motive

# Home Device Manager 3.0.3.6
# Hotfix Readme

# Home Device Manager 3.0.3.6 Hotfix Readme

# Description

**Note:** This hotfix is cumulative and includes changes from the following other hotfixes:

- HDM 3.0.3.1
- HDM 3.0.3.2
- HDM 3.0.3.3
- HDM 3.0.3.4
- HDM 3.0.3.5

# Resolved issues

**The following issues are resolved in this hotfix:**

| |
|---|
| HDM-1625: Password not hidden in device history |
| HDM-1727: Log files not updated in real time |
| HDM-1924: When gateway switches WAN connections, the CR port mappings are not recreated / updated |
| HDM-1933: Device type not updated on distributed system |
| HDM-2128: When alarm details field is more than 4000 characters, it causes transaction rollbacks and prevents processing of device alarms |
| HDM-2140: lnPercentFreeBlocks miscalculated in sp_check_for_table_reorg script |
| HDM-2141: Disable row movement needed after "alter table shrink" |
| HDM-2152: setConnectionRequestURL is re-encoding encoded values |
| HDM-2153: setConnectionRequestURL does not URL encode the encrypted username and password |
| HDM-2525: CLONE - Filter on parameters to be cached |
| HDM-2548: TR-111 associations between GW and STB are getting removed |
| HDM-2675: Policy Advanced Schedule issue |
| HDM-2774: CLONE - Saving CPE ACS Username and Password of Failed Authentication to Database Table |
| HDM-2849: CLONE - Add capability to provide WebService Notification filtering based on Policy Class |
| HDM-2851: CLONE - HDM 3.1 TLD:TRS - 4.8-17 - NBI Callback Feature - Check for callBackInfo and invoke the plugin with callBackInfo. |
| HDM-3081: During activation tests CPE activation is failed although all steps needed for activation seems to be carried out correctly |

| |
|---|
| HDM-3085: Ghost repeated operations on HDM |

**The following issues are fixed in previous 3.0.3.x hotfixes:**

| | |
|---|---|
| HDM-1806: Inform Parameter Criteria not working correctly at event based policies at activation | 3.0.3.5 |
| HDM-1393: Weekly HDM DB cleanup script is failing | 3.0.3.5 |
| HDM-1301: Add an SCE property to disable the real time CR for an instant policy | 3.0.3.5 |
| HDM-1638: Alarm raised on deleted device | 3.0.3.5 |
| HDM-1611: Alarms not removed for deleted devices | 3.0.3.5 |
| HDM-1610: Alarm cannot be deleted | 3.0.3.5 |
| HDM-1946: Provide a new NBI API to update the CR URL of a given device | 3.0.3.5 |
| HDM-1765: Frequent inform alarms are not cleared if alarm definition is deleted | 3.0.3.5 |
| HDM-1759: Pruning script needed to prune old data | 3.0.3.5 |
| HDM-1990: HDM purge script has issue with gRefreshKeepList=false | 3.0.3.5 |
| HDM-1997: Bad behaviour of DynamicVariables management by NBI when trying to clear set variables compared to 3.0.2.7 | 3.0.3.5 |
| HDM-996: Increase storage for custom function context variables | 3.0.3.4 |
| HDM-1255: abortOperation from NBI does not work for queued actions | 3.0.3.4 |
| HDM-1285: registerDevice NBI method fails on duplicate Dynamic Variables, but no error | 3.0.3.4 |
| HDM-1324: findPolicyNameById NBI method does not work if the policy has been modified via GUI | 3.0.3.4 |
| 65871: add support for new PD-194 specific ChangeDeploymentState custom RPC | 3.0.3.3 |
| 66259: Empty dynamic variable in nbiService.registerDevice() voids *all* dynamic variables | 3.0.3.3 |
| 64234: use 2nd level caching (ehcache) for DeviceFilter and related objects | 3.0.3.2 |
| 64384: Connection Request to LAN device is issued even when CR Available flag on Device Type is false | 3.0.3.2 |
| 64971: STUNUsername/password set to white space instead of null during pre-activation | 3.0.3.2 |
| 65274: MESSAGE ID is not unsignedInt as per specs in UDP CR Get from HDM. (STUN) | 3.0.3.2 |
| 65698: Pre-activation policy - Remove unnecessary warning from log | 3.0.3.2 |
| 65759: Instant trigger policy and best effort CR has some issues | 3.0.3.2 |
| 65841: NATCRURL is not used during pre-activation of LAN devices even though it might be available | 3.0.3.2 |
| 65847: HDM does not issue retries up to the number specified by alcatel.cr.retries | 3.0.3.2 |
| 65851: Large number of session timeouts seen with custom function that updates a lot of parameters in device cache data records | 3.0.3.2 |
| 65973: add opaque transaction ID to NBIOperationResult | 3.0.3.2 |

| | |
|---|---|
| 65974: acsURL should be added to the RegistrationData in autoregistration module | 3.0.3.2 |
| 66004: No more then 16 events allowed | 3.0.3.2 |
| 65977: Allow customization of title bar in management console | 3.0.3.2 |
| 66022: Support DB server version 10.2.0.4 | 3.0.3.2 |
| 66096: Policy max runs per device per window executes the policy one more time than it is suppose to do | 3.0.3.2 |
| 66126: NBI incompatibility errors seen when invoking HDM NBI using SynchDeviceOps | 3.0.3.2 |
| 66169: IWE Axis call looking for alu-client-config.wsdd instead of client-config.wsdd | 3.0.3.2 |
| 64159: Notification Web Service Plugin Interop with .NET | 3.0.3.1 |

# Known issues

The following issues are known in this hotfix:

HDM-3074 : Support of SDO Call back feature in next version of IWE-3.0.3.2

# Prerequisites

Any of the following version(s) is the prerequisite for this hotfix:

- HDM 3.0.3
- HDM 3.0.3.1
- HDM 3.0.3.2
- HDM 3.0.3.3
- HDM 3.0.3.4
- HDM 3.0.3.5
- If you are using IWE, you will need to upgrade IWE to IWE 3.0.3.2 version or above. For details on performing this upgrade, see the HDM-IWE Release 3.0.3.2 Hotfix Readme file in your software distribution for HDM-IWE 3.0.3.2.

# Manifest

```
Readme3.0.3.6.html
Database/hdm_scheduled_cleanup.sql
Database/hdmreports_scheduled_cleanup.sql
```

```
Database/master_schema_upgrade.sql
Database/record_hotfix_version.sql
NBI Integration Toolkit/NBIRegistrationService.wsdl
NBI Integration Toolkit/NBIService.wsdl
NBI Integration Toolkit/build.xml
NBI Integration Toolkit/manifest.xml
NBI Integration Toolkit/run.bat
NBI Integration Toolkit/custom-functions/*
NBI Integration Toolkit/javadoc
NBI Integration Toolkit/lib/*
NBI Integration Toolkit/src/*
NBI Notification Plugin doc-literal/manifest.xml
NBI Notification Plugin doc-literal/wsdl/notification-service-doc-literal.wsdl
NBI Notification Plugin doc-literal/lib/*
NBI Notification Plugin/manifest.xml
NBI Notification Plugin/wsdl/notification-service.wsdl
NBI Notification Plugin/wsdl/registration-service.wsdl
NBI Notification Plugin/lib/*
Rebrand-scripts/Readme.txt
Rebrand-scripts/branding.properties
Rebrand-scripts/reBrand.sh
Scripts/updateServers.sh
Server/Distributed/hdm-distributed.ear
Server/GK7R.zip
Server/V9JJ.zip
Server/cpe-authenticator.jar
Server/hdm-nbi-non-ssl.ear
Server/hdm.ear
customfunctions/functions/portmapping.js
customfunctions/functions/portmapping.xml
samples/customfunctions/ChangeDUstate.js
samples/customfunctions/ChangeDUstate.xml
```

# Installation instructions

Depending on the deployment configuration (distributed vs. non-distributed, SSL vs. non-SSL NBI), you will need to perform one or more of the installation procedures listed below. For additional information on deployment architectures, see the installation section of the *Home Device Manager Deployment Guide, Version 3.0.0* (3JB-00029-ABAA-PCZZA) and the *Home Device Manager Installation Guide, Version 3.0.3* (3JB-00056-AAAA-PCZZA). To obtain these documents, you may access the Alcatel-Lucent OnLine Customer Support (OLCS) site at http://support.alcatel-lucent.com, select **Documentation** from the **Jump to Content page** drop-down list in the upper right of the window. On the **Product Index** (Alphabetical listing) page, select the Home Device Manager product to see a listing of all documents available.

## To prepare for the Home Device Manager update

1. Back up all data and installation directories:

   a. Create a hot backup of the data in the Home Device Manager OLTP database. This precaution enables rolling back the database to the previous version, if necessary.

b. Create a backup of the application server directory on each host in the HDMDomain (for example, `/opt/hdm`). Each individual application server requires a backup and storage for rollbacks to bring the servers to the same state as before the upgrade was installed.

2. Back up the existing `hdm.ear` file (or the `hdm-nbi-non-ssl.ear` file if the non-SSL option is used) from `/HDMDomain/`.

3. If you have a distributed domain deployment, back up the `hdm-distributed.ear` from `/HDMDistributedDomain/` on each server in the distributed domain.

4. Block all northbound and southbound traffic to servers by stopping all Home Device Manager Managed Servers:

   a. Log in to the Oracle WebLogic Server Console.

      i. In a browser, go to the following URL: `https://`*`adminhost.yourcompany.com:9002`*`/console`

         where:

         - *adminhost.yourcompany.com* is the address of the host on which the Administration Server is installed.
         - *9002* is the domain-wide administration port of the Administration Server.

         The login page appears.

      ii. To log in, type the credentials for your server administration account into the **Username** and **Password** boxes, and then click **Log In**.

      **Note**

      The Application Server Administrator account was created during the installation of the WebLogic Administration Server.

   b. From the directory tree (on the left), expand the **Environment** and click **Clusters**. The **Summary of Clusters** page is displayed.

   c. Click the **HDMCluster** link. The **Settings for HDMCluster** page is displayed.

   d. Click the **Control** tab and select the check box next to **Server**. This means that you are selecting all servers in the cluster.

   e. Click **Shutdown**, then select **When work completes**. You can alternatively choose the **Force Stop Now** option if you wish to stop the servers immediately without waiting. A confirmation dialog appears.

   f. Click **Yes** to proceed. The process may take several minutes. If the process appears to hang, use the **Force Stop Now** option instead, if you did not already choose this option above.

   g. Before proceeding, confirm that the state of the Home Device Manager servers appear as **SHUTDOWN** in the table.

5. On each Managed Server host, verify that all Managed Server processes are stopped using this command:

```
ps -ef|grep install_dir
```

where *install_dir* is the name of the directory in which the Home Device Manager is installed on the host. No Managed Server process should appear in the output.

6. If you have a distributed domain deployment, repeat step 4, but this time connect to the WebLogic Server Console of the protocol tier Administration Server.

7. If you have a distributed domain deployment, repeat step 5, but this time for the Managed Server hosts of the protocol tier.

## To delete the existing Home Device Manager application

1. Log in to the Oracle WebLogic Server Console:

   a. In a browser, go to the following URL: `https://adminhost.yourcompany.com:9002/console`

      where:

      - *adminhost.yourcompany.com* is the address of the host on which the Administration Server is installed.
      - *9002* is the domain-wide administration port of the Administration Server.

      The login page appears.

   b. To log in, type the credentials for your server administration account into the **Username** and **Password** fields, then click **Log In**.

      **Note**

      The Application Server Administrator account was created during the installation of the WebLogic Administration Server.

2. In the left panel of the console, click **Deployments**, then click **Lock & Edit**. The **Summary of Deployments** page appears on the right.

3. On the **Summary of Deployments** page, select the check box next to the Home Device Manager application (`hdm-nbi-non-ssl_ear` or `hdm_ear`, depending on whether the non-SSL or SSL version of Home Device Manager is being used for this deployment).

4. Click the **Delete** button. A confirmation dialog appears.

5. Click **Yes** to proceed.

6. In the left panel of the console, click **Activate Changes**.

7. Before proceeding, confirm that the Home Device Manager application does not appear on the **Summary of Deployments** page.

8. If you have a distributed domain deployment, repeat steps 1 through 7, but this time connect to the WebLogic Server Console of the protocol tier Administration Server. The `hdm-distributed` application needs to be deleted in this case.

## To update the database schema

1. From the Home Device Manager Hotfix software distribution, copy the `master_schema_upgrade.sql`, `hdm_scheduled_cleanup.sql` and `hdmreports_scheduled_cleanup.sql` files, which are located in the `/Database/` directory, into a temporary directory on the Administration Server host.

2. Use SQL*Plus to complete the following steps:

   a. Log in to the database instance:

      `sqlplus` *hdm_dbuser/password@net_service_name*

      where:

      - *hdm_dbuser* is the user name for the Home Device Manager OLTP schema owner account.
      - *password* is the password for the Home Device Manager OLTP schema owner account.
      - *net_service_name* is the net service name of the database instance.

   b. To upgrade the schema, type:

      ```
      @master_schema_upgrade.sql
      ```

   c. To update the cleanup procedures, type:

      ```
      @hdm_scheduled_cleanup.sql

      @hdmreports_scheduled_cleanup.sql
      ```

## To install Oracle WebLogic patches to correct real-time updating of log files

**Note**

This step is needed to fix issue HDM-1727: Logfiles not updated in real-time.

1. From the Home Device Manager Hotfix software distribution, copy `GK7R.zip` and `V9JJ.zip`, which are located in the `/Server/` directory, to a temporary directory on the Administration Server and on every Managed Server host in the HDMCluster.

2. From the Home Device Manager Hotfix software distribution, copy the `updateServers.sh` script, which is located in the `/Scripts/` directory, to the Administration Server and to every Managed Server in the cluster by placing the file in the same temporary directory that you used in step 1. (The `updateServers.sh`, `GK7R.zip`, and `V9JJ.zip` files must be located in the same directory.)

3. On **the Administration Server**, complete these steps:

   a. Change directory to the temporary directory in which you placed `GK7R.zip`, `V9JJ.zip`, and `updateServers.sh`.

   b. Run the `updateServers.sh` script on the Administration Server host by using the following command:

      `updateServers.sh` *BEA_home admin_server_host admin_server_port admin_user admin_pwd*

      where:

      - *BEA_home* is the root installation directory of the Administration Server
      - *admin_server_host* is the fully qualified host name of the Administration Server for the domain
      - *admin_server_port* is the Administration Server port number
      - *admin_user* is the Administration Server user name
      - *admin_pwd* is the password associated with the Administration Server user name

   c. Stop the Administration Server and restart it.

4. On **each Managed Server host in the cluster**, complete these steps:

   a. Change directory to the temporary directory in which you placed `GK7R.zip`, `V9JJ.zip`, and `updateServers.sh` on that Managed Server.

   b. Run the `updateServers.sh` script on that Managed Server using the following command:

      `updateServers.sh` *BEA_home_mgd_server admin_server_host admin_server_port admin_user admin_pwd*

      where:

      - *BEA_home_mgd_server* is the root installation directory of the Managed Server
      - *admin_server_host* is the fully qualified host name of the Administration Server for the domain
      - *admin_server_port* is the Administration Server port number
      - *admin_user* is the Administration Server user name
      - *admin_pwd* is the password associated with the Administration Server user name

   c. Stop the Managed Server and restart it.

5. If you have a distributed domain deployment, repeat steps 1 through 4 on all hosts of the protocol tier.

## To install the updated CPE Authenticator jar file

**Note**

This step is needed to fix issue HDM-2774 : Saving CPE ACS Username and Password of Failed Authentication to Database Table.

If you decide to make a back up of the old cpe-authenticator.jar file, please make sure you copy the old cpe-authenticator.jar file in a different directory. Do not keep the old cpe-authenticator.jar file in the weblogic92/server/lib/mbeantypes directory of the HDMDistributedDomain/lib directory for the distributed domain deployment hosts. Keeping the old cpe-authenticator.jar file in the same directory as the new one may cause WebLogic to load the old cpe-authenticator.jar file instead.

1. Log on to the Administration server host.
2. From the Home Device Manager Hotfix software distribution, copy `cpe-authenticator.jar`, which is located in the `/Server/` directory, to the `weblogic92/server/lib/mbeantypes` directory on the administration host of the `HDMDomain` domain and to the `HDMDistributedDomain/lib` directory for the distributed domain deployment hosts if the distributed domain deployment tier is used.
3. Stop all Managed Servers on this host and restart them.
4. Repeat the above steps 2 through 3 for all managed server hosts in the `HDMDomain` domain and in the `HDMDistributedDomain` if the distributed domain deployment is used.

## To start the Home Device Manager Managed Servers

1. Log in to the Oracle WebLogic Server Console:
   a. In a browser, go to the following URL: `https://`*`adminhost.yourcompany.com:9002`*`/console`

      where:

      - *adminhost.yourcompany.com* is the address of the host on which the Administration Server is installed.
      - *9002* is the domain-wide administration port of the Administration Server. The login page appears.

   b. To log in, type the credentials for your server administration account into the **Username** and **Password** fields, then click **Log In**.

      **Note**

      The Application Server Administrator account was created during the installation of the WebLogic Administration Server.

2. From the directory tree (on the left), expand the **Environment** and click **Clusters**. The **Summary of Clusters** page appears.

3. Click the `HDMCluster` link. The **Settings for HDMCluster** page appears.

4. Click the **Control** tab and select the check box next to **Server**. This means you are selecting all servers in the cluster.

5. Click the **Start** button. A confirmation dialog appears.

6. Click **Yes** to proceed. The process may take several minutes.

7. Before proceeding, confirm that the state of the Home Device Manager Managed Servers appear as **RUNNING** in the table.

8. If you have a distributed domain deployment, repeat steps 1 through 7, but this time connect to the WebLogic Server Console of the protocol tier Administration Server.

## To install the Home Device Manager application

1. From the Home Device Manager Hotfix software distribution, copy the `hdm-nbi-non-ssl.ear` or `hdm.ear` file (located in the `/Server/` directory) into the `/HDMDomain/` directory on the Administration Server host.

2. Log in to the Oracle WebLogic Server Console:

   a. In a browser, go to the following URL: `https://`*adminhost.yourcompany.com*`:`*9002*`/console`

      where:

      - *adminhost.yourcompany.com* is the address of the host on which the Administration Server is installed.
      - *9002* is the domain-wide administration port of the Administration Server. The login page appears.

   b. To log in, type the credentials for your server administration account into the **Username** and **Password** boxes, and then click **Log In**.

      **Note**

      The Application Server Administrator account was created during the installation of the WebLogic Administration Server.

3. In the left panel of the console, click **Deployments**, then click **Lock & Edit**. The **Summary of Deployments** page appears on the right.

4. On the **Summary of Deployments** page, click the **Install** button. The **Install Application Assistant** page appears on the right.

5. Using the file browser under the **Location** area, navigate to the `/HDMDomain/` directory that has the Home Device Manager application (`hdm-nbi-non-ssl.ear` or `hdm.ear` file, depending on whether the non-SSL or SSL version of the Home Device Manager application is being used for this deployment).

6. Click the radio button next to the `hdm-nbi-non-ssl.ear` or `hdm.ear` file. Click **Next** to proceed.

7. On the **Choose targeting style** page, choose the **Install this deployment as an application** option. Click **Next** to proceed.

8. On the **Select deployment targets** page, select the **All servers in the cluster** option. Click **Next** to proceed.

9. On the **Optional Settings** page:

   - For the *Security* section, choose **DD Only: Use only roles and policies that are defined in the deployment descriptors** option.

   - For the *Source Accessibility* section, choose **Copy this application onto every target for me** option.

10. Click the **Finish** button to complete the installation. This process may take a few minutes. Before proceeding, confirm that the state of the Home Device Manager application appears as **New** in the table.

11. In the left panel of the console, click the **Activate Changes** button. This process may take a few minutes. Before proceeding, confirm that the state of the Home Device Manager application appears as **Prepared** in the table.

12. On the **Summary of Deployments** page, select the check box next to the Home Device Manager application.

13. Click the **Start** button, and then click the **Servicing all requests** option. A confirmation dialog appears.

14. Click **Yes** to proceed. This process may take a few minutes. Confirm that the state of the Home Device Manager application appears as **Active** in the table.

15. If you have a distributed domain deployment, repeat steps 1 through 14, but this time connect to the WebLogic Server Console of the protocol tier Administration Server. The `hdm-distributed.ear` application needs to be installed to the `/HDMDistributedDomain/` on the protocol tier Administration Server host in this case.

## To record the hotfix version number

1. From the Home Device Manager Hotfix software distribution, copy the `record_hotfix_version.sql` file, which is located in the `/Database/` directory, into a temporary directory on the Administration Server host.

2. Use SQL*Plus to complete the following steps:

   a. Log in to the database instance:

      `sqlplus` *hdm_dbuser/password@net_service_name* where:

      - *hdm_dbuser* is the user name for the Home Device Manager OLTP schema owner account.

- *password* is the password for the Home Device Manager OLTP schema owner account.
- *net_service_name* is the net service name of the database instance.

b. To record the hotfix version, type:

```
@record_hotfix_version.sql
```

# To install the NBI Notification Plugin with Document/Literal style (optional)

1. Copy the jar files located in the `NBI Notification Plugin doc-literal/lib` to `/opt/hdm/lib`, where `/opt/hdm` is the root directory of your HDM installation.

2. Log in to the Server Configuration Console and add the following server properties:

   - `nbi.notification.sender.plugin.url.1`: Provide the fully qualified paths to the plugin jar files. In a Solaris environment, the URL address must be valid and well-formed. Use the !/ delimiter to separate .jar files in the .jar URL connection. For example, the SCE property may look like this:

     ```
     nbi.notification.sender.plugin.url.1 = jar:file:////opt/hdm/lib/↵
     nbi-notification-plugin-doc-literal.jar!/;jar:file:////opt/hdm/lib/XmlSchema-1.↵
     4.3.jar!/;jar:file:////opt/hdm/lib/axis2-kernel-1.5.1.jar!/;jar:file:////opt/↵
     hdm/lib/axis2-adb-1.5.1.jar!/;jar:file:////opt/hdm/lib/axiom-impl-1.2.8.jar!/↵
     ;jar:file:////opt/hdm/lib/axiom-api-1.2.8.jar!/;jar:file:////opt/hdm/lib/neethi-2.↵
     0.4.jar!/;jar:file:////opt/hdm/lib/httpcore-4.0.jar!/;jar:file:////opt/hdm/lib/↵
     axis2-transport-http-1.5.1.jar!/;jar:file:////opt/hdm/lib/axis2-transport-local-1.↵
     5.1.jar!/
     ```

   - `nbi.notification.sender.plugin.name.1`: Provide the fully qualified class name of the Doc/Literal web service notification plugin. For example, the SCE property should look like this:

     ```
     nbi.notification.sender.plugin.name.1 = com.alcatel.hdm.nbi.notification.plugin.↵
     DocLiteralWebservicesPlugin
     ```

3. Verify that you have correctly installed the Web Service Notification Plugin. From the Server Configuration Console, set the debug log levels by changing the values of the following properties to `DEBUG`, and check the trace log files at the moment the NBI notification is sent.

   - `com.alcatel.hdm.service.nbi.notification.logLevel=DEBUG`
   - `com.alcatel.hdm.nbi.notification.plugin.logLevel=DEBUG`

4. Configure the server properties for web service end point subscription for the Doc/Literal web service notification plugin. These must be configured for the DocLiteralWebServicePlugin to work; i.e. for sending notifications to the OSS listener (only for the Doc/Literal style):

   - To send `NBIOperationResult`, set the server property `nbi.notification.plugin.reference.operationresult.urls.1`

- To send `NBIBulkOperationResult`, set the server property `nbi.notification.plugin.reference.bulkoperationresult.urls.1`
- To send `NBIEventTriggeredPolicyResult`, set the server property `nbi.notification.plugin.reference.eventtriggeredpolicyresult.urls.1`
- To send `NBIInitiateConnectionResult`, set the server property `nbi.notification.plugin.reference.initiateconnectionresult.urls.1`
- To send `NBIDeviceActionResult`, set the server property `nbi.notification.plugin.reference.deviceactionresult.urls.1`
- To send `NBIDeviceRegistrationNotification`, set the server property `nbi.notification.plugin.reference.deviceregistrationnotification.urls.1`
- To send `NBIDeviceInformEvent`, set the server property `nbi.notification.plugin.reference.deviceinformevent.urls.1`
- To send `NBIDeviceActivationNotification`, set the server property `nbi.notification.plugin.reference.deviceactivationnotification.urls.1`
- To send `NBIDeviceReplacementEvent`, set the server property `nbi.notification.plugin.reference.devicereplacementevent.urls.1`
- To send `NBIUnknownGatewayEvent`, set the server property `nbi.notification.plugin.reference.unknowngatewayevent.urls.1`
- To send `NBIUnmatchingHttpUsernameEvent`, set the server property `nbi.notification.plugin.reference.unmatchinghttpusernameevent.urls.1`
- To send `NBIAlarm`, set the server property `nbi.notification.plugin.reference.alarm.urls.1`

Note: The Doc/Literal web service notification plugin(`com.alcatel.hdm.nbi.notification.plugin.DocLiteralWebservicesPlugin`) always looks for and sends to the web service end point subscription that ends with *.1; for example, `nbi.notification.plugin.reference.notificationType.urls.1`.

## To verify that the Home Device Manager hotfix installation was successful

1. Verify the version number:
   a. In a browser, go to the HDM Management Console at the following URL:

      `https://`*hdm.yourcompany.com*`:`*7004*`/hdm`

      or

`http://hdm.yourcompany.com:7003/hdm`

where:

- *hdm.yourcompany.com* is the host name for one of the following:
  - The load balancer that fronts the HDMCluster of Managed Servers in the application tier.
  - An instance of the Managed Server in the application tier.
- *7004* is the SSL port for the host.
- *7003* is the non-SSL port for the host.

The login page appears.

b. In the upper-left corner, pause on the product name, Home Device Manager. A tooltip appears with the following version information:

**HDM Management Console version** *Hotfix Version*

c. Log in by typing your credentials, and then click **Log On**.

2. By completing each of the steps above and yielding the expected results, you are done with the required installation steps for this hotfix. If the procedure above does not yield the expected results, there is a problem with the installation. In that case, roll the installation back according to *To roll back your Home Device Manager hotfix* section.

## To re-brand hdm.ear files with product title text and text color changes

The re-branding script and supporting files are located in the `Rebrand-scripts` directory of the software distribution. Detailed instructions are contained in the Readme.txt file in that directory.

# Implementation details for HDM 3.0.3.6

## To install the updated Portmapping Custom Function

**Note**

This step is needed to fix issue HDM-1924: When Gateway Switches WAN Connections, the CR Port Mappings Are Not Recreated / Updated.

To install the updated Portmapping Custom Function, upload the custom function, which consists of `portmapping.js` and `portmapping.xml` from the `customfunctions/functions` directory of the software distribution. You can use

the Custom Function toolkit that is distributed in the HDM 3.0.3 software distribution to update/install this portmapping custom function.

# Northbound interface impact

### Incoming NBI invocations to HDM

A new API, `setConnectionRequestURL`, is added to the NBI. This API allows customers to update the CR URL of a given device and is needed to support the use cases in the Generic TR-069 Proxy, which translates between TR-069 and non-TR-069 protocols such as Telnet and SNMP. Customers are not affected by this change unless they will use this new API. For details on this new API, see the related Javadoc in the {{{NBI Integration Toolkit/javadoc }}} folder of the HDM 3.0.3.6 software distribution.

### Outgoing NBI communications to External Systems

A new attribute, `opaqueTransactionId`, is added to the `NBIOperationResult` notification. Customers using reference web-service notification might have issues when receiving the `NBIOperationResult` notification. The web-service end point must be rebuilt using the new `notification-service.wsdl` provided. If this task is not performed, customers may observe compability issues and receive errors.

For customers using JMS notification, the jar file `ala-nbi-commons.jar` must be replaced with the old one.

# To install PD-194 Support

Beginning with the 3.0.3.6 hotfix, HDM now supports PD-194 (Software Module Management using TR-069). This feature includes these RPCs:

- ChangeDUState (ACS RPC)
- AutonomousDUStateChangeComplete (CPE RPC)

This feature must be activated by uploading the custom function, comprising the `ChangeDUstate.js` and `ChangeDUstate.xml` files, from the `samples/customfunctions` directory. You can use the Custom Function toolkit that is distributed in the HDM 3.0.3 software distribution to create the function `changeDeploymentStateFunction` in HDM. There is no GUI update to support this function. It is triggered through the NBI `createSingleDeviceOperationByDeviceGUID` (FunctionCode 120).

For details on the PD-194 specification, please consult the Broadband Forum website. HDM replies to CPEs in different cases (SCE + namespace combinations) as described below.

- **Control of DSL forum namespace `xmlns:cwmp="urn:dslforum-org:cwmp-1-x` in HDM RPCs** : PD-194 requires using `xmlns:cwmp="urn:dslforum-org:cwmp-1-2"`. For backward compatibility with CPEs that do not support this namespace, an SCE property `replay.cpe.cwmp.namespace` is introduced. The behavior of this property is as follows:

- When a CPE sends messages with namespace `cwmp-1-0`, HDM sends reply RPCs with the same namespace `cwmp-1-0`.
- If the SCE flag is set to **true**, HDM replays the same namespace that the CPE used to send the message to HDM.
- If the SCE flag is set to **false**, HDM sends messages with the default name space `cwmp-1-0`
- The SCE property is global with replay flag set to **false** by default.
- Overview :

| *CPE namespace* | *SCE definition* | *HDM namespace* |
|---|---|---|
| 1-0 | not defined | 1-0 |
| 1-2 | not defined | 1-0 |
| 1-0 | false | 1-0 |
| 1-2 | false | 1-0 |
| 1-0 | true | 1-0 |
| 1-2 | true | 1-2 |

# To understand the new SCE property nbi.notification.registration.landevice.delay.seconds

A new SCE property `nbi.notification.registration.landevice.delay.seconds` is added to address issue 65841: NATCRURL is not used during pre-activation of LAN devices even though it might be available.

During the activation of a LAN device behind a gateway using Zero Touch, if the LAN device is managed without a STUN server and is using only NAT, then a Port Mapping action will be queued to the gateway. At the same time in parallel, the OSS will be notified of this LAN device registration via the Device Registration notification. When the OSS calls HDM back with a `registerDevice()`, HDM will attempt to complete the LAN device activation by issuing a Connection Request to the LAN device. If this happens before Port Mapping is successfully executed and its result is successfully processed, HDM will not have the NAT CR URL ready; for this reason, a Connection Request to the LAN device cannot be issued effectively.

The new SCE property `nbi.notification.registration.landevice.delay.seconds` can be used to introduce a delay in HDM sending the Device Registration notification to the OSS. This way, the Port Mapping can be given a chance to complete first, so that when OSS is notified, the NAT CR URL for the LAN device is available and can be used to complete the LAN device activation sequence in a much more timely manner.

# To understand the SCE property alcatel.cr.retries behavior change

In order to fix defect `65847: HDM does not issue retries up to the number specified by alcatel.cr.retries`, the behavior of the SCE property `alcatel.cr.retries` has been changed. It now reflects the additional attempts beyond the initial attempt HDM will make to contact a device. This property functions at a high level, dictating how many times HDM will go through the process of attempting to contact a device. Each iteration of this process may result in more than one actual HTTP connection attempt being made to the device. These additional HTTP connection attempts are dictated by the SCE property`alcatel.cr.http.retries`.

An additional SCE property `alcatel.cr.http.retries` has been added. This parameter defaults to a value of 3. This property dictates how many additional HTTP connection attempts will be made to a device per HDM attempt to contact the device.

`alcatel.cr.retries` reflects how many additional times beyond 1 that HDM will attempt to contact a device.

`alcatel.cr.http.retries` reflects how many actual HTTP connection attempts will be made per HDM connection request iteration.

## Best Effort CR

Max CR attempts = (1 + alcatel.cr.retries) * (1 + alcatel.cr.http.retries)

## Real Time CR

If alcatel.cr.retries==0 Max CR attempts = (1 * (1 + alcatel.cr.http.retires) )

If alcatel.cr.retries>0 Max CR attempts = (1 * (1 + alcatel.cr.http.retires) ) + ( (1 + alcatel.cr.retries) * (1 + alcatel.cr.http.retires) )

# To understand the new SCE property hdm.managementconsole.disable.policycreate.realtime.cr

This SCE property has been added to prohibit the creation of new policies using a real-time connection request. This property was implemented to help eliminate the possibility of operator error in enabling real-time connection request for large policy runs and it functions system wide for all users. The property works by disabling the check box to select **Use Real-Time Connection Request** in the policy window.

After this SCE property is set to **true**, the check box will be unchangeable and the current state of real-time connection request on any existing policy cannot be changed. For this reason, customers must edit the state of the **Use Real-Time Connection Request** check box for any existing policy to be in the desired state. Once the checkbox is set to the

desired state for all policies, this SCE parameter can be set to **true** to prohibit the creation of any new policies that have the **Use Real-Time Connection Request** setting.

## To understand the new tag <cachedParameters> for filtering parameters

To address HDM-2525, a new tag <cachedParameters> has been established. The tag filters the device parameters to be cached per device type (NOT per device). This avoids unnecessary cluttering of the PARAMETERVALUE table. If the tag is not set, all of the parameters are cached. The filtering is done for both Device Action Results – GetParameterValues, SetParameterValues, GetParameterAttributes, SetParameterAttributes, AddObject, or DeleteObject – and Informs. White listing of parameters is preferred over black listing. A new table in the database called CACHED_PARAMETER stores the filtered parameters. A sample use of the new tag is shown below:

```
<cachedParameters>

 <parameterName>InternetGatewayDevice.DeviceInfo.HardwareVersion</parameterName>
 <parameterName>InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.↲
WANPPPConnection.{i}.MACAddress.{i}</parameterName>
 <parameterName>InternetGatewayDevice.DeviceInfo.SoftwareVersion</parameterName>
 <parameterName>InternetGatewayDevice.ManagementServer.PeriodicInformInterval</↲
parameterName>
 <parameterName>InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.↲
WANIPConnection.</parameterName>

</cachedParameters> ↲
```

## To understand web service notification filtering based on Policy Class

**Description:**

To address HDM-2849, HDM now includes a web service notification filtering capability based on the **Class** of a policy. This capability is implemented through two new properties.

Web service endpoint subscription:

`nbi.notification.plugin.reference.eventtriggeredpolicyresult.policyClass.`*DataCollectionTag*`.urls`

Web service notification retry:

`nbi.notification.plugin.reference.eventtriggeredpolicyresult.policyClass.`*DataCollectionTag*`.retry`

where *DataCollectionTag* is the string entered as the **Class** of the data collection policies.

This capability enables users to collect data and monitor policies by obtaining the results of GPVs that are performed using specific event-triggered policies as identified by the user. Results of the data collection are sent through a web service notification to a custom web service. The custom web service can then save the results outside of the HDM database and process the results as needed.

**To implement this capability:**

1. For each event-triggered policy for which GPV data collection is desired, use the **New Policy** window of the HDM Management Console to set the **Class** parameter for the policy to a user-defined value; for example: `DataCollection`.

2. Establish the `nbi.notification.plugin.reference.eventtriggeredpolicyresult.policyClass.`*DataCollectionTag*`.urls` property, where *DataCollectionTag* is the value entered in the **Class** parameter for the policy.

3. Optionally, set the value of the corresponding retry property `nbi.notification.plugin.reference.eventtriggeredpolicyresult.policyClass.`*DataCollectionTag*`.retry`. By default, the value of the retry properties is false if the property is not added or does not exist. For details on how the web service notification retry properties work, see "Understanding web services notification retries" in the *HDM 3.0.0 Programming Guide*, 3JB-00029-ADAA-PCZZA.

**HDM behavior:**

Whenever an event-triggered policy contains a **Class** and that policy execution is completed on a given device, HDM checks for the presence of the `nbi.notification.plugin.reference.eventtriggeredpolicyresult.policyClass.`*DataCollectionTag*`.urls` property. If the property is present and if the **Class** parameter value matches the *DataCollectionTag*, HDM sends the results, `NBIEventTriggeredPolicyResult` notifications, of all event-triggered policies created for the purpose of data collection to the specified webservice endpoint. For details on setting up the web service notification capability, see the *HDM 3.0.0 Programming Guide*, 3JB-00029-ADAA-PCZZA.

Note that if the `nbi.notification.plugin.reference.eventtriggeredpolicyresult.policyClass.`*DataCollectionTag*`.urls` property is not established and if a policy contains a value for the **Class** parameter, HDM uses the existing property `nbi.notification.plugin.reference.eventtriggeredpolicyresult.urls` and performs appropriate processing based on that property.

# To save the CPE ACS username and password of failed authentications to a database table

Prior to implementation of HDM-2774, CPE failed authentications were logged in HDM authorization logs. In deployments with a very large number of devices and a large number of servers, it is now easier to process CPE failed authentication information because the username, password, and cause are saved in a separate database table.

The FAILED_LOGINS table previously held only the username, in the USERNAME column, for failed CPE authentications. This table has been enhanced to include two new columns: PASSWORD and CAUSE.

To implement this revised functionality, follow the instructions in "To prepare for the Home Device Manager update", "To update the database schema", and "To install the updated CPE Authenticator jar file" section.

# To roll back your Home Device Manager hotfix

1. Before uninstalling components on a Solaris host:

   a. Be sure to preserve the backup you created from your existing installation during the initial hotfix installation; that is, do not overwrite that backup with a new backup.

   b. Back up all data in the Home Device Manager OLTP database.

   c. Create a current backup image of the Home Device Manager host.

2. Block all northbound and southbound traffic to servers by stopping the Home Device Manager application. This is described in Step 4 of the section "To prepare for the Home Device Manager update".

3. On each managed server, replace `ala-nbi-notification-plugins.jar` with the backup that you made prior to upgrade.

4. Using SQL*Plus, connect to the Home Device Manager database instance and restore the old version information.

   a. Log in to the database instance:

      `sqlplus` *hdm_dbuser/password@net_service_name* where:

   - *hdm_dbuser* is the user name for the Home Device Manager OLTP schema owner account.
   - *password* is the password for the Home Device Manager OLTP schema owner account.
   - *net_service_name* is the net service name of the database instance.

   b. Issue the following SQL commands (edit the indicated values below appropriately):

```
SQL> DELETE from version_info where productversion = '<this_hotfix_version>↵
';
 SQL> UPDATE ConfigurationItem
 SET value='<version_before_hotfix>' WHERE
 name='hdm.product.display.version';
 SQL> commit;
 SQL> exit;
```

# Installation instructions for Traffic Manager

Depending on the hardware architecture selected, the appropriate binaries of the Traffic Manager Installer. The binaries for Sun SPARC will be available in Traffic-Mgr_3.0.3.2/solaris-sparc and the binaries for Intel-x86 will be available in Traffic-Mgr_3.0.3.2/solaris-x86. For further installation instructions, see the installation section of the *Traffic Regulation Module Deployment Guide, version 3.0.3*.

# Support and contact information

If you encounter issues with this product, visit the Online Customer Support (OLCS) [http://support.alcatel-lucent.com] website. After registering and logging on, you can access troubleshooting resources.

In addition, you can contact Alcatel-Lucent Support as follows:

- Toll-free phone (within U.S.): 1-866-582-3688, option 1
- Outside U.S.: +1 613 784 6100 (United States)

Alcatel-Lucent is interested in feedback about your experience with this product and its documentation. If you have comments or suggestions, send email to pubs@motive.com [mailto:pubs@motive.com].

# Legal notice



**Document number:** 3JB-00056-ARAA-PCZZA-01 **Issue date:** February 2012