HARMONY

05 December 2023

HARMONY MOBILE CONNECTOR

Installation Guide

CHECK POINT™

Check Point Copyright Notice

© 2022 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.



Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.



Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
05 December 2023	Updated the link to download Harmony Mobile Connector package in *"Prerequisites" on page 8*.
18 October 2023	Updated the link to download Harmony Mobile Connector package in *"Installing and Configuring Harmony Mobile Connector" on page 11*.
15 May 2023	Added TLS update in *"Installing and Configuring Harmony Mobile Connector" on page 11*.
9 February 2023	Added port details for India region in *"Prerequisites" on page 8*.
29 November 2022	Updated *"Related Documents" on page 37*.
25 November 2022	First release of this document.

Table of Contents

Introduction to Harmony Mobile Connector ... *6*
Solution Architecture ... *6*
Prerequisites ... *8*
Installation ... *10*
Installing Gaia ... *10*
Installing and Configuring Harmony Mobile Connector ... *11*
Configuring the Connector in Harmony Mobile Administrator Portal ... *19*
Advanced Configuration ... *31*
Migrating Encryption Keys from User Device Management (UDM) to Connector ... *31*
Setting up an On-Premises SMTP Service (without UEM) ... *31*
Working with a Proxy ... *32*
Using a UEM with a Self-Signed Certificate ... *33*
Setting up High Availability for the Connector ... *34*
Viewing Connector ... *34*
Upgrading Harmony Mobile Connector from R80.XX to R80.40 ... *34*
Saving the Encrypted MDM Password ... *35*
Related Documents ... *37*

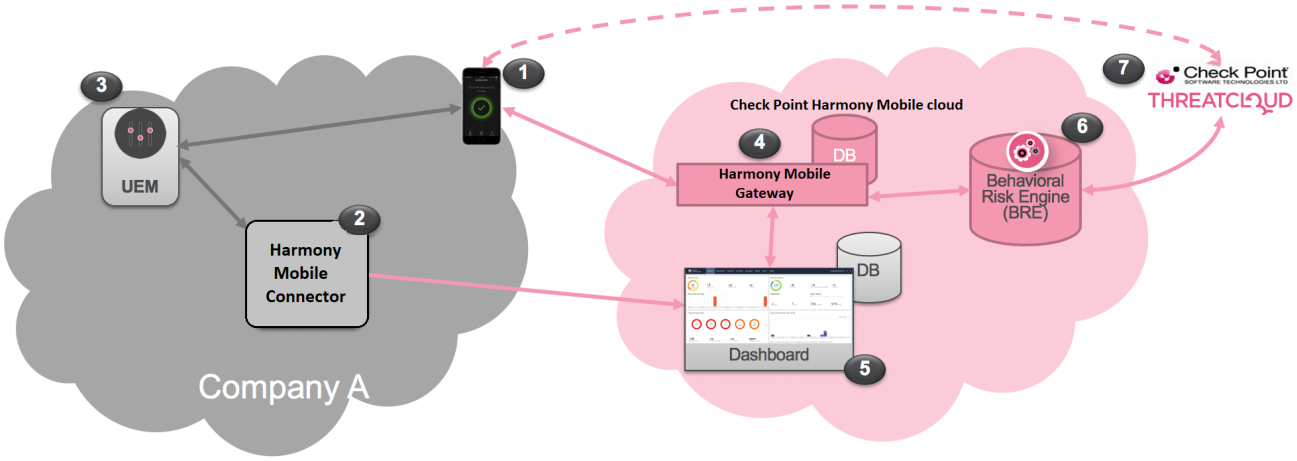
Introduction to Harmony Mobile Connector

Harmony Mobile Connector (previously known as SandBlast Mobile Connector) is a web-based application that integrates your Harmony Mobile dashboard and your on-premises Unified Endpoint Management (UEM) solution.

To secure the user Personally Identifiable Information (PII) within your organization's environment, the Connector populates the Harmony Mobile dashboard with encrypted hash values instead of plain text for the device / user name, user email address, and device phone number.

This document describes how to install the Harmony Mobile Connector and provides the configuration instructions for different deployment scenarios.

Solution Architecture



	Component	Description
1	Harmony Mobile Protect App	■ The Harmony Mobile Protect App is a lightweight app for iOS® and Android™ that gathers data and helps analyze threats to devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the solution, which it uses to identify suspicious or malicious behavior. ■ To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects. ■ The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience. ■ No Personal Information is processed by or stored in the App.

	Component	Description
2	Harmony Mobile Connector	■ Harmony Mobile Connector is a proxy application that resides within the organization's data center that provides an integration interface between your Harmony Mobile dashboard and your on-prem services. Supported on-prem services are UEM and SMTP.
3	UEM	■ Unified Endpoint Management ■ Device Management and Policy Enforcement System (generalized term to replace MDM/EMM).
4	Harmony Mobile Gateway	■ The cloud-based Check Point Harmony Mobile Gateway is a multi-tenant architecture to which mobile devices are registered. ■ The Gateway handles all solution communications with enrolled mobile devices and with the customer's (organization's) dashboard instance. ■ No Personal Information is processed by or stored in the Gateway.
5	Management Dashboard	■ The cloud-based web-GUI Check Point Harmony Mobile Management dashboard enables administration, provisioning, and monitoring of devices and policies and is configured as a per-customer instance. ■ The dashboard can be integrated with an existing UEM solution for automated policy enforcement on devices at risk. ■ When using this integration, the UEM serves as a repository with which the dashboard syncs enrolled devices and identities. ■ Personal Information[1], such as user name, email address, and phone number, is processed by and may be stored in the dashboard.
6	Behavioral Risk Engine	■ The cloud-based Check Point Harmony Mobile Behavioral Risk Engine uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis. ■ The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity. ■ The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected. ■ No Personal Information[1] is processed by or stored in the Engine.
7	ThreatCloud	■ ThreatCloud powers the Anti-Phishing, Safe Browsing, and URL Filtering technologies for Harmony Mobile.

Prerequisites

1. Download Check Point R80.40 (Virtual Machine installation). For more information, see sk160736.

   The Gaia operating system is based on 64-bit Linux Red Hat 7.
2. Download the Harmony Mobile Connector installation file - HMC R80.40 T17.
3. Create a new Virtual Machine (VM) with these specifications:
   - Cores - 4
   - Memory - 4GB
   - Disk space - 200GB
4. IPs and ports required to connect the Harmony Mobile Connector:

Description	Source	Destination	Port	Region
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	Harmony dashboard URL 52.87.59.245	443	US
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	Harmony dashboard URL 52.17.79.161	443	EU
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	Harmony dashboard URL 13.237.221.74	443	AU
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	us-relay.locsec.net	443	US
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	eu-relay.locsec.net	443	EU
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	uk-relay.locsec.net	443	UK
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	au-relay.locsec.net	443	AU
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	ca-relay.locsec.net	443	CA
Connection to Harmony Mobile	Customer Harmony Mobile Connector server	in-relay.locsec.net	443	IN

Description	Source	Destination	Port	Region
Connection to Customer UEM	Customer Harmony Mobile Connector server	Customer UEM	443 BlackBerry UEM only: 18084	ANY

Installation

Installing Gaia

To install a VM with R80.40 version:

1. Install Gaia on an open server or on a server that was upgraded from a previous Gaia version. For instructions, see:

   https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_Installation_and_Upgrade_Guide/Topics-IUG/Getting-Started.htm

2. Run the Gaia First Time Configuration Wizard. For instructions, see:

   - https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_Installation_and_Upgrade_Guide/Topics-IUG/Running-FTCW-in-Gaia-Portal.htm?Highlight=First%20Time%20Configuration%20Wizard
   - sk69701

   Note - Gaia for Harmony Mobile Connector does not require a separate license. It is part of the Harmony Mobile license agreement.

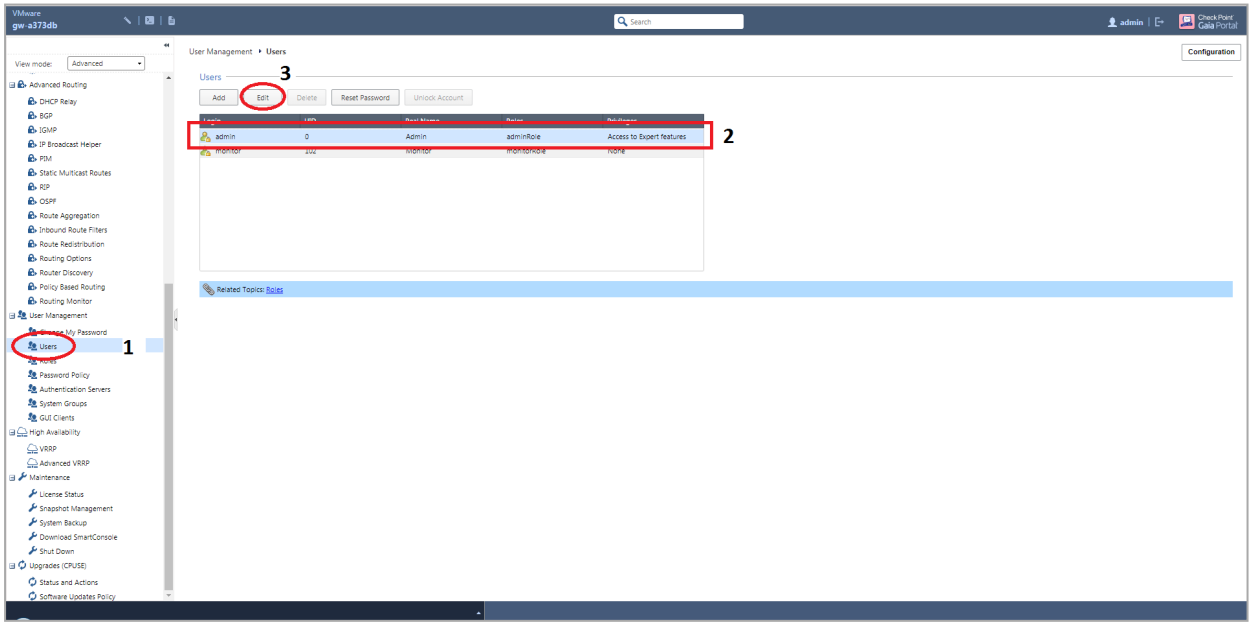
After you install the VM, change the admin user to use `bash`:

1. Log in to Gaia: `https://<gaia_vm_ip>`

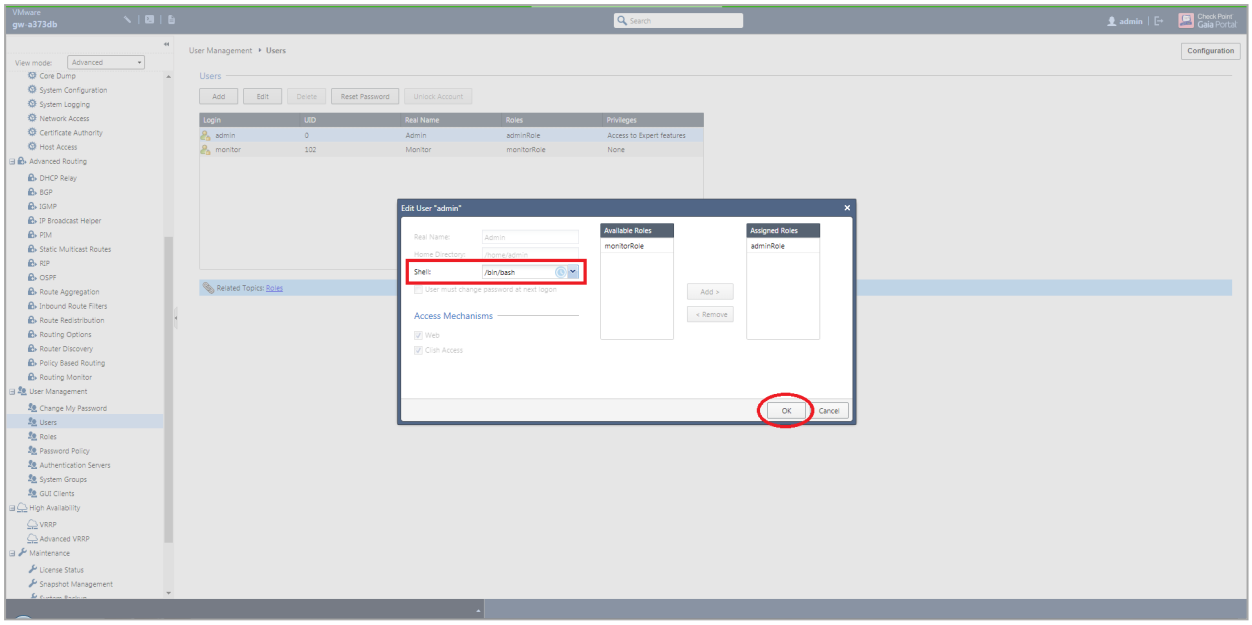
   Username - admin

   Password - The password set when you installed Gaia.

2. Under **User Management**, click **Users**.
3. Select your admin user and click **Edit**.



4. Change **Shell** to `/bin/bash` and click **OK**.



Installing and Configuring Harmony Mobile Connector

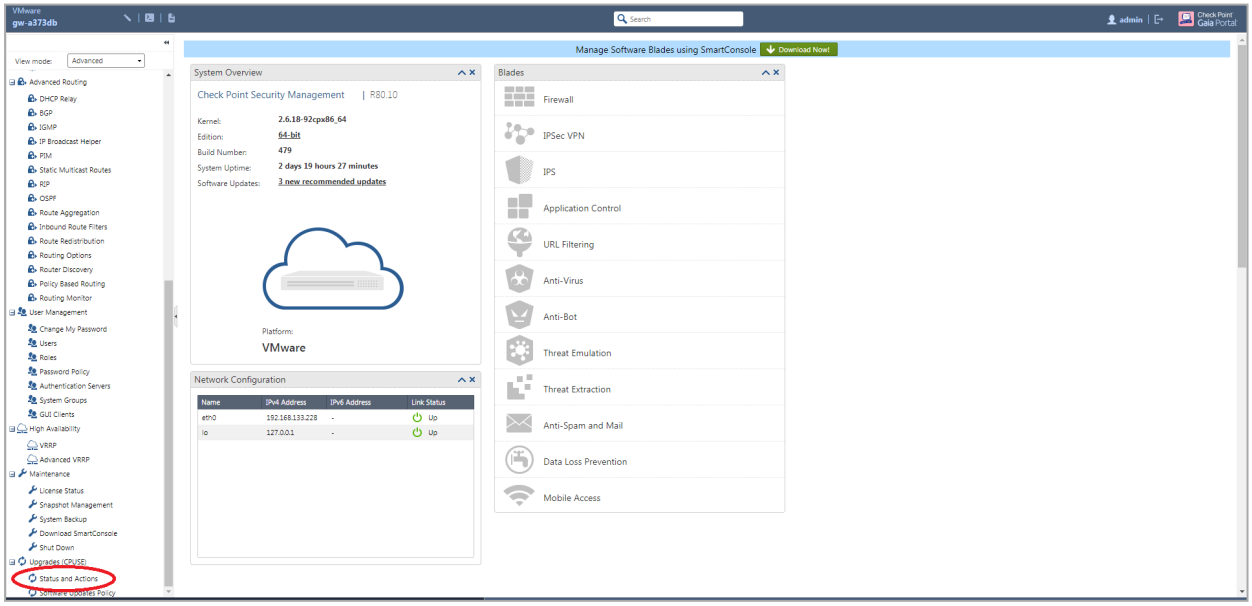
To install the Harmony Mobile Connector package:

1. Log in to Gaia: `https://<gaia_vm_ip>`

   Username - admin

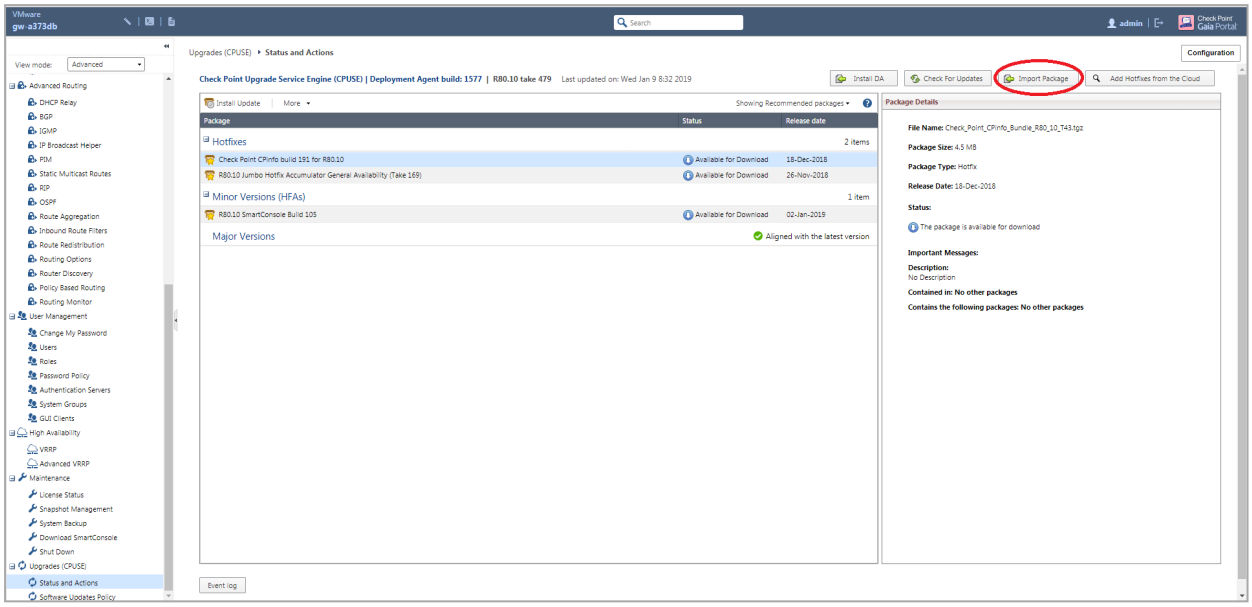
   Password - The password set when you installed Gaia.

2. On the left pane, under **Upgrades (CPUSE)**, click **Status and Actions**.

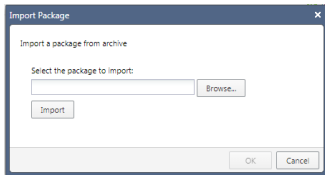


3. Click **Import Package**.

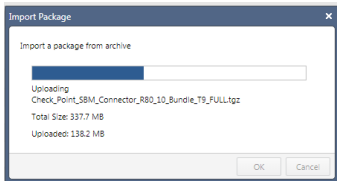
   To download the Harmony Mobile Connector package, click HMC R80.40 T17.



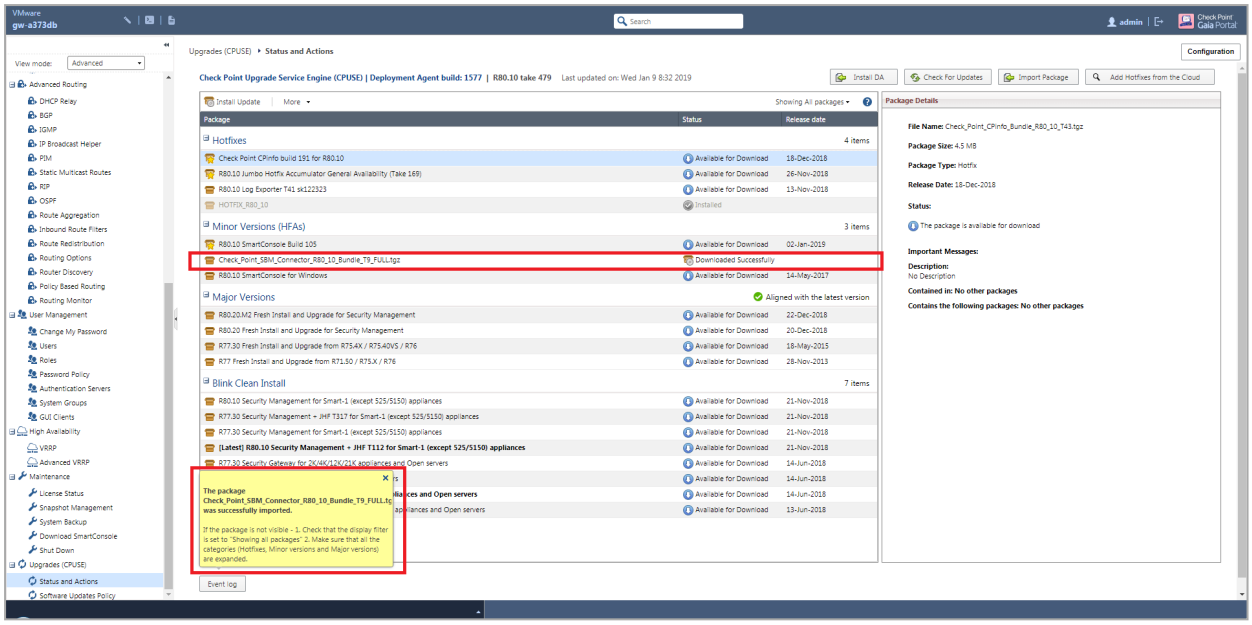
4. In the **Import Package** window, browse and select the Harmony Mobile Connector package downloaded in step 3 and click **Import**.



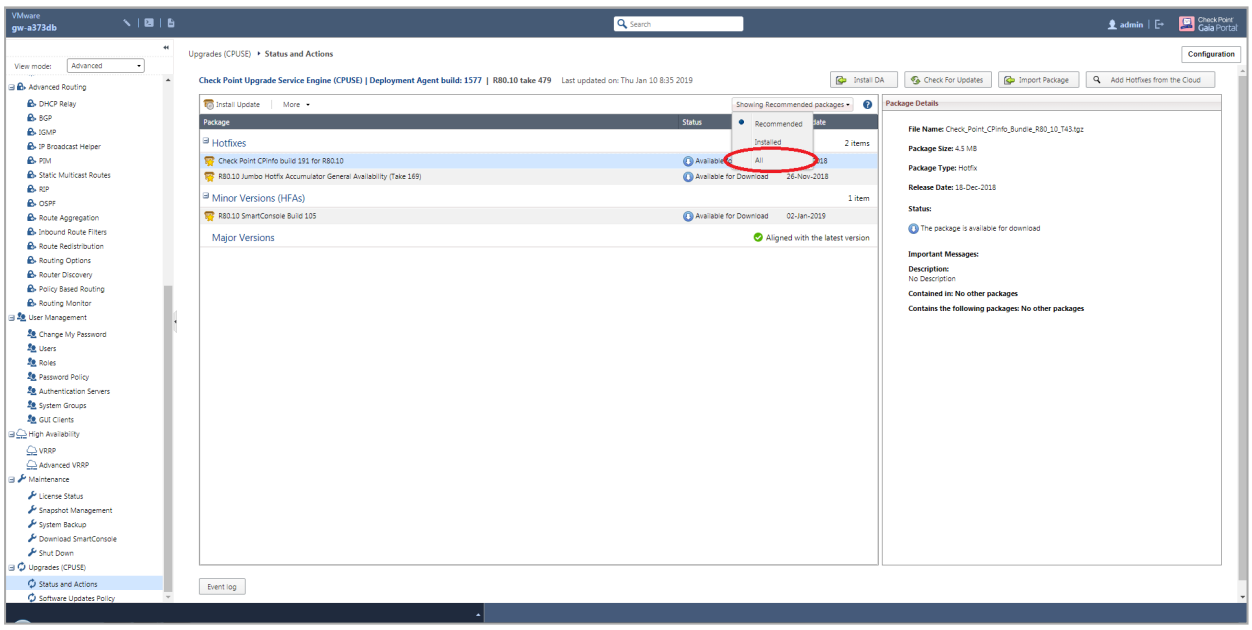
   Wait for the upload and import to finish.



When the import is completed, a message appears in the bottom left corner of the screen.

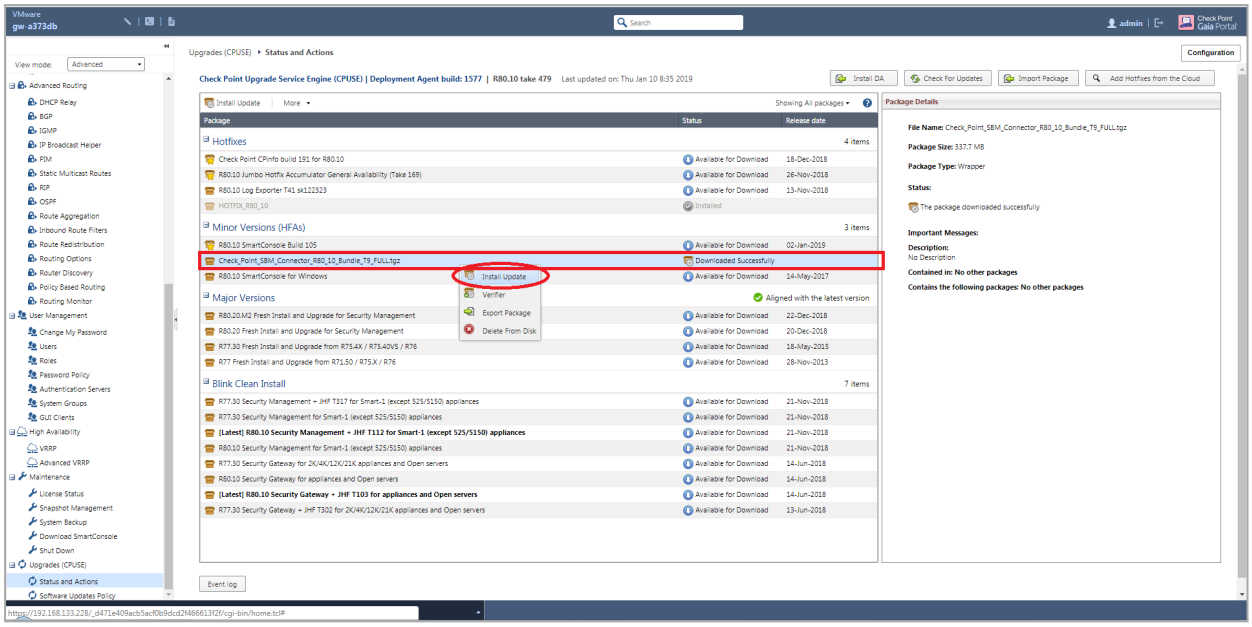


5. To view the imported package, under **Showing Recommended Packages**, select **All**.

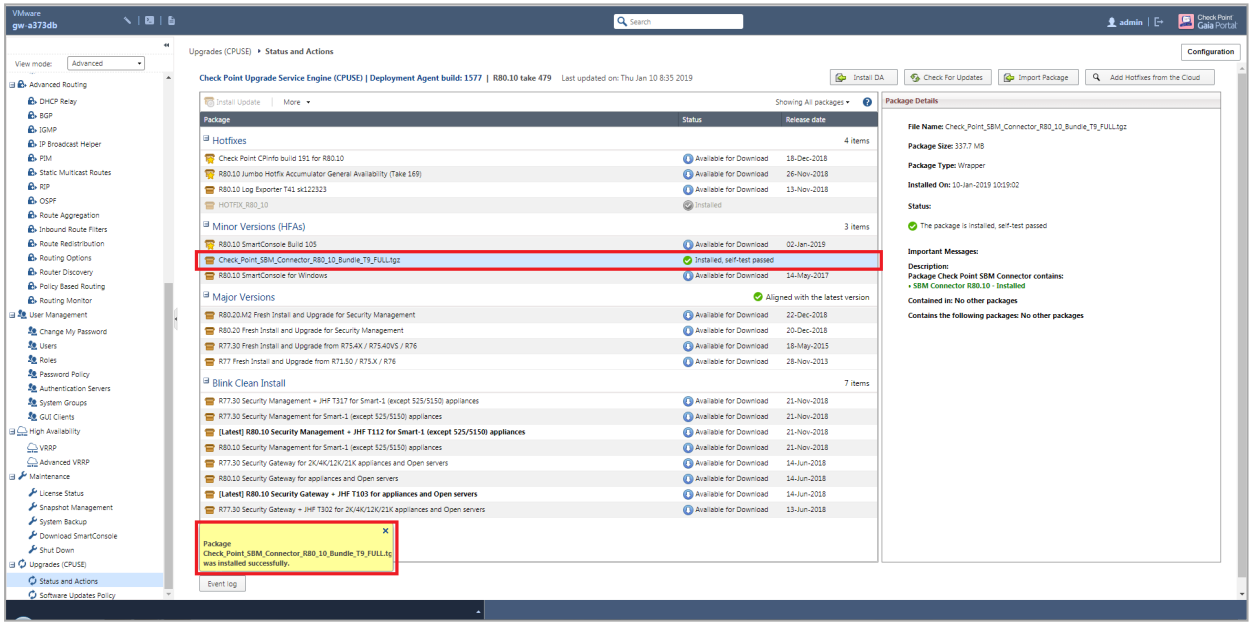


The imported Harmony Mobile Connector package is listed under **Minor Versions (HFAs)**, with **Downloaded Successfully** status.

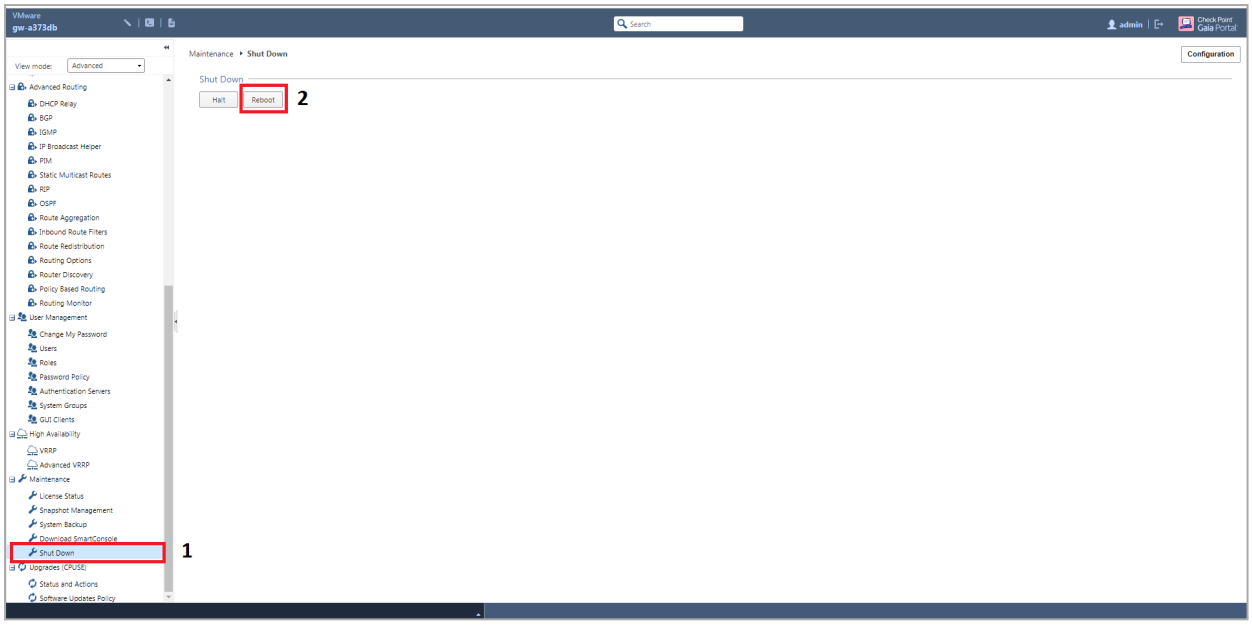
6. Right-click the package and select **Install Update**.



When the installation completes, the package status changes to **Installed** and a message appears in the bottom left corner.



7. Under **Maintenance**, click **Shut Down** > **Reboot**.



TLS update:

Update Transport Layer Security (TLS) to version 1.2. To update, follow the steps 1 to 5 in sk176289.

Important Note - TLS update is a mandatory step for Harmony Mobile Connector installation.

To configure the Harmony Mobile Connector:

1. Connect to the VM through `ssh` and your initial credentials in Expert mode.
2. To create private and public keys, run:

   ```
   sbmc_create_keys
   ```

   Sample output:

   ```
   [Expert@gw-a373db:0]# sbmc_create_keys
   Started creating the SandBlast Connector keys
   ..................................++
   ..........................................................................................................................++
   writing RSA key
   SandBlast Connector keys creation finished successfully
   ```

3. Copy the public key for the Harmony Mobile dashboard configuration:

   ```
   cat /web/conf/sbmc_public_key.pub
   ```

4. Open the settings file `vi /opt/CPsbmc/components/api_dispatcher/application.yml`, and update these:

   - Configure Relay settings:

     ```
     relay:
         url: <Relay URL according to the region>
         task_info_key: <Harmony Mobile dashboard URL (without https)>
     ```

     Example:

     ```
     relay:
         url: https://us-relay.locsec.net
         task_info_key: "my.dashboard.checkpoint.com"
     ```

   - Update pii filter_url:

     ```
     pii:
         filter_url: "http://localhost:7777/"
     ```

   - Update private_key_path:

     ```
     signature:
         private_key_path: "/web/conf/sbmc_private_key.pem"
     ```

- Configure on-premises UEM credentials if you need to store the UEM login credentials in the Connector configuration.

  (You can also configure the UEM in the Infinity Portal. For more information, see Integrate UEM with Connector)

  Note - When you update the MDM credentials in the `application.yml` file, remove only the # sign from the updated rows and the credentials keyword row. Verify the structure is as follows:

  ```
  mdm:
   credentials:
      <relevant MDM credentials>
  ```

  - **XenMobile Basic Authentication**:

    MDM credentials:

    ```
    username: <username>
    password: <encrypted password>
    URL: <Server URL>
    mdmType: "xenmobile"
    ```

  - **XenMobile Bearer Token Authentication**:

    MDM credentials:

    ```
    customer_id: <customer id>
    client_id: <client id>
    secret_key: <encrypted secret key>
    URL: <Server URL>
    mdmType: "xenmobile"
    ```

  - **BlackBerry UEM**:

    MDM credentials:

    ```
    username: <username>
    password: <encrypted password>
    URL: <Server URL>
    provider: <provider> (most probably "AD")
    domain: <domain>
    SRPID: <SRP ID>
    mdmType: "bbuem"
    ```

  - **Airwatch**:

    MDM credentials:

    ```
    username: <username>
    password: <encrypted password>
    URL: <Server URL>
    aw-tenant-code: <API KEY>
    mdmType: "airwatch"
    ```

- **MobileIron Core**:

  MDM credentials:

  ```
  username: <username>
  password: <encrypted password>
  URL: <Server URL>
  mdmType: "mobileiron"
  ```

- **JAMF**:

  MDM credentials:

  ```
  username: <username>
  password: <encrypted password>
  URL: <Server URL>
  mdmType: "jamf"
  ```

- **Generic MDM (for example, Mdportsolution)**:

  MDM credentials:

  ```
  username: <username>
  password: <encrypted password>
  URL: <Server URL>
  mdmType: "generic"
  ```

- Configure on-premises SMTP:

  ```
  smtp:
      enable: true
      smtpSSLEnable: true (in case of SMTPS, port 465)
  ```

- Configure on-premises SYSLOG:

  ```
  syslog:
        enable: true
  ```

5. Update the pii protector settings

   ```
   vi /opt/CPsbmc/components/pii_protector/application.yml
   ```

   Update these fields:

   ```
   zuul:
       routes:
           proxy:
               url: <Harmony Mobile dashboard URL>
   ```

   Example:

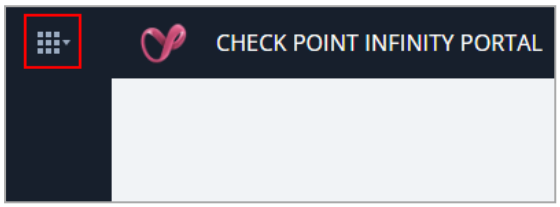
   ```
   zuul:
       routes:
           proxy:
               url: https://my.dashboard.locsec.net/
   ```

   Note - For the **Harmony Mobile dashboard URL**, enter the **Dashboard URL** value in the New Connector window. Add `https://` at the beginning of the URL and close it with a '/' character.

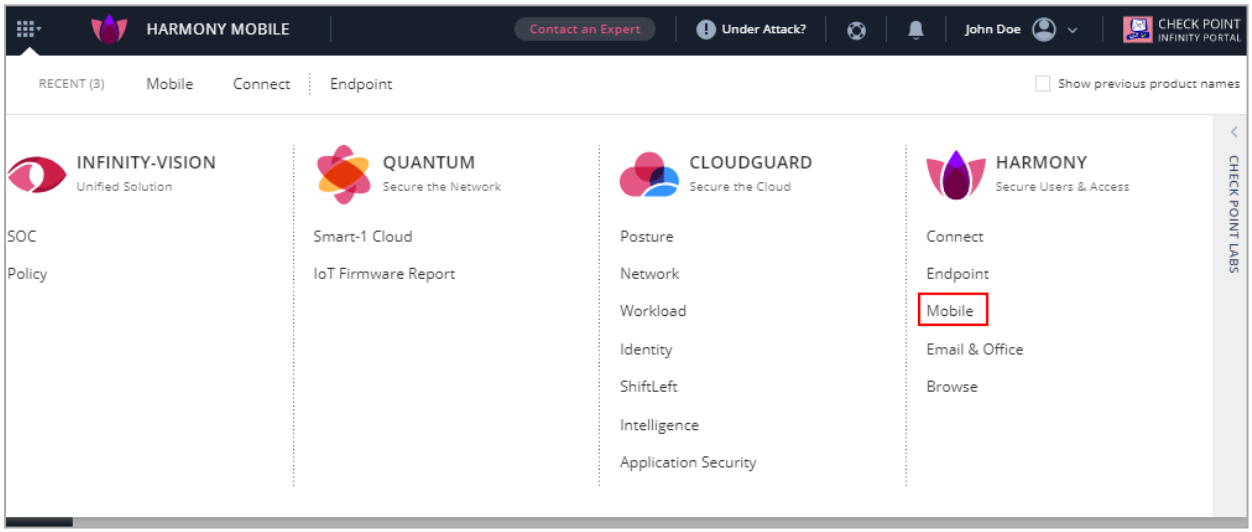
Configuring the Connector in Harmony Mobile Administrator Portal

To log in to the Harmony Mobile Administrator Portal:

1. Sign in to *Check Point Infinity Portal*.
2. Click the **Menu** button in the top left corner.



3. Under **Harmony**, click **Mobile**.

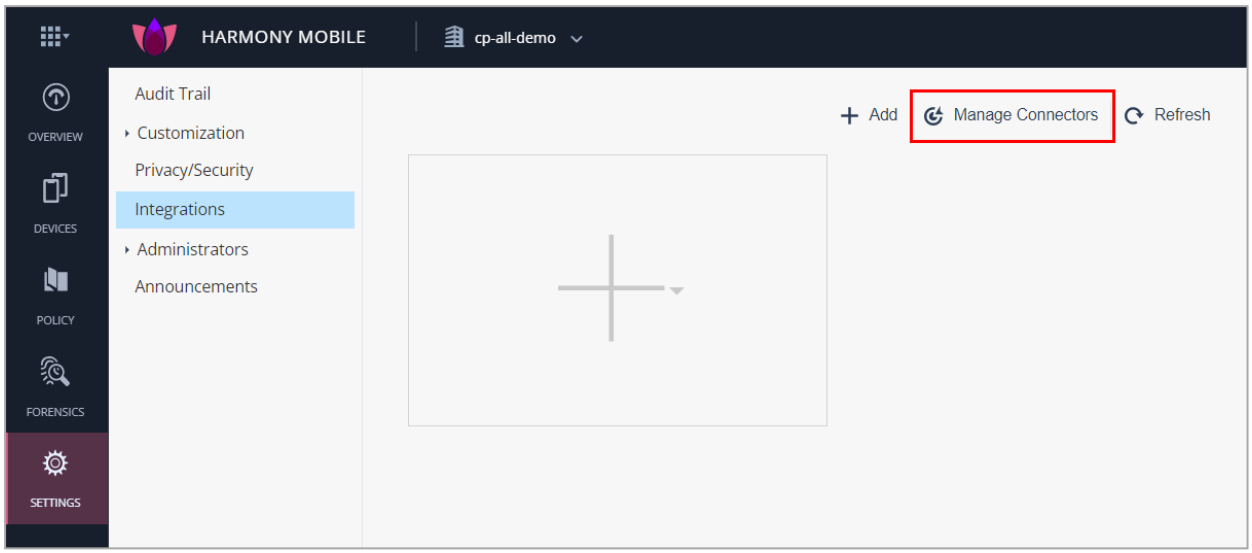


4. Accept the terms of service and click **Try Now** (Applies only for first-time login).

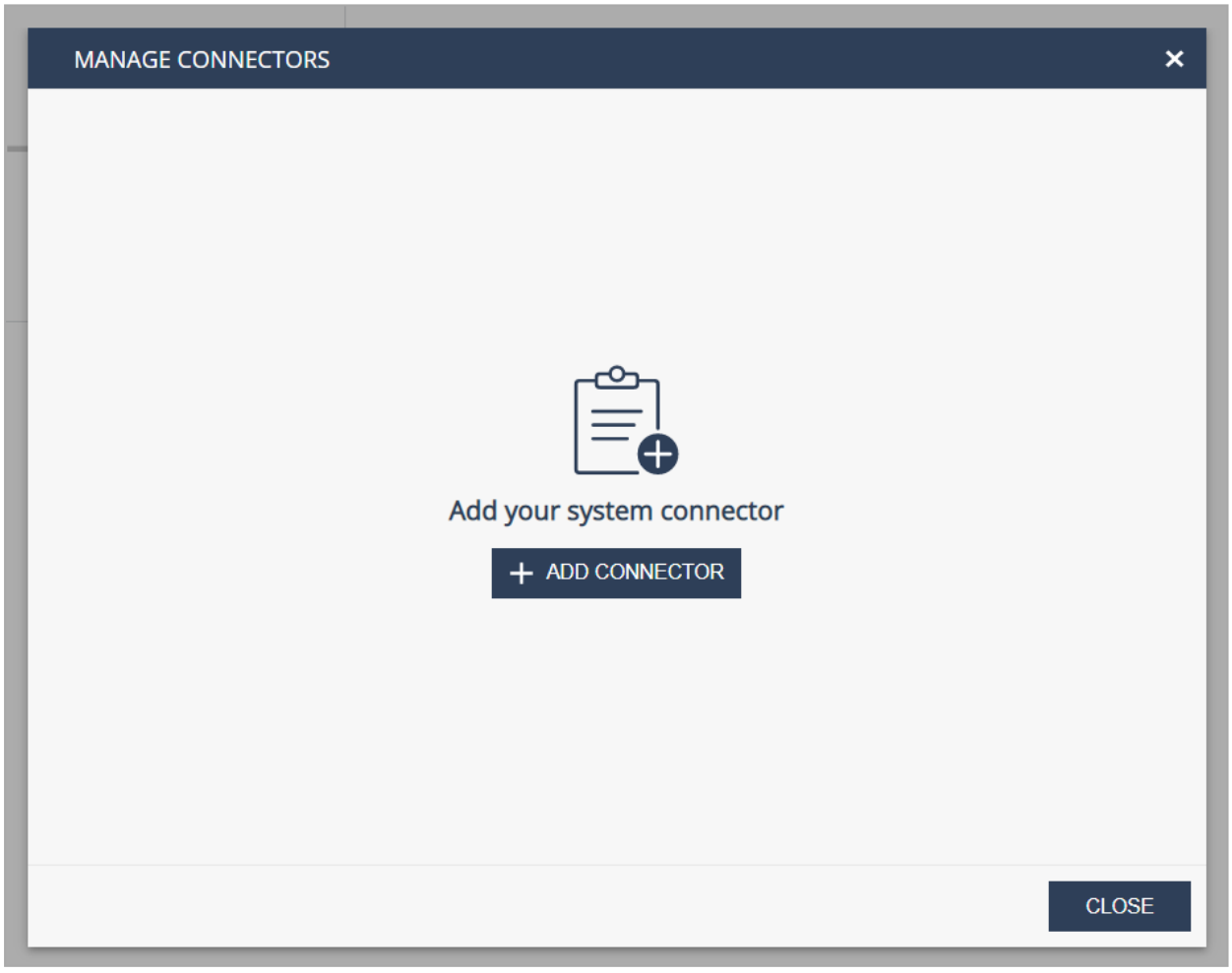
   The Harmony Mobile home page appears.

To configure a new Connector:

1. In the Harmony Mobile Administrator Portal, go to **Settings** > **Integrations**.
2. Click **Manage Connectors**.



3. In the **Manage Connectors** window, click **+Add Connector**.



4. In the **New Connector** window:

a. Enter a **Connector Name**.

b. Upload or copy and paste the public key from the Install and Configure Harmony Mobile Connector section.

c. In **Server Address** and in **HA Server Address** (optional), enter the Harmony Mobile Connector Virtual Machine address.

d. **Dashboard URL** is auto-generated and read-only.

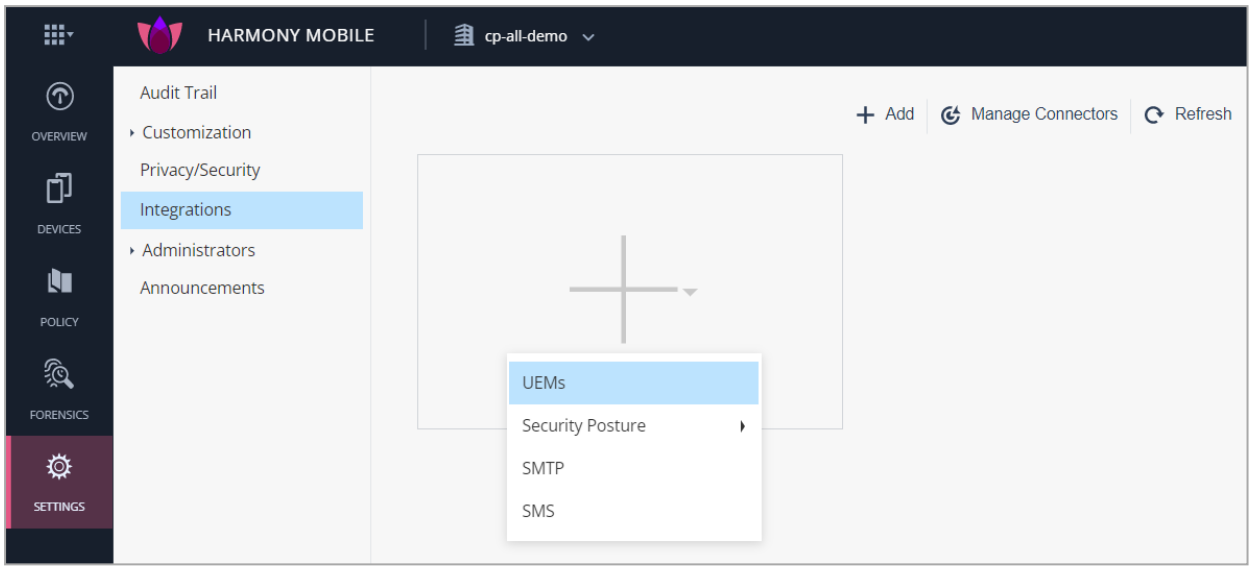
e. **(Optional) Directory Service** - Select this check box to configure directory service. To configure, see Configuring directory service.

f. Click **Create**.

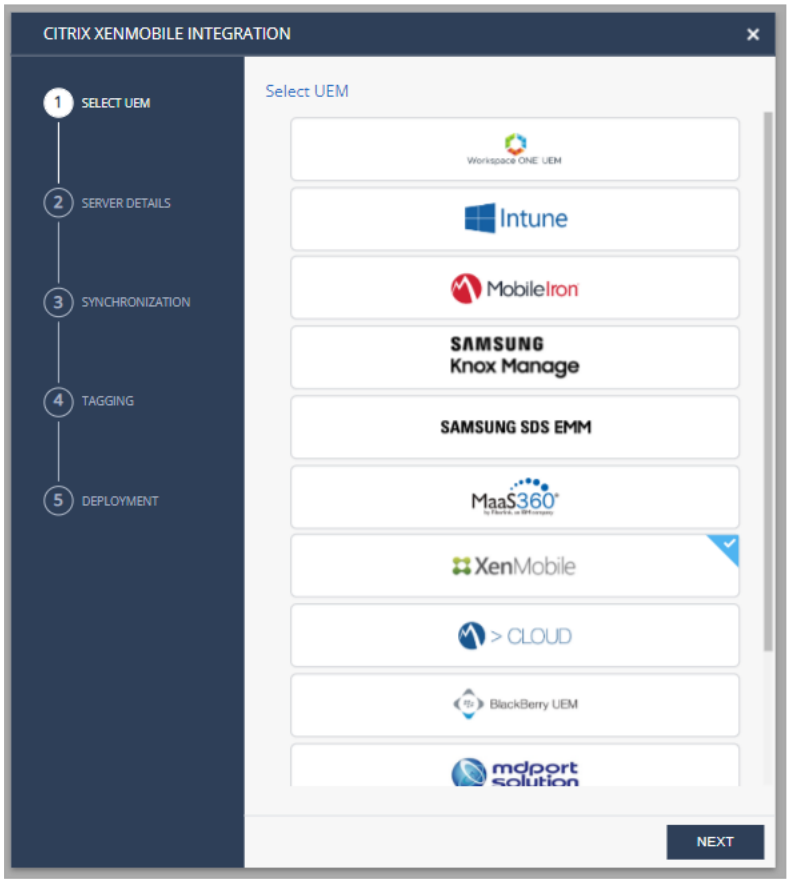


To integrate the UEM with Connector:

1. In the Harmony Mobile Administrator Portal, go to **Settings** > **Integrations**.
2. Click **+** and select **UEMs**.



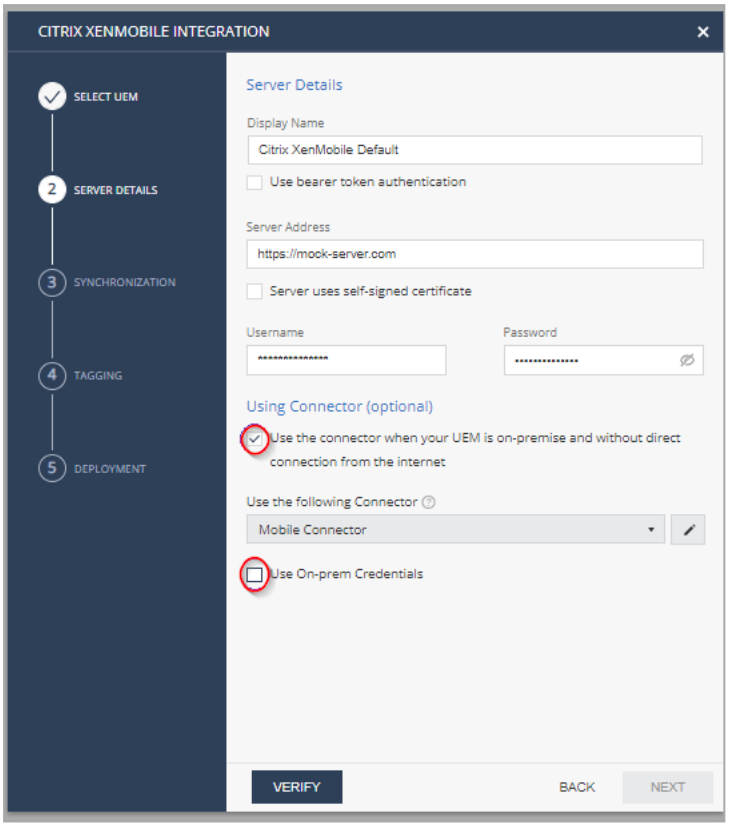
3. Select a UEM service and click **Next**.



4. In the **Server Details** tab, select the checkbox under **Using Connector** section.

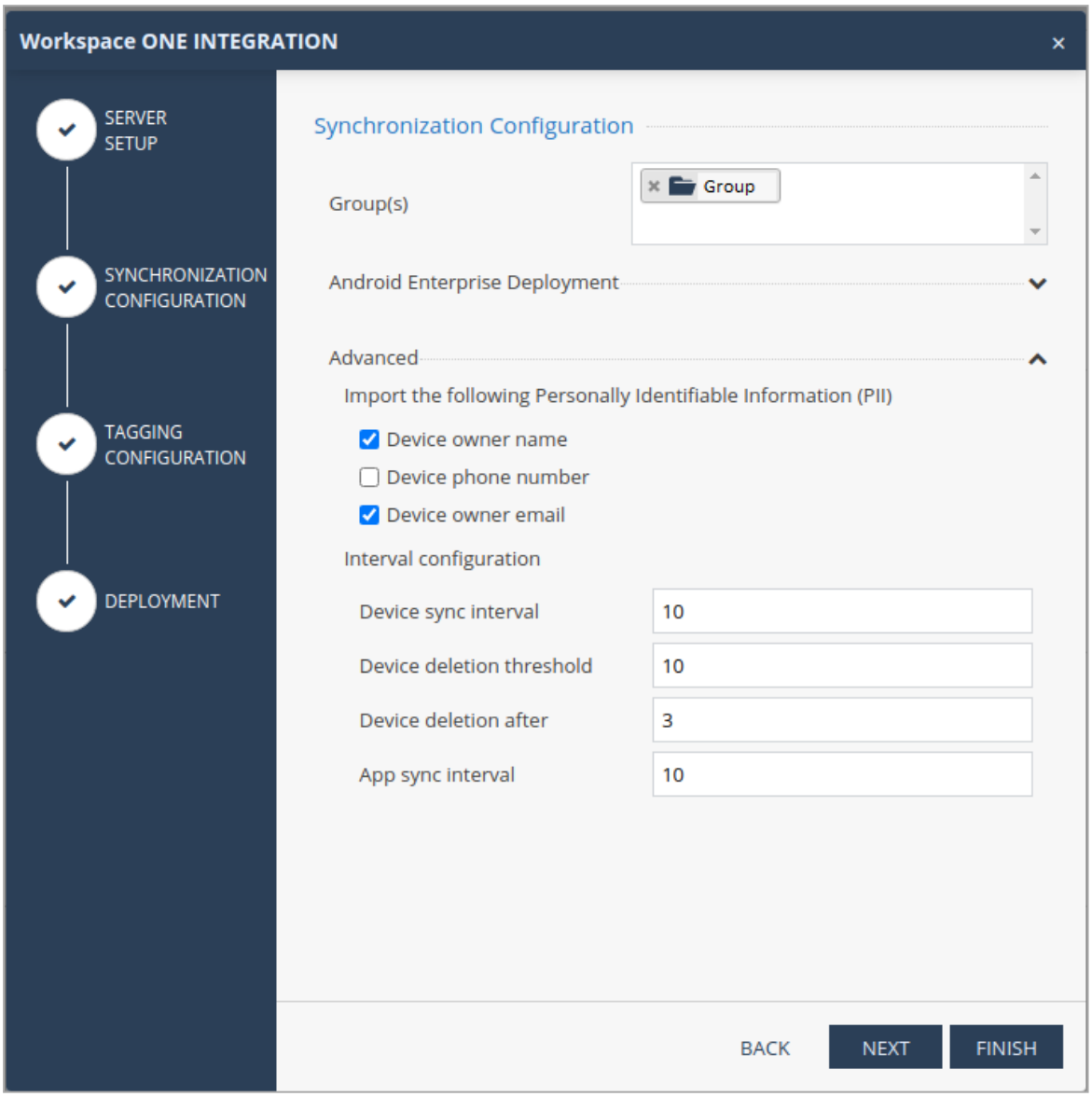
5. If the UEM login credentials are stored in the Connector configuration (see On-premises UEM login credentials), select the **Use On-prem Credentials** checkbox.

   Otherwise, enter the UEM server details.



6. Click **Verify** and **Next**.

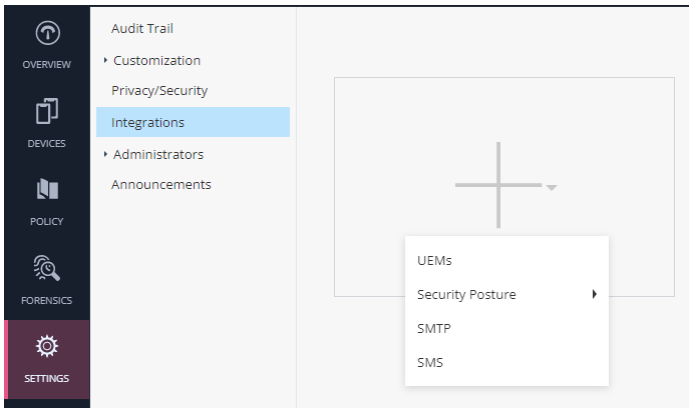
7. For on-premises SMTP support:
    a. Click the **Synchronization Configuration** tab.
    b. To import the device username and email address from the MDM, select the **Device owner name** and **Device owner email** checkboxes.



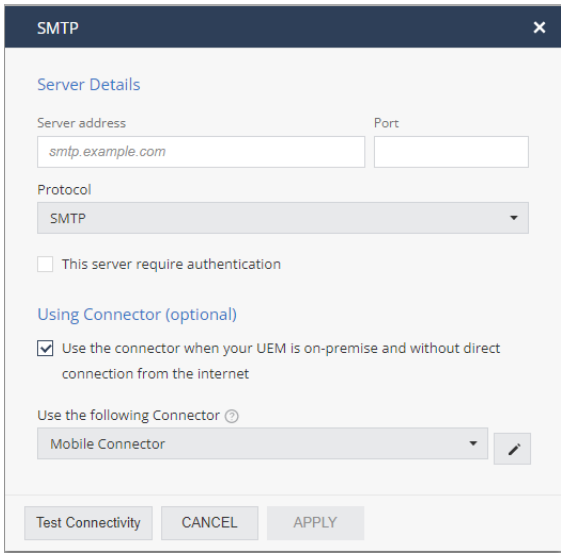
8. Click **Next** and **Finish**.
9. Verify these conditions:
    - The device is synchronized in UEM.
    - The device data appears as decrypted in the on-premises Harmony Mobile dashboard.

(Optional) For on-premises SMTP support:

1. In the Harmony Mobile Administrator Portal, go to **Settings** > **Integrations**.
2. Click **+** and select **SMTP**.



The **SMTP** window appears.



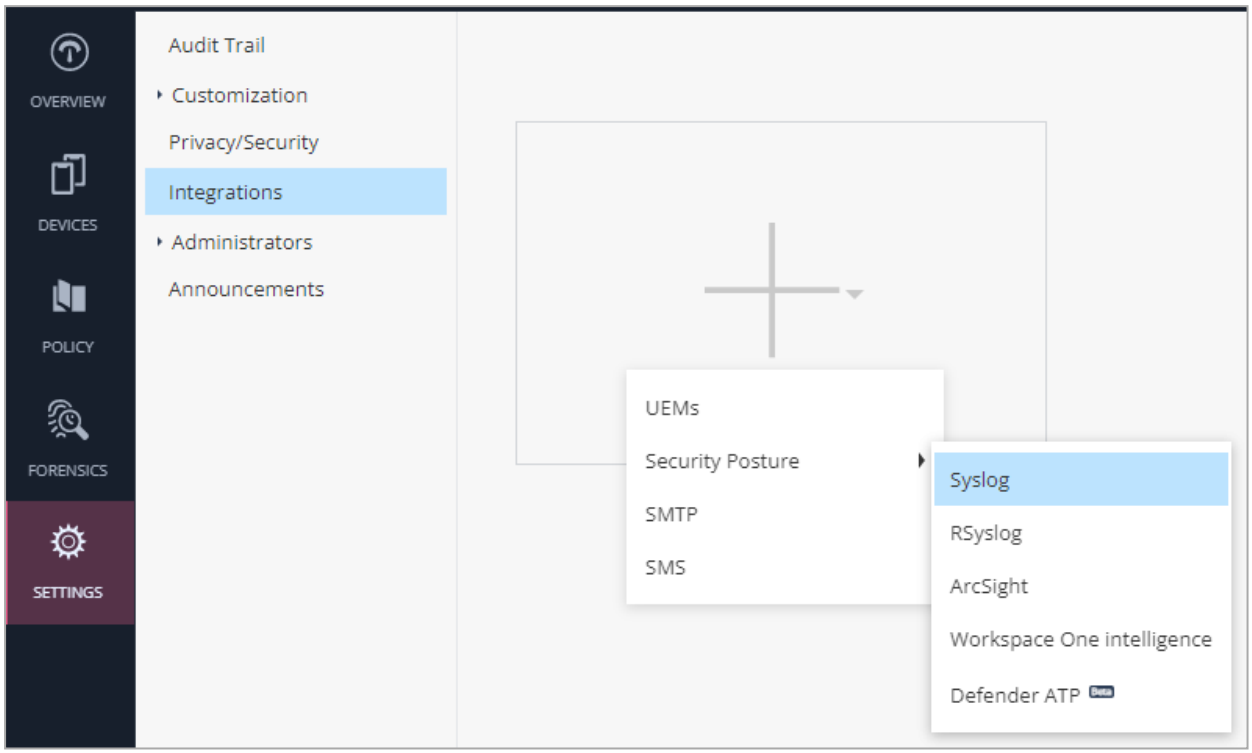
3. Configure **Server Details**:
   a. SMTP transport for ports 25 and 587.
   b. SMTPS transport for port 465.
4. To use the connector with an on-premises UEM without a direct internet connection, select the checkbox under **Using Connector** section.
5. Click **Test Connectivity**.

   If there are no errors, click **Apply**.

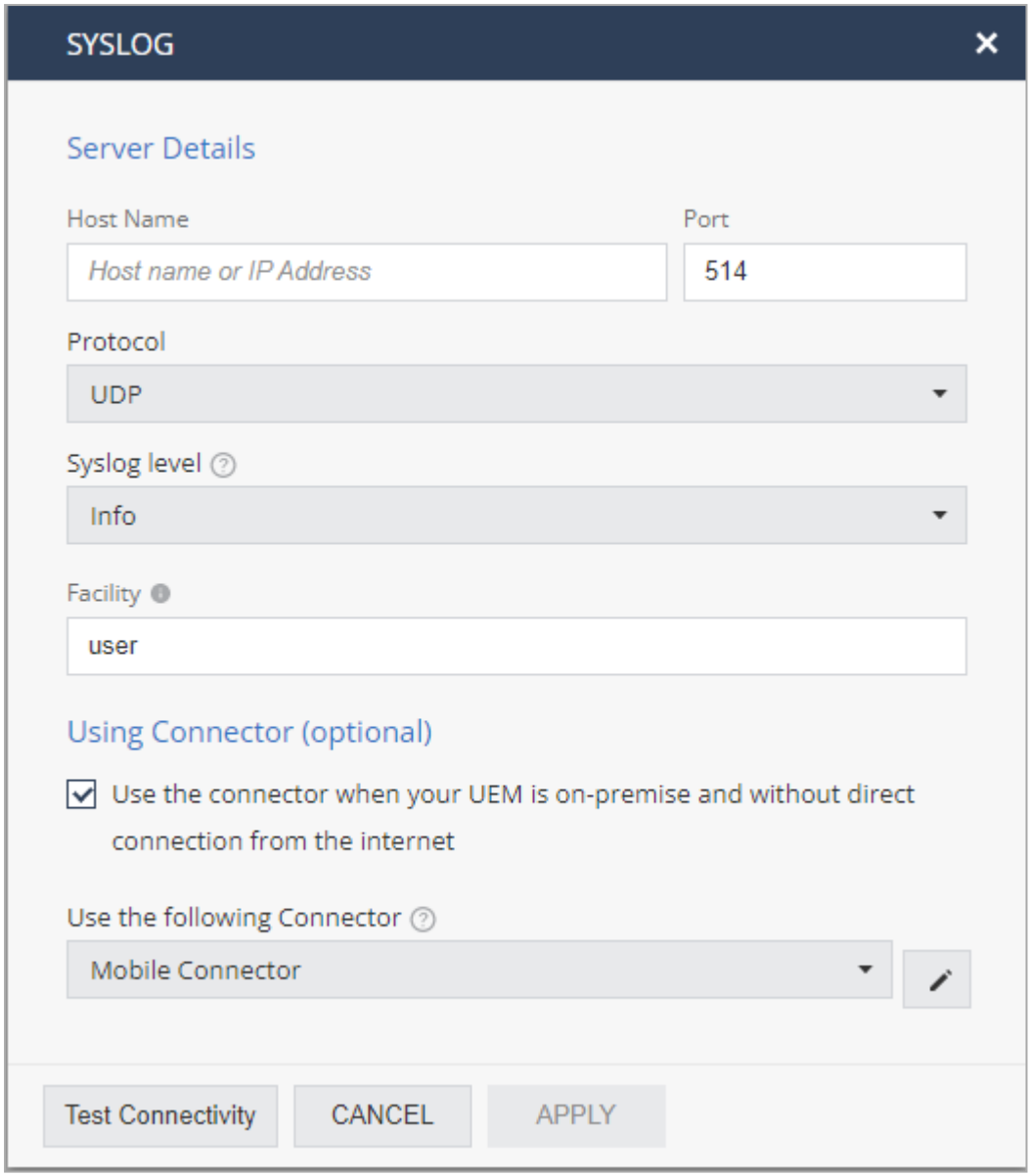
(Optional) For on-premises Syslog support:

1. In the Harmony Mobile Administrator Portal, go to **Settings** > **Integrations**.
2. Click **+** and select **Security Posture**.

   Select **Syslog** or **ArcSight**. The **Syslog** window appears.



3. Configure Syslog **Server Details**.



4. To use the connector with an on-premises UEM without a direct internet connection, select the checkbox under **Using Connector** section.
5. Click **Test Connectivity**.
6. If there are no errors, click **Apply** and then **Save**.
7. Verify these conditions:
   - The device is synchronized in UEM.
   - The device data appears as decrypted in the on-premises Harmony Mobile dashboard.

(Optional) Configuring the directory service:

The Harmony MobileConnector directory service enables you to search the Active Directory (AD) using LDAP, and to enroll users to Harmony Mobile.

Open and update this settings file:

```
vi /opt/CPsbmc/components/directory_service/application.yml
```

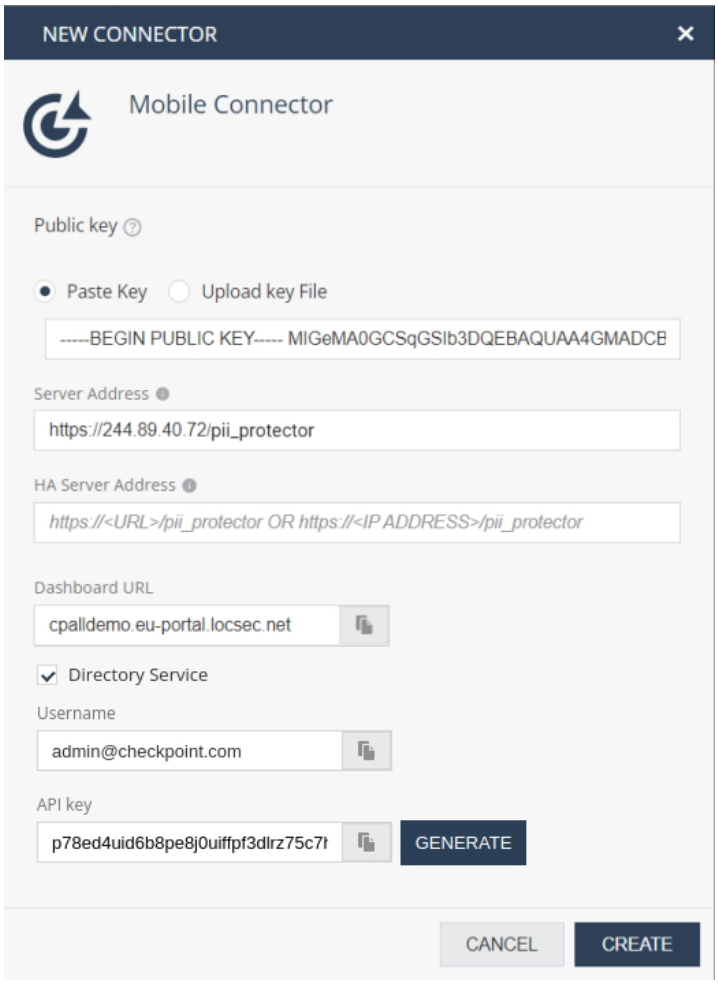
- Configure ldap settings:

```
ldap:
   url: <ldap server URL >
   base: <base branch>
   userDN: <user dn>
   password: <ldap password>
```

Example:

```
ldap:
   url: "ldap://192.168.133.70:389"
   base: "DC=locsec,DC=net"
   userDN: "CN=Administrator,CN=Users,DC=locsec,DC=net"
   password: "1234"
```

- Configure SBM settings:




```
sbm:
   dashboardUrl: <Harmony Mobile dashboard URL>
   username: <admin in Harmony Mobile dashboard>
   apiKey: <API key generated by the admin>
```

Example:

```
sbm:
   dashboardUrl: "https://cpalldemo.eu-portal.locsec.net/"
```

```
username: "admin@checkpoint.com"
apiKey: <Generated API key>
```

Notes -

- For the **Harmony Mobile dashboard URL**, enter the **Dashboard URL** value in the **New Connector** window. Add `https://` at the beginning of the URL and close it with a '/' character.
- For the **API key**, click **Generate** in the **New Connector** window and copy the generated API key.

- Configure Directory Service login:

```
login:
     username: <username>
     password: <encrypted password>
```

- Access Directory Service UI and enroll devices:

  a. Restart Harmony MobileConnector:

  ```
  sbmc_stop
  sbmc_start
  ```

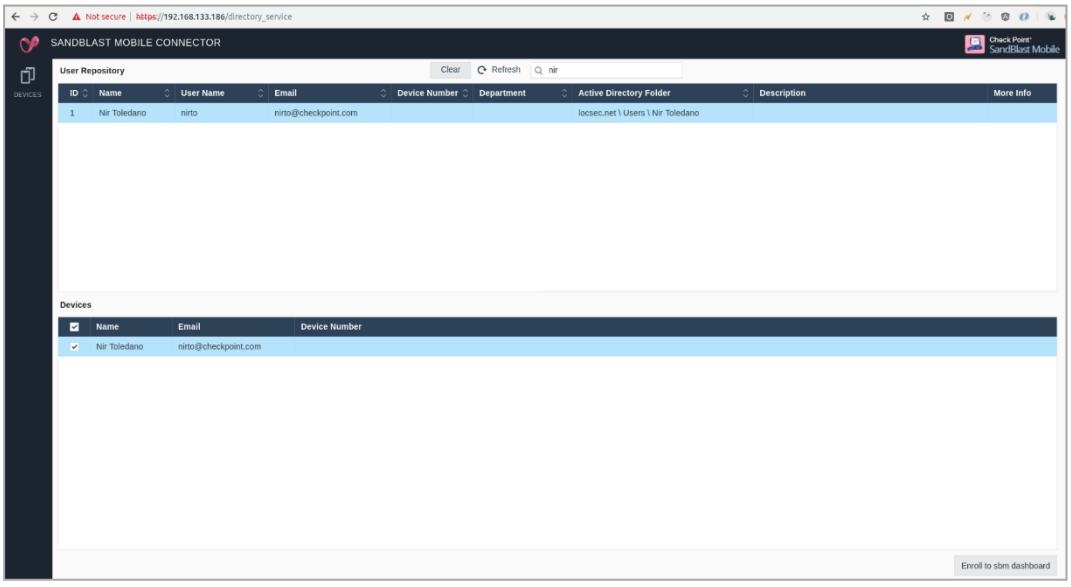
  b. Browse to `http://connector-ip/directory_service`

  c. To log in, enter username and password.

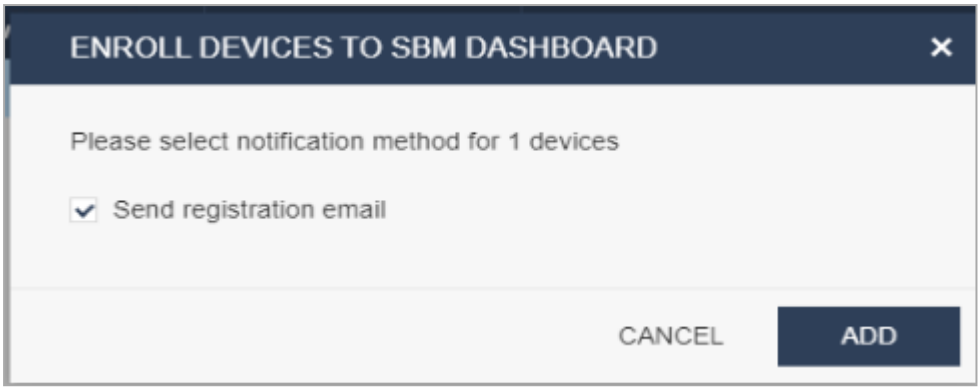
  d. Use the search bar to search for a user. In the search results, select a user from the **User Repository** table.

  The selected user's devices are displayed in the **Devices** table. Note that this is only for users with a listed email address.

  e. To add a device to Harmony Mobile dashboard, select the required device and click **Enroll to SBM dashboard**.



f. Clear the **Send registration email** checkbox and click **Add**.



Advanced Configuration

Migrating Encryption Keys from User Device Management (UDM) to Connector

1. Install and configure the Harmony Mobile Connector on a new VM. For more information, see *"Installing and Configuring Harmony Mobile Connector" on page 11*.
2. Copy these files from the UDM server:

   ```
   /opt/CPudm-R80.20/conf/pii_encryption_predefined.iv
   /opt/CPudm-R80.20/conf/pii_encryption_predefined.key
   /opt/CPudm-R80.20/conf/pii_fields.xml
   /opt/CPudm-R80.20/conf/pii_filter.properties
   /opt/CPudm-R80.20/conf/pii_encryption.key
   /opt/CPudm-R80.20/conf/pii_encryption.iv
   ```

3. Back up the encryption keys on the connector machine:

   ```
   /opt/CPsbmc/components/pii_filter/conf
   ```

4. Copy the files from step 2 to the Harmony Mobile Connector:

   ```
   /opt/CPsbmc/components/pii_filter/conf/
   ```

5. Restart the Harmony Mobile Connector:

   ```
   sbmc_stop
   sbmc_start
   ```

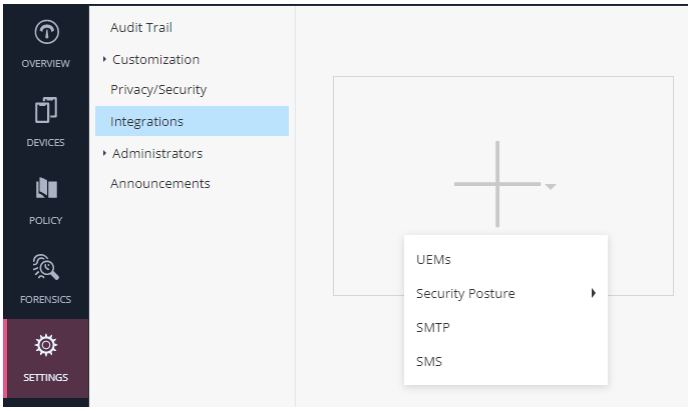
6. Edit the MDM integration wizard in Harmony Mobile dashboard. Clear the **Server is behind UDM System** checkbox and follow the procedures in *"Configuring the Connector in Harmony Mobile Administrator Portal" on page 19*.

Setting up an On-Premises SMTP Service (without UEM)

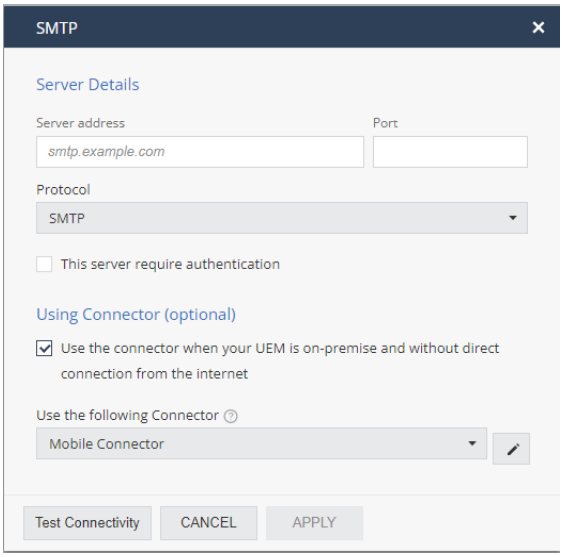
1. Install Gaia.
2. In *"Installing and Configuring Harmony Mobile Connector" on page 11* , follow all the procedures except the pii protector settings.
3. Configure your on-premises SMTP service:

a. In the Harmony Mobile Administrator Portal, go to **Settings** > **Integrations**.

b. Click **+** and select **SMTP**.



The **SMTP** window appears.



c. Configure **Server Details**:

   i. SMTP transport for ports 25 and 587.

   ii. SMTPS transport for port 465.

d. To use the connector with an on-premises UEM without a direct internet connection, select the checkbox under **Using Connector** section.

e. Click **Test Connectivity**.

   If there are no errors, click **Apply**.

Working with a Proxy

To connect a proxy from the Harmony Mobile Connector to the internet or to the UEM:

1. Log in to the VM through `ssh`.
2. Update the settings to access Harmony Mobile dashboard through the proxy.

a. Open this settings file:

```
vi /opt/CPsbmc/components/pii_protector/application.yml
```

b. Update the relevant settings in the file (server > Proxy), for example:

```
proxy:
         enabled: true
         host: "myproxy.mydomain.com"
         port: 8080
         authentication-required: true
         user: "proxy_user"
         password: "proxy_password"
```

3. Update the settings to access the Harmony Mobile Connector cloud component through the proxy.

a. Open this settings file:

```
vi /opt/CPsbmc/components/api_dispatcher/application.yml
```

b. Update the relevant settings in the file:

i. relay Proxy:

Example:

```
proxy:
        enable: true
        host: "myproxy.mydomain.com"
        port: 8080
        username: "proxy_user"
        password: "proxy_password"
```

ii. MDM Proxy:
If there is a proxy to connect to the UEM.

Example:

```
proxy:
         enable: true
         host: "myproxy.mydomain.com"
         port: 8080
         username: "proxy_user"
         password: "proxy_password"
```

Using a UEM with a Self-Signed Certificate

To use a UEM server with a self-signed certificate (not signed with a valid Certificate Authority):

1. Download the UEM certificate in a Privacy Enhanced Mail (PEM) format and copy it to the Harmony Mobile Connector server.
2. Connect to the VM through `ssh` with your user credentials.
3. Update the settings file to use the self-signed certificate:

a. Open the settings file:

```
vi /opt/CPsbmc/components/api_dispatcher/application.yml
```

b. When you connect to the UEM, use the self-signed certificate.
mdm > ssl > `use_self_sign_certificate`

Path to the UEM certificate:
mdm > ssl > `certificate_path`

Example:
```
use_self_sign_certificate: true
certificate_path: "/web/conf/my_uem_certificate.pem"
```

Note - The option to disable the SSL verification to the MSD should be used only in Proof of Concept (POC) and **not** in production.

Setting up High Availability for the Connector

To set up a high availability for the Harmony Mobile Connector:

1. Create a copy of the existing VM that runs the Harmony Mobile Connector.
2. Change the new VM IP address (in Gaia).

   In clish:

   ```
   show interface eth0
   set interface eth0 ipv4-address <ip> mask length <16/23>
   save config
   ```

3. Add the new IP address to the UEM settings in Harmony Mobile dashboard.

Viewing Connector

To set up a new viewing connector (an instance without API dispatcher. Read-only):

1. Follow the steps in *"Setting up High Availability for the Connector" above* to set up the additional Harmony Mobile Connector VM.
2. In the Expert mode, on the Harmony Mobile Connector, run these commands:
   - To restart SBMC:

     sbmc_stop; sbmc_start
   - To deactivate api_dispatcher:
     - source /opt/CPsbmc/scripts/sbmc_functions.sh
     - stop_component api_dispatcher

Upgrading Harmony Mobile Connector from R80.XX to R80.40

1. Create a snapshot of the current R80.XX virtual machine.
2. Connect to the VM through `ssh` and log in to Expert mode with your username and password.

3. Run this script to back up the configuration files:

```
SBMCBACKUPDIR=/var/log/SBMCBACKUP
mkdir $SBMCBACKUPDIR
cp $SBMCDIR/components/api_dispatcher/application.yml $SBMCBACKUPDIR/api_
dispatcher_application.yml
cp $SBMCDIR/components/pii_protector/application.yml $SBMCBACKUPDIR/pii_
protector_application.yml
cp -r $SBMCDIR/components/pii_filter/conf $SBMCBACKUPDIR/conf
cp /web/conf/sbmc_private_key.pem $SBMCBACKUPDIR/sbmc_private_key.pem
cp /web/conf/sbmc_public_key.pub $SBMCBACKUPDIR/sbmc_public_key.pub
```

4. Upgrade to R80.40.
5. Install the Harmony Mobile Connector. For more information, see *"Installing and Configuring Harmony Mobile Connector" on page 11*.
6. Restore files from backup:

```
SBMCBACKUPDIR=/var/log/SBMCBACKUP
cp $SBMCBACKUPDIR/sbmc_private_key.pem /web/conf/sbmc_private_key.pem
cp $SBMCBACKUPDIR/sbmc_public_key.pub /web/conf/sbmc_public_key.pub
rm -rf $SBMCDIR/components/pii_filter/conf
cp -r $SBMCBACKUPDIR/conf $SBMCDIR/components/pii_filter/conf
cp $SBMCBACKUPDIR/pii_protector_application.yml $SBMCDIR/components/pii_
protector/application.yml
```

7. Update the `$SBMCDIR/components/api_dispatcher/application.yml` configuration file with the relevant values from `$SBMCBACKUPDIR/api_dispatcher_application.yml`.
8. Restart SBMC:

```
sbmc_stop
sbmc_start
```

Saving the Encrypted MDM Password

To save the encrypted MDM password in the Connector configuration files:

1. Connect to the VM through `ssh` and log in to Expert mode.
2. Run this command and replace <mdm_password> with your MDM password:

```
curl_cli --request POST
'http://localhost:7777/json_map?action=hide' --header 'Content-Type:
application/json' --data-raw
'{"fields":[{"id":"PASSWORD","value":"<mdm_
password>","type":"USERNAME"}]}'
```

   The output displayed is the encrypted password.

   Note - To successfully run the command, make sure to enter the correct input parameters and avoid extra space characters.

3. Edit the settings file `vi /opt/CPsbmc/components/api_dispatcher/application.yml` and paste the output password to the relevant MDM configuration.

   Example:

```
mdm:
    credentials:
                the relevant mdm you use:
                          password: <paste output password here>
```

Related Documents

Harmony Mobile Connector is only relevant for on-premises UEM solutions. It supports these UEM integrations:

- BlackBerry UEM Integration Guide
- WorkspaceOne Integration Guide
- MobileIron Core Integration Guide
- Citrix XenMobile Integration Guide