bat** file on Windows (or **installslave.sh** on Linux) by either double-clicking the file or running the command in the folder where **installslave.bat** (or **installslave.sh**) is located.

For information about deploying IMC in distributed mode, see IMC deployment guides.

[ Table of Contents ]

---

# Platform Specific Issues

## Windows - General Issues

- Please be especially careful about how filenames are capitalized and used. This is essential in order to ensure consistent behavior across platforms that might use case-sensitive file systems.

## Linux - General Issues

- The IMC server must be run from a root user account in order to receive SNMP traps, accept syslog messages, and facilitate ftp file transfers.
- UNIX filenames are case sensitive. Care must be taken when references are made to python scripts and xml files.

[ Table of Contents ]

---

# Port Usage

IMC uses the following TCP/IP ports.

| Component | Subcomponent | Protocol | Port | Configurable | Use | Server | Client | Notes |
|---|---|---|---|---|---|---|---|---|
| IMC Platform | - | TCP | 8025 | No | Used by the **jserver** process to receive the | IMC master server. | IMC master server. | Internal use. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | SHUTDOWN command. | | | |
| IMC Platform | - | TCP | 9091 | No | JMX monitoring port used by the **jserver** process. | IMC master server. | IMC master server. | Internal use. |
| IMC Platform | - | TCP | 9044 | No | Used by the **HPE IMC Server** service to receive the SHUTDOWN command. | IMC master and subordinate servers. | IMC master and subordinate servers. | Internal use. |
| IMC Platform | - | TCP | 9055 | No | Used by the **Deployment Monitoring Agent** process to receive the SHUTDOWN command. | IMC master and subordinate servers. | IMC master and subordinate servers. | Internal use. |
| IMC Platform | - | TCP | 61616 | No | Used for communication in a distributed deployment environment. | IMC master server. | IMC master and subordinate servers. | Internal use. |
| IMC Platform | - | TCP | 61626 | No | Used for communication between the **HPE IMC Server** and **Deployment Monitoring Agent** processes. | IMC master and subordinate servers. | IMC master and subordinate servers. | Internal use. |
| IMC Platform | Resource Management | UDP | 161 | No | Used to access network devices through SNMP. | Network devices. | IMC master and subordinate servers. | |
| IMC | Resource | UDP | 162 | No | Used to receive | IMC | Network | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Platform | Management | | | | SNMP Traps from network devices. | master and subordinate servers. | devices. | |
| IMC Platform | Resource Management | TCP | 22 | No | SSH/SFTP port, which the configuration center uses to back up and restore the device software and configuration file through SSH/SFTP. | Network devices. | IMC master and subordinate servers. | |
| IMC Platform | ICC | TCP | 20/21 | No | FTP port, which the configuration center uses to back up and restore the device software and configuration file through FTP. | Network devices. | IMC master and subordinate servers. | |
| IMC Platform | ACL Management | TCP | 23 | No | Telnet port, which the resource management module, ACL management module, and configuration center use to access the device through Telnet. | Network devices. | IMC master and subordinate servers. | |
| IMC Platform | Alarm Management | TCP | 25 | No | SMTP port, which the resource management module uses to send alarms | SMTP Server | IMC master and subordinate servers. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | through email. | | | |
| IMC Platform | Resource Management | ICMP | | No | ICMP port, which the resource management module uses to discover devices and check the reachability of the devices. | Network devices. | IMC master and subordinate servers. | |
| IMC Platform | Resource Management | UDP | 69 | Yes | IMC-specific tftp daemon. | IMC master and subordinate servers. | | |
| IMC Platform | Resource Management | TCP | 80 | Yes | Used to launch the Web network management system of the device. | Network devices. | IMC master and subordinate servers. | |
| IMC Platform | Virtual Resource Management | TCP | 443 | Yes | HTTPS port, which the virtual network management module uses to obtain VMware virtual network data in SSL. | | IMC master and subordinate servers. | |
| IMC Platform | Syslog Management | UDP | 514/515 | Yes | IMC-specific syslog daemon. | IMC master and subordinate servers. | Network devices. | |
| IMC Platform | Resource Management | TCP/UDP | 137 | No | NetBIOS name resolution service port, used by the IMC resource management module and | | IMC master and subordinate servers. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | terminal access module. | | | |
| IMC Platform | - | TCP | 8080 | Yes | IMC-specific Web server for HTTP protocol, which can be changed during installation. | IMC master server. | | |
| IMC Platform | - | TCP | 8443 | Yes | IMC-specific Web server for HTTPS protocol, which can be changed during installation. | IMC master server | | |
| IMC Platform | - | TCP | 8800 | No | IMC messaging gateway listening port. | IMC master and subordinate servers. | IMC master and subordinate servers. | Internal use. |
| IMC Platform | - | TCP | 21190-21199 | No | Used for communication in HPE IMC Server, euplat and seplat. | IMC master and subordinate servers. | IMC master and subordinate servers. | Internal use. |
| IMC Platform | - | TCP | 1433 | Yes | SQL Server database listening port (on Windows only). | SQL Server. | IMC master and subordinate servers. | |
| IMC Platform | - | TCP | 3306 | Yes | MySQL database listening port. | MySQL Server. | IMC master and subordinate servers. | |
| IMC Platform | - | TCP | 1521 | Yes | Oracle database listening port (on Linux only). | Oracle Server. | IMC master and subordinate servers. | |
| IMC | DBMan | TCP | 2810 | No | Used for | DBMan. | DBMan | Internal |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Platform | | | | | communication in DBMan. | | | use. |

**Note:** *On Linux, you must run IMC with root privileges to bind TCP/IP ports 69, 162, and 514.*

**Note:** *IMC cannot be bound to TCP/IP ports 69, 162, and 514 if they are used by other SNMP, TFTP, or syslog applications.*

**Note:** *Make sure the firewall on each IMC server does not block programs javaw.exe and java.exe. The programs are located in directory \common\jre\bin (/common/jre/bin/java for Linux) of the IMC installation path.*

[ Table of Contents ]

---

# Memory Allocation

The amount of memory allocated to the IMC jserver can be adjusted by a script. The memory size should be tuned to make use of as much memory as required by your particular IMC server. Move to the "client\bin" (or "client/bin" on Linux OS) sub-directory of the original IMC installation directory (using the "cd" command), and use the `setmem.bat (or setmem.sh on Linux OS)` script.
For example, to allocate 1024 MB RAM, move to the "installation directory\client\bin" (or "installation directory/client/bin" on Linux OS) directory, and run the script:

`setmem.bat` *`2048`* (Windows OS)

`setmem.sh` *`2048`* (Linux OS)

The default and maximum memory that can be allocated to the IMC jserver is listed below:

| OS Type | Default allocatable memory | Maximum allocatable memory |
|---|---|---|
| Windows 64-bit | 2048 MB | Depending on the physical memory |
| Linux 64-bit | 2048 MB | Depending on the physical memory |

[ Table of Contents ]

---

# Known Problems

## Installation/Upgrade/Patch

- If you use the Windows Server 2019 operating system, you must install the Windows10.0-KB5005112, Windows10.0-KB5022840 and KB5026362 patches. The patches can be downloaded at the following URLs: https://support.microsoft.com/en-us/topic/kb5005112-servicing-stack-update-for-windows-10-version-1809-august-10-2021-df6a9e0d-8012-41f4-ae74-b79f1c1940b2; https://support.microsoft.com/en-us/topic/february-14-2023-kb5022840-os-build-17763-4010-e914539f-d2bc-4af9-bc01-5964c0ab3903; https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2023/05/windows10.0-kb5026362-x64_6984e22fb6e5980f59d8731da8b38415146acb50.msu. After patches are successfully installed, the operating system need to be restart.
- Upgrading iMC PLAT 7.3 (E0702) enterprise edition to iMC PLAT 7.3 (E0703) enterprise edition failed. To solve this problem, stop the iMC service and put the deploy.jar file in the iMC/deploy/components/iMC-NBAM/V700R002B05D009/ directory to another directory before upgrading iMC PLAT 7.3 (E0702) enterprise

edition. After upgrading, copy the deploy.jar file back to the iMC/deploy/components/iMC-NBAM/V700R002B05D009/ directory.
- For a correct installation, the installation path can contain letters, digits, underlines, and spaces, but cannot contain other special characters.
- If the system installed with IMC has insufficient memory, java overflow might occur. To prevent this issue, install IMC in a 64-bit OS with sufficient memory.
- During IMC platform upgrade from 7.1 (E0303L07), the system might display a message that directory iMC/deploy/jdk should be deleted manually. If you see the message, perform the following steps:
  - Start Windows Task Manager.
  - On the Processes tab, click the View menu and select Select Columns. Select the Command Line column and click OK.
  - Select the process named javaw.exe and click End Process.
  - In the dialog box that displays the upgrade error message, click Retry.
- You must install the performance and alarm components.
- The imcvnmdm process cannot start on an IMC server running iMC PLAT 7.3 (E0703) or a later version upgraded from iMC PLAT 7.3 (E0703).
- Versions iMC E0705P11 and iMC E0705P12 can be upgraded to iMC PLAT E0706. Normally, a prompt window displaying "Please upgrade components in the tools folder after upgrading the platform." opens when you enter the Choose Target Folder page after finishing common component upgrade for iMC PLAT. However, the prompt window might open unexpectedly before or when you upgrade the common components, which will cause an upgrade failure. To try again, click OK immediately to close the window.
- If version iMC PLAT 7.3 E0706 is installed, you must upgrade all components to version E0706 or compatible versions. For IMC to operate correctly, uninstall the components without compatible versions.
- With Windows Server 2019, some processes cannot be started in the deployment monitoring agent after IMC has running for more than one month. The workaround is to restart the imcsysdm.exe process.

## Other Problems

- The ADP task will fail when the creation time of the initial configuration file on the Web interface is different from the timestamp stored in the database. To solve this issue, please navigate to the **Service > Auto Deployment Plan > Initial Configuration File Management** page to manually delete and re-create the initial configuration file.
- As from iMC PLAT 7.3 (E0705), in the database distributed deployment environment, the database address for DMA can only be an IP address. Follow these steps to configure the database IP address for DMA: 1. Execute the iMC/deploy/instInfoMgr.bat -modify dbAddr=database IP address command in Windows environment, or execute the iMC/deploy/instInfoMgr.sh -modify dbAddr=database IP address command in Linux environment. 2. Set the database IP address for the db-config address parameter in the iMC/common/conf/server_addr.xml file.
- If the V1 report page cannot be opened, refresh the page to resolve this problem.
- Symptom: When you use HTTP to open the IMC page through a Chrome browser, the IMC page cannot be opened, and the browser prompts that "ERR_TOO_MANY_REDIRECTS, There were too many redirects."
- After IMC (windows edition) is upgraded to IMC PLAT 7.3 (E0504P04), the memory usage of the IMC service process becomes high.
- The endpoint Real-Time Location feature depends on the topology connection relationship of the gateway device. Make sure the topology connection relationship of the gateway device is correct.
- If the performance module is not deployed, a page error occurs when a user logs in to IMC.
- if EIA and IMC PLAT are deployed in centralized mode, the IMC page cannot be opened after IMC runs for a period of time.
- When traps are queried by trap OID, the query results are displayed in the SNMPv2c format by default.
- If the SendSmsTrapContentType parameter has been set in the qvdm.conf configuration file in IMC PLAT 7.2, you must reset the parameter on the System > System Configuration > SMSC Settings > SMS Content Format Configuration page after IMC is upgraded to version 7.3.
- When you modify a trap definition, the corresponding trap to alarm rule is not modified synchronously.
- Auto forwarding recovered alarm configuration is added to IMC PLAT 7.3 (E0504P02). If you do not need this feature, select No for Auto Forwarding Recovered Alarm Configuration on the System > System Configuration > System Settings page.
- If the system is busy, the progress bar may be shown for a long time when you perform an operation.
- IMC does not support the PoE features of Comware V3 devices.

- Configuration Center does not support the software upgrade of IRF devices through SSH/SFTP.
- Configuration Center does not support the software upgrade of old IRF2 devices or a device with dual main boards.
- If you configure a link aggregation across different units of IRF/IRF2 devices, the layer 2 topology cannot display the links because the master device cannot collect complete information about links of the subordinate members. Ensure you configure link aggregations only on the master device.
- When you view the check result of a compliance check task, the system might display "Do you want to abort the script?" if the check result contains too many devices and policies. Click **No** to continue the operation.
- A prompt "Connection to the server disconnected. Check the connection and try again" is displayed after the realtime performance monitoring runs for a while. Ignore the message and click **OK**.
- If the device model is not correct for a third-party device, select **System > Device Model** to edit the setting.
- In an SNMP packet, the SNMP variables of the visible string type, the encoding mode must be GBK or ASCII.
- If you upgrade your IMC to IMC PLAT 7.3, make sure you upgrade all components after the upgrade package is installed. Otherwise, IMC cannot start.
- The device locations might change on the Google map topology in windows of different sizes or in full screen with different resolutions.
- Discontinue monitoring the VM performance indices when the VM migrated to other hypervisor.
- If you cannot open the Applet topology after upgrading Java to the latest version for the client, select Control Panel > Java > Security, and set the Security Level to Middle.
- When you execute the backup.bat(.sh) script to back up IMC before upgrading IMC, only files are backed up, but the database is not backed up.
- In the dashboard, the realtime performance monitoring data for memory utilization is displayed for CPU utilization.
- In the converged topology, the status of a subview is always displayed as grey, which is displayed based on alarms of the highest level on the devices in the subview.
- The following problems occur to the 3D chassis in the data center: the added virtual devices and trays cannot be displayed; the device locations in the 3D chassis are incorrect; after you configure the chassis, the newly added devices can be displayed only after the 3D chassis is reloaded.
- In the Linux system, import device software fails when both IPv4 and IPv6 exist.
- If IP addresses on two different network segments are configured on the IMC server, the non-default initial configuration file fails to be downloaded when a device with zero configurations is automatically deployed.
- The SNMP test fails when the device location information is null.
- A user creates a view on the Flex-based display tiling page and adds performance trend widgets and widgets of other types for the view. The user configures no parameters for all widgets. The view displays the URL of the third-party control when the user accesses the view page for the first time. The URL of the third-party control disappears and the performance trend widgets become unavailable when the user accesses the view page for a second time.
- After VLAN interfaces are undeployed for tenants through RAM, the system prompts a configuration conflict if you deploy the same VLAN interfaces.
- When VLANs are deployed to a device, access interface configurations fail.
- After the Telnet or SSH parameters are modified for devices, the devices are not immediately synchronized in the ACL manager.
- A Cisco low-end switch is added to the IMC platform with the SSH access method, Password authentication mode, and an empty password field. When an operator syncs or tests connectivity to the switch, the memory usage of the resource background process soars in seconds and the process eventually crashes.
- Some of the E1POS interfaces of a device are not displayed on the device interface list, which is accessed by selecting POS Access > Interfaces on the device details page.
- When a user logs on to IMC with the browser in windowed mode and then maximizes the browser, the page size cannot be adjusted. To solve this problem, refresh the page.
- After the BIMS component is deployed on IMC, the V2 report still cannot be viewed. To solve this problem, delete the castor-0.9.9.1.jar in **iMC\client\repository\castor\jars** folder, and copy the castor-1.2.jar from **iMC\client\web\apps\rptviewer\WEB-INF\lib** folder to the **iMC\client\repository\castor\jars** folder.
- Chrome42+ disables NPAPI, including JRE. Because of this, IMC cannot open applet when using Chrome 42+.
- There are more than 20 devices in a filter rule, fail to add the Syslog filter rule.
- Add monitor again after the VM migrated to other hypervisor, discontinue monitoring the VM performance indices when the VM migrated to other hypervisor.
- This symptom occurs when use the converged topology feature. In the converged topology, the status of a subview is always displayed as grey, which is displayed based on alarms of the highest level on the devices in the subview.
- Open data center topology, The following problems occur to the 3D chassis in the data center: the added virtual devices

and trays cannot be displayed; the device locations in the 3D chassis are incorrect; after you configure the chassis, the newly added devices can be displayed only after the 3D chassis is reloaded.

- This symptom occurs when IP addresses on two different network segments are configured on the IMC server. The non-default initial configuration file fails to be downloaded when a device with zero configurations is automatically deployed.
- An operator frequently switches between floors of a room, On a room topology, frequent switches between floors cause the windows and doors to display incorrectly.
- A user creates a view on the Flex-based display tiling page and adds performance trend widgets and widgets of other types for the view. The user configures no parameters for all widgets. The view displays the URL of the third-party control when the user accesses the view page for the first time. The URL of the third-party control disappears and the performance trend widgets are unavailable when the user accesses the view page for the second time.
- This symptom occurs if the target device is not synchronized after VLAN interfaces are undeployed. After VLAN interfaces are undeployed for tenants through RAM, the system prompts a configuration conflict if you deploy the same VLAN interfaces.
- This symptom occurs if the Layer 2 aggregate interface configuration changes made in the VLAN manager are not synchronized to devices. When VLANs are deployed to a device, access interface configurations fail.
- This symptom occurs when the Telnet or SSH parameters are modified for devices. After the Telnet or SSH parameters are modified for devices, the devices are not immediately synchronized in the ACL manager.
- A Cisco low-end switch is added to the IMC platform with the SSH access method, Password authentication mode, and an empty password field. An operator tests connectivity to the switch, or sync the device to IMC platform. When an operator syncs or tests connectivity to a newly added Cisco low-end switch, the memory usage of the resource background process soars in seconds and the process eventually crashes.
- An operator accesses the POS Access > Interfaces page from the device details page. Some of the E1POS interfaces of a device are not displayed on the device interface list page.
- This symptom occurs when the CAS version is earlier than E0209.No data is collected when VRM monitors CAS.
- On the custom topology, device labels are modified to Korean character strings, and they become illegible after the topology is reloaded.
- The default background of the H3C Web desktop edition is changed to the HPE image.
- In HPE RSM edition, the HPE logo is not aligned to the upper-left corner on the login page.
- The topology does not support displaying complete distributed trunk links for HPE switches.
- Traps cannot be received when the trap OID exceed 128 characters or the trap packet exceeds 4096 bytes.
- When the SNMP packet maximum size on a device is set to a value greater than 4096, SNMP packets from the device cannot be parsed.
- In a non-English operating system, you must modify the language to English (United States) in the Control Panel > Region and Language window. Then, click Copy settings in the Administrative tab, and select Welcome screen and system accounts and New user accounts.
- In an English operation system, you must use the default language format in the Control Panel > Region and Language window.
- The Axis2(CVE-2010-1632) vulnerability exists. To solve this problem, manually delete the folder iMC\client\web\apps\imcws.
- After Java 8 is installed, a security warning dialog box displaying that the publisher is unknown appears when you click SSH on device Action list. To solve this problem, manually import the iMC\client\security\newksp12.p12 certificate file into the Signer CA certificate of jdk.
- If you select multi-level view for the Syslog upgrade rule, the device Syslogs cannot be upgraded to alarms according to the upgrade rule.
- If the value format is not ,. for the Oracle database client character set, the performance threshold cannot be modified.
- The display on the page is inconsistent with the actual deployment information if the subcomponents that do not stop the master server process (for example, APME) are updated or deployed on the subordinate server.
- The custom view data summary reports V2 created before the upgrade will be lost after the IMC platform is upgraded to IMC PLAT 7.3 (E0503).
- After IMC is upgraded, clear the cache of the browser to get the optimal access experience.
- When you configure SNMPv3 to send traps or informs to IMC, set the engine ID to 800063A2800123456789ABCDEF0123.
- The topology cannot be displayed and operated on touch screens.
- When IMC has ever upgraded to IMC PLAT 7.2 (E0403P02), IMC PLAT 7.2 (E0403P03), or IMC PLAT 7.2 (E0403P06), jserver cannot start after the iCC component is uninstalled.

- When IMC is upgraded from versions earlier than IMC PLAT 7.2 (E0403P10), the system prompts "Checking the installation environment failed."
- When IMC is upgraded to IMC PLAT 7.3 (E0506) in Windows, the memory usage of the dma and dms processes increases.
- The operator cannot be assigned privilege to part of user groups and the number of user groups cannot be larger than 2000.
- After modifying the database password, you must click the Environment tab on the Intelligent Deployment Monitoring Agent, and click Change Password to change the password synchronously on the dialog box that opens. Then, you must click Configure in the Database Backup and Restore area, and click OK on the Auto Backup and Recovery Settings dialog box that opens.
- The Tomcat service might exit exceptionally with a low probability if the topology, 3D room, and dashboard functions are used for a long time.
- If a large number of widgets exist on the homepage, a certain widget might be blank and prompt that "Please wait" when the homepage is opened.
- The NullPointerException errors might occur on the At a glance page if you query the detailed performance data of interface traffic for the first time within the custom time range.
- The topology is not available in tablet model. To use the topology on a touch-screen endpoint, disable the tablet model and use a mouse.
- Adding devices to the rack topology fails if IMC is running in the Linux + Oracle environment. To solve this problem, manually perform the following storage process in the database:
  declare columnDThreeExistedCount number;
  begin
  select count(1) into columnDThreeExistedCount from all_tab_cols t where t.table_name =
  upper('tbl_d3topo_deviceinfo') and t.column_name=upper('decribe');
  if columnDThreeExistedCount = 0 then
  execute immediate
  'ALTER TABLE tbl_d3topo_deviceinfo ADD decribe varchar(1024)';
  end if;
  end;
- In hierarchical NMS, the lower-level NMS performance view of the dashboard cannot obtain the performance view of the lower-level system if the username and password of the current user are used when the lower-level NMS system is added.
- For hierarchical IMC to operate correctly, please first upgrade the lower-level IMC and then upgrade the upper-level IMC, or restart the upper-level IMC after upgrading the lower-level IMC.
- In an active/standby IMC server scenario, please copy the iMC/common/conf/ks.dat and iMC/server/conf/imchw.conf files in the IMC installation directory on the active IMC server to the corresponding directories on all standby IMC servers. After copying these files, restart the IMC service to make these files take effect. If a standby IMC server is deployed with a separate database and the deployment monitoring agent is not installed on the database server, please copy the two files to the iMC/dbman/etc/ directory of the database server.
- After message push is enabled on the Task Management > Message Options page, some pages in IMC cannot operate correctly.
- After you upgrade IMC, clear the browser cache before logging in to IMC.
- An upper-level IMC system supports a maximum of 10 lower-level IMC systems, and each lower-level IMC system can manage a maximum of 5000 devices.
- The operator password cannot exceed 32 characters. In RADIUS, LDAP, or TACACS authentication, the user password on the authentication server cannot exceed 32 characters.
- If WSM is upgraded from IMC WSM 7.2 (E0502) or earlier, the WSM-related processes still exist after the WSM component is uninstalled.
- When a Window server with IMC installed is restarted, shut down, or logged off, the intelligent deployment monitoring agent must be ended through the ending program window if many service components are deployed.
- When a component is upgraded, the intelligent deployment monitoring agent prompts that "Checking the installation environment failed." if many service components are deployed and the component upgraded has many history versions.
- When the operating system is started, make sure the database is started before IMC.
- When the public components are updated in Windows, the system prompts that JDK upgrade fails. To solve this problem, manually stop the DHCP Client and Windows Event Log services for Windows, and then upgrade IMC.
- The operating system time must be the same on the master and subordinate servers.

- When use HTTPS to access IMC on a Chrome browser of certain versions, the homepage might be opened very slowly. This problem is caused by the Chrome browser. To avoid this problem, use the latest Firefox or IE browser.
- IMC fails to access some Huawei devices by using SSHv2. To solve this problem, use the undo ssh server authentication-type keyboard-interactive enable command on the devices to disable keyboard-interactive and then save the configuration.
- The 64-bit Firefox does not support NPAPI plugins (including JAVA), and support for NPAPI plugins is disabled in Firefox 52 and later. To access IMC features correctly through Firefox, use 32-bit Firefox of a version earlier than Firefox 52 or use Firefox ESR of a version later than Firefox 52. The operating system on which Firefox runs must have the 32-bit JAVA plugin installed.
- When there is a large amount of data in the generated performance report, the data on the horizontal axis and vertical axis might be very dense.
- The performance component must be installed.
- An upper-level NMS cannot view the server resources of a lower-level NMS if there is a GAP between the upper-level NMS and lower-level NMS.
- Exceptions occur in the Web manager, refresh, and server events if you execute the actions and configurations in the right pane of the server details page.
- For hierarchical IMC to operate correctly, please first restart upper-level IMC when restarting all the IMC's.
- When you click Expand All and Collapse All multiple times, the page responds slowly.
- Typically, 200,000 or less items of data can be exported successfully. Exporting too many data might fail.
- When the SQL Browser service is not started, some IMC processes might fail to start properly.
- When IMC is installed in the Linux environment, the characters on the installation interface are not clear during the installation process.
- If the upper NMS synchronizes devices in the hierarchical NMS environment, the devices managed by lower NMSs are not completely synchronized to the upper NMS.
- If auto discovery is performed, the auto discovery result does not display discovered devices.
- The system responds slowly to the operation of selecting or clearing checkboxes if you have operated IMC for a period of time after login.
- When IMC is deployed or upgraded in Red Hat Enterprise Linux Server 7.4, the progress bar is not displayed during the deployment/upgrade process.
- Support for automatically fixing SQL server orphaned users was added in iMC PLAT 7.3 (E0506P07). To enable this feature, set the resolve_orphan_user attribute in the iMC\client\web\apps\imc\reports\initPara.properties file to 1, and then restart jServer.
- When using the MySQL 8.0 database, you must modify the MySQL configuration file (my.ini in the Windows environment or my.cnf in the Linux environment) as follows: add loose-local-infile=1 to [client].
- Querying syslog only loads first 100000 enteries.
- To enable putty 0.70 in IMC PLAT 7.3 E0705P12, please manually create a file named putty07 in IMCROOT/server/conf directory.
- Duplicate files exist in the iCC device configuration backup file directory. You need to manually delete them.
- Topology report does not contain the aggregated sub link interface information.
- During SSH parameter verification, timeout will be prompted if the password is wrong.

[ Table of Contents ]

---

Issued: Jun 2023