IMC

Intelligent Management Center PLAT 7.3 (E0504P04)

Table of Contents

What's New in this Release

This version can be upgraded from only IMC PLAT 7.3 (E0504) and IMC PLAT 7.3 (E0504P02).

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 HP'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, HP 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 (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.
- Batch server deletion in the SSA module.
- 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 HP 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 (E0504P04) fixes the following problems, including all bugs fixed in IMC PLAT 7.2 (E0403) and later versions.

Resolved Problems in IMC PLAT 7.3 (E0504P04)

1. The status of ports is incorrectly displayed when you view the HP 2530-48G or HP 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. HP1920 device configuration backup fails in IMC.

35. An HP 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 HP 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 HP 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 HP 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 HP 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 HP 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 HP 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 7.
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 HP 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 the SSA version is upgraded from IMC PLAT 7.1 (E0303) to IMC PLAT 7.1 (E0303P13).A page error occurs when a user configures server power supply trap information.
14. 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).
15. 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.
16. 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.
17. 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.
18. This symptom occurs when the sending alarm SMS message feature is enabled in IMC that runs in Linux.Alarm SMS messages cannot be received.
19. 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.
20. 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.
21. An operator disables the route topology feature and then synchronizes devices. The custom topology still contains links added by the route topology feature.
22. 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.

23. 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.
24. 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.
25. 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.
26. An error page appears after an operator configures the alarm reporting feature for the first time on the hierarchical IMC alarming configuration page.
27. When an operator modifies index settings on the Add Monitor page and attempts to select the Global Index Settings option, a page error appears.
28. Monitor data loss occurs on the realtime performance monitoring page after a performance management module upgrade.
29. SMS messages cannot be sent by using the Convert Mail into SMS sending method after the reboot of IMC.
30. When a single mail notification rule on the Alarm Notification page contains more than one recipient address, sending of alarm notification mails fails.
31. 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.
32. If a .csv file contains SNMPv3 parameters, it cannot be imported to auto deployment plans.
33. 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'.
34. Database files backed up by running DBMan commands cannot be restored through DBMan.
35. After a device that includes aggregation interfaces is added to IMC, the VLAN device list does not display the device.
36. When the log level of the alarm module is set to Debug, CoreDump sometimes occurs in the background process of the alarm module.
37. 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.
38. 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.
39. 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 (E0504P04) distribution list contains the following files and folders:

1. **manual\readme_plat_7.3 (E0504P04).html** - This file
2. **windows\install** - IMC installation program
3. **linux\install** - IMC installation program for Red Hat Enterprise Linux

[Table of Contents]

Installation Prerequisites

Server Requirements

The following are the minimum hardware requirements and supported software programs to run IMC:

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

- Operating system (Versions marked X64 are recommended):
  - Windows Server 2008 with Service Pack 2
  - Windows Server 2008 X64 with Service Pack 2
  - Windows Server 2008 R2 with Service Pack 1
  - Windows Server 2012 with KB2836988
  - Windows Server 2012 R2
  - Red Hat Enterprise Linux 5.5 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.5 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.9 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 5.9 X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 6.x X64 (Enterprise and Standard versions only)
  - Red Hat Enterprise Linux 7.x X64 (Enterprise and Standard versions only)

- VMware:
  - VMware Workstation 6.5.x
  - VMware Workstation 9.0.x
  - VMware ESXi Server 4.x
  - VMware ESXi Server 5.x
  - VMware ESXi Server 6.0

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

- Database
  - Microsoft SQL Server 2008 Service Pack 3 (Windows only)
  - Microsoft SQL Server 2008 R2 Service Pack 2 (Windows only)
  - Microsoft SQL Server 2012 Service Pack 3 (Windows only)
  - Microsoft SQL Server 2014 (Windows only)
  - Oracle 11*g* Release 1 (Linux only)
  - Oracle 11*g* Release 2 (Linux only)
  - Oracle 12*c* Release 1 (Linux only)
  - MySQL Enterprise Server 5.5 (Linux and Windows) (Up to 1000 devices are supported)
  - MySQL Enterprise Server 5.6 (Linux and Windows) (Up to 1000 devices are supported)

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

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

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
  - 2048 MB of RAM
  - 50 GB hard disk space

- Operating system
  - Windows XP SP3 or later

- Browser
  - IE 10 or 11 is recommended.
  - Firefox 30 or later is recommended.
  - Chrome 44 or later is recommended.
  - Turn off the blocking settings in the browser.
  - Add the IMC website to the trusted sites of the browser.
  - The recommended resolution width is 1280.
  - JRE 1.6.0_update27 or later is recommended. If a client has no JRE, IMC prompts the user to install JRE for the client.

[Table of Contents]

Installing and Upgrading IMC

To install IMC on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2, 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. Click **Install** on the **Monitor** tab of the Deployment Monitoring Agent
5. Select the **windows/install/components** directory in the upgrade package and click **OK**.
6. Click **OK** in the popup message dialog box.
7. Click **Start** in the **Upgrade Common Components** dialog box to upgrade common components.
8. After common components are upgraded, click **Close**.
9. 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.
10. The Deployment Monitoring Agent displays all components that need to be upgraded. Click **OK** to start upgrading.
11. In distributed deployment mode, upgrade all components deployed on every subordinate server.
12. 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 HP'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, HP 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 v7.0 or higher to work with IMC PLAT 7.0. 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, delete the folder in the **\common\jre** directory of the IMC installation path and continue to upgrade.*
5. *For data integrity, HP 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.*

[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 HP 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 "admin" 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	N
IMC Platform	-	TCP	8025	No	Used by the **jserver** process to receive the SHUTDOWN command.	IMC master server.	IMC master server.	Int use
IMC Platform	-	TCP	9091	No	JMX monitoring port used by the **jserver** process.	IMC master server.	IMC master server.	Int use

IMC Platform	-	TCP	9044	No	Used by the **HP IMC Server** service to receive the SHUTDOWN command.	IMC master and subordinate servers.	IMC master and subordinate servers. Int 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. Int use
IMC Platform	-	TCP	61616	No	Used for communication in a distributed deployment environment.	IMC master server.	IMC master and subordinate servers. Int use
IMC Platform	-	TCP	61626	No	Used for communication between the **HP IMC Server** and **Deployment Monitoring Agent** processes.	IMC master and subordinate servers.	IMC master and subordinate servers. Int use
IMC Platform	Resource Management	UDP	161	No	Used to access network devices through SNMP.	Network devices.	IMC master and subordinate servers.
IMC Platform	Resource Management	UDP	162	No	Used to receive SNMP Traps from network devices.	IMC master and subordinate servers.	Network 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 through email.	SMTP Server	IMC master and subordinate servers.

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 terminal access module.		IMC master and subordinate servers.

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.	Int use
IMC Platform	-	TCP	21190-21199	No	Java RMI communication port.	IMC master and subordinate servers.	IMC master and subordinate servers.	Int 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 Platform	DBMan	TCP	2810	No	Used for communication in DBMan.	DBMan.	DBMan.	Int 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` *`1024`* (Windows OS)

`setmem.sh` *`1024`* (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 32-bit	512 MB	1024 MB
Windows 64-bit	2048 MB	Depending on the physical memory
Linux 32-bit	512 MB	1280 MB
Linux 64-bit	2048 MB	Depending on the physical memory

[Table of Contents]

Known Problems

Installation/Upgrade/Patch

- 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.

Other Problems

- 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 7.1, 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.
- A server automatic deployment plan contains a Windows OS template that has more than three partitions with the Use free capacity option selected.IMC failed to deploy the OS template in a server automatic deployment plan.
- This symptom occurs when DHCP is configured to assign IP addresses on a bare metal server and auto deployment is enabled in SSA.Auto deployment is not triggered for a bare metal server.
- This symptom occurs when a user operates multiple servers at the same time. For example, a user synchronizes server A and adds server B to SSA for management at the same time.An error occurs when IMC obtains server information.
- This symptom occurs when SSA monitors multiple servers.SSA collects data incorrectly.
- 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 HP 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.

[Table of Contents]

Issued: Apr. 2017