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.

Check Point R77.30.01 UDM HF2
For more about this release, see the R77.30.01 UDM HF2 home page http://supportcontent.checkpoint.com/solutions?id=sk110357.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=49984.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on User and Device Management R77.30.01 UDM HF2 Administration Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 October 2016</td>
<td>Corrected filepaths</td>
</tr>
<tr>
<td>06 June 2016</td>
<td>First release of this document for HF2</td>
</tr>
</tbody>
</table>
Introduction

UDM (User and Device Management) is a web based application that manages a range of user and device related tasks in an organization. A typical user accesses organizational resources from multiple devices: computers, laptops, smartphones, and tablets. UDM provides a unified environment for managing various user and device related tasks, such as provisioning, transparency of access via SmartLog logs, viewing user and device details, certificate management, AD user management, and FDE password recovery (for Endpoint Security clients).

With UDM, security administrators can delegate user and device management tasks to Help Desk administrators. This delegation of responsibilities lets the network security team handle security policy issues and the Help Desk team manage some user access tasks.

UDM includes:

- **Remote Access certificate management**
  - Manage, create, and revoke user certificates for remote access.
  - Use email templates to send information to users on how to connect remotely from their devices.

- **Integration with Active Directory**
  - See all users in the organization and the devices they are using to connect to organizational resources.
  - Change the status of Active Directory users when necessary (expired, disabled, or locked).
  - Manage Active Directory user groups.

- **Integration with SmartLog**
  - See user login and activity logs.
  - Search and filter logs for a specified user.
  - See if a device is connected or disconnected.

- **Integration with Endpoint Security Server**
  - See activity of users and devices.
  - Use Full Disk Encryption password recovery.
  - Active Directory integration.

- **Integration with Capsule Cloud**
  - See logs of Capsule Cloud users.
  - Send new registration codes to users.

- **Integration with Mobile Threat Prevention**
  - Enroll and revoke devices with Mobile Threat Prevention.
  - View event logs originating from the Mobile Threat Prevention Cloud.
  - Browse securely to the Mobile Threat Prevention Management Dashboard.
• **Mobile Access Suspicious Account Activity Monitoring**
  - Increase the visibility of security incidents by involving end-users with potential security incidents related to their Mobile Access or Capsule Workspace account.
  - Send SMS or Email notification to end-users upon security incidents on their account.
  - End-users can use a Self Service Portal to: See account information, respond to suspicious activity, add or revoke certificates, change their mobile number in LDAP.

This guide contains tasks for security administrators and Help Desk administrators. The table shows the chapters that apply to each type of administrator:

<table>
<thead>
<tr>
<th>Chapters</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>Security Administrator</td>
</tr>
<tr>
<td>Setting Up UDM</td>
<td></td>
</tr>
<tr>
<td>Working with Mobile Threat Prevention</td>
<td></td>
</tr>
<tr>
<td>Managing Users and Devices</td>
<td>Help Desk Administrator</td>
</tr>
<tr>
<td>Monitoring Logs and Devices</td>
<td></td>
</tr>
<tr>
<td>Task Scenarios</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Scenarios</td>
<td></td>
</tr>
</tbody>
</table>

**Installing UDM**


You must install UDM R77.30.01 HF2 on top of UDM R77.30.01 HF1.

**The workflow is:**

1. Install UDM R77.30.01 HF1 on the UDM server.
2. Install UDM R77.30.01 HF2 on the UDM server.
3. Enable UDM in SmartDashboard.

**To install UDM R77.30.01 HF1 on a Gaia Security Management Server:**

1. Back up your R77.30 Security Management Server.
2. Create a temporary directory.
4. Save the file to a temporary directory.
5. Connect to the management server with SSH.
6. Run these commands in expert mode:
   - `tar -zxvf R77.30.01_HF1.Linux.tgz`
   - `./UnixInstallScript`
7. Reboot.
To install UDM R77.30.01 HF2 on a Gaia Security Management Server:

1. Back up your R77.30.01 HF1 Security Management Server.
2. Create a temporary directory.
4. Save the file to a temporary directory.
5. Connect to the management server with SSH.
6. Run these commands in expert mode:
   - `tar -zxvf R77.30.01_HF2.Linux.tgz`
   - `./UnixInstallScript`
7. If you had an active UDM environment with R77.30.01 HF1 that included Mobile Threat Prevention, set this in the UDM configuration file:
   
   ```
   pii.filter.decryption.enforce.magic.value = false
   ```
   in `udmenv.properties`
8. Reboot.

To enable the UDM Portal:

1. After the hotfix installation finishes, open SmartDashboard.
2. Open the UDM Management object.
3. In the General Properties > Management tab, make sure that Management & User Portal is selected.
4. Click OK.
5. Install Database.
6. Define the UDM Server as a GUI client.
7. In your Firewall policy, make a rule to allow CPMI traffic from the UDM server to the Management Server.
8. In a standalone environment, install policy.
9. Make sure that UDM is running. Open a browser and go to this URL:

   ```
   https://<UDM server FQDN URL>/udm_portal
   ```
10. Make sure that SmartDashboard and other SmartConsole clients are not connected to the Security Management Server. This is necessary during the first login to UDM or while configuring it for the first time.
11. Enter the login credentials and the IP address of your Security Management Server.

Multi-Domain Server Configuration

You can use your R77.30.01 UDM HF2 UDM server to log in to a Domain Management Server in a Multi-Domain Security Management environment. The configuration here also enables the UDM to send logs to the Domain Management Server.

To configure the UDM in a Multi-Domain Security Management environment:

1. Make sure that SmartDashboard and SmartDomain Manager are closed.
2. On your UDM Server, open this file:
   ```
   $UDMDIR/conf/cmas_list.conf
   ```
3. Add the Domain Management Server to the file with this syntax:

   `<Domain Management Server IP address>:WSPort=<Domain Management Server port>:MDSip=<Multi-Domain Server IP address>`

   For example: 192.0.2.1:WSPort=30000:MDSip=192.0.2.2

4. Run: udmstop

5. Run: udmstart

If you do not know the IP address or port of the Domain Management Server, you can find them in this file: `$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf`

If you do not see this file, contact Check Point support.

This is a sample `webservices_cmas_ports.conf` file:

```plaintext
: (My_Management_Server
   :port (30000)
   :port_SL (30001)
   :ip_addr (192.0.2.1)
)
```
Setting Up UDM

The procedures in this chapter are for security administrators.

SmartDashboard Prerequisites

Before Help Desk administrators can use the UDM Portal, you must make sure these SmartDashboard prerequisites are met on the existing Security Management Server or Domain Management Server where you enabled the UDM Portal.

- SmartLog is enabled
- An LDAP server object is defined
- A mail server is configured
- A mail template is configured
- An administrator for UDM is defined and granted UDM permissions

Enabling SmartLog

UDM interacts with SmartLog to show logs. SmartLog must be enabled to see UDM user device data.

To enable SmartLog in SmartDashboard:
1. Log in to SmartDashboard.
2. From the **Network Objects** tree, double-click the UDM management server object.
   - The **General Properties** page opens.
3. Click **Logs** and select **Enable SmartLog**.
4. Click **OK**.

If you use SmartLog on a log server, you must also do these steps:
1. On the UDM server, go to the file:
   - $UDMDIR/conf/udmenv.properties
2. Change the parameter `logserver.joinLogs = false` to:
   - `logserver.joinLogs = true`
3. Run: `udmstop`
4. Run: `udmstart`

Configuring LDAP Account Units

UDM interacts with your organization’s Active Directory to give your environment authentication and directory services. UDM uses an LDAP account unit interface to query and change items in your User Directory.

If an LDAP account unit is not already defined in SmartDashboard, define one for your User Directory. You must define at least one Account Unit to work with UDM.
To configure an LDAP account unit:

1. Log in to SmartDashboard.
2. In the objects tree, click **Servers and OPSEC**.
3. Right-click **Servers** and select **New > LDAP Account Unit**.
   The LDAP Account Unit Properties window opens.
4. Configure these settings:
   - **General tab**
   - **Servers tab**
   - **Objects Management tab**
   - **Authentication tab**
5. Click **OK** and then **Close**.

**General Tab**

The **General** tab lets you configure how the Security Management Server uses the Account Unit. You can select one or more of these options:

- **CRL retrieval** - The Security Management Server manages how the CA sends information about revoked licenses to the Security Gateways.
- **User Management** - The Security Management Server uses the user information from this LDAP server. Make sure that User Directory is enabled on the Security Management Server.
- **Active Directory Query** - This AD (Active Directory) server is used as an Identity Awareness source. This option is only available if the **Profile** is set to Microsoft_AD.

LDAP SSO (Single Sign On) is only supported for Account Unit Objects that use **User Management**.

To configure the **General tab**:

1. Enter the **Name** for the Account Unit.
2. From **Profile**, select the LDAP vendor.
3. Enter the prefix or domain for the Account Unit. This value is used when the same user name is used in multiple Account Units.
   - **Prefix** - For servers that do NOT use AD.
   - **Domain** - For AD servers. This value is also necessary for AD Query and SSO.
4. Select one or more of the Account Unit usage options.
5. For LDAP user information that uses non-English languages, select **Enable Unicode** support.
6. To configure and enable Kerberos SSO for Identity Awareness:
   a) Click **Active Directory SSO configuration**.
   b) Configure the settings.
   c) Click **OK**.
7. Configure the other tabs or click **OK**.

**Servers Tab**

The **Servers** tab lets you create and manage the LDAP servers that are used by this Account Unit. You can add LDAP server objects or create new ones.
Use the Update Account to All Servers window to configure the login parameters for all the servers for this Account Unit. If the servers use different login information, edit the parameters for each server.

To configure the login parameters for all the servers:
1. Click **Update Account Credentials**.
   The Update Account to All Servers window opens.
2. Enter the login parameters.
3. Click **OK**.

To remove a server from the Account Unit:
Select the server and click **Remove**.

To manage the servers for the Account Unit:
1. Do one of these actions for the server:
   - To add a server, click **Add**.
   - To edit a server, select the server and click **Edit**.
   The LDAP Server Properties window opens.
2. If necessary, create a new SmartDashboard server object:
   a) Click **New**.
      The Host Node window opens.
   b) Enter the settings for the LDAP server.
   c) Click **OK**.
3. From Host, select the server object.
4. Configure the settings for the LDAP server.
5. Optional: Click the Encryption tab and configure the SSL encryption settings.
6. Click **OK**.
7. Configure the other tabs or click **OK**.

   **Note** - The UDM can use only one server from the servers list of an LDAP account unit.

**Objects Management Tab**
The **Objects Management** tab lets you select which LDAP server object SmartDashboard queries for the applicable connections and users. You can also enable password protection for this object.

To configure the Objects Management tab:
1. From **Manage objects on**, select the LDAP server object.
2. Click **Fetch branches**.
   The Security Management Server queries and shows the LDAP branches.
3. **Optional**: Click **Add**, **Edit** and **Delete** to manage the LDAP branches.
4. **Optional**: Select **Prompt for password when opening this Account Unit**.
5. From **Return entries**, configure the number of entries that are stored in the LDAP database.
6. Configure the other tabs or click **OK**.
Authentication Tab

The Authentication tab lets you configure the authentication scheme for the Account Unit. You can use a common group path to optimize group membership queries. One path for all the LDAP group objects is created and only one query is necessary for the group objects.

To configure the Authentication tab:

1. Optional: Select Use common group path for queries.
2. Select one or more authentication schemes that are used to authenticate users in this Account Unit.
3. Select the default settings for new LDAP users:
   - User template - Template that you created
   - Default authentication scheme
4. Optional: Select and configure the login failure settings.
5. For IKE users in this Account Unit, enter the pre-shared secret key.
6. Configure the other tabs or click OK.

Configuring a Mail Server

A mail server must be defined in SmartDashboard to enable sending emails with connection instructions to users.

If a mail server is not already defined in SmartDashboard, define one. You can use this procedure or configure a mail server from the Certificate Distribution wizard in the Mobile Access tab.

To configure a mail server:

1. In SmartDashboard, select the Data Loss Prevention tab > Additional Settings > Mail Server > Mail Servers > New.
   The Mail Server window opens.
2. Enter the mail server Name and select the Host object.
3. If the selected server requires authentication:
   a) Select Server Requires Authentication.
   b) Enter the applicable User Name and Password credentials.
4. Configure these parameters:
   a) Port - Select a port for the mail server.
   b) Enable SSL Encryption - Select this checkbox to encrypt emails using SSL.
   c) From Address - Enter the mail address that is shown when sending emails. In UDM you can define a different "from" email address for connection instruction emails.
5. Click OK.

Configuring Email Templates

Mobile devices connect to network resources using a Check Point application. The client application can use certificate-only authentication or two-factor authentication with client certificates and username/password. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway. The system uses email templates for distributing certificates to users.
Make sure email templates for client certificate emails are defined in SmartDashboard. If there are no email templates, configure at least one.

To configure an email template:
1. In SmartDashboard, select the Mobile Access tab and then the Client Certificates page.
2. In the Email Templates for Certificate Distribution pane, select New. The Email Template window opens.
3. Enter a Name for the template.
4. Optional: Enter a Comment. Comments show in the Mail Template list on the Client Certificates page.
5. Optional: Click Languages to change the language of the email.
6. Enter a Subject for the email. Click Insert Field to add a predefined field, such as a Username.
7. In the message body add and format text. Click Insert Field to add a predefined field, such as Username, Registration Key, or Expiration Date.
8. Click Insert Link to add a link or QR code and select the type of link to add. For each link type, you select which elements will be added to the mail template:
   The text in Display Text is the text that shows on the link.
9. Click OK.
10. Optional: Click Preview in Browser to see a preview of how the email will look.
11. Click OK.

Insert Link

When you select Insert Link in the email template, there are multiple options. For each option choose the link format:

- **QR Code** - Users scan the code with their mobile devices.
- **HTML Link** - Users tap the link on their mobile devices.

You can select both QR Code and HTML link to include both in the email.

Types of links:

- **Site and Certificate Creation** - For users who already have a Check Point app installed. When users scan the CR code or go to the link, it creates the site and registers the certificate.
  - **Select the client type that will connect to the site** - Select one client type that users will have installed.
- **Download Application** - Lets users download a Check Point App for their mobile devices.
  - **Select the client device operating system**
  - **Select the client type to download**
- **Custom URL** - Send users to a URL that you enter.
  - **Link URL** - Enter the full URL of the site.
  - **Display Text** - Enter the text to show on the HTML link.
Defining a UDM Administrator

Define an administrator in SmartDashboard for Help Desk administrators that will use UDM.

To define a UDM administrator:

1. In SmartDashboard, click **Users and Administrators** in the objects tree.
2. Right-click **Administrators** and select **New Administrator**.
   The Administrators Properties window opens.
3. In the General Properties pane, enter the **User Name**, **Email Address**, **Comment** (optional), and **Expiration Date**.
4. Select an existing UDM Permissions Profile from the list or click **New** to create one.
5. If you selected **New**, the Permissions Profile Properties window opens. Do these steps:
   a) In **Name**, enter a name for the profile. For example, UDM_profile.
   b) Below **Allow Access via**, make sure **Management Portal and SmartConsole Applications** is selected.
   c) Below **Permissions**, select **Customized** and click **Edit**.
      The Edit Permission of Profile window opens.
   d) In the **General** tab, select these options:
      - **Endpoint Security Server** - **Read only** to enable login to the Endpoint Security Server when necessary.
      - **Client Certificates** - To enable the certificate management options.
      - **User and Device Management Configuration** - Select one:
        - **Read/Write** - To enable UDM use and configuration, including changing the policy, LDAP, and Exchange settings.
        - **Read Only** - To enable a Help Desk administrator to use the UDM portal but not change its configuration.
   e) In the **Monitoring and Logging** tab, select these options to let Help Desk see SmartLog logs:
      - **Monitoring** - **Read/Write**
      - **Track Logs** - **Read only**
      - **Identities**
      - **Show Identities by default**
   f) In the **Events and Reports**, **Provisioning**, and **Endpoint** tabs clear all checkboxes.
   g) Click **OK** in the Edit Permissions of Profile window.
6. Click **OK** in the Permissions Profile Properties window.
7. Click **OK** in the Administrator Properties window.
   The defined administrator has permissions to work with UDM.

**Note** - These are the minimal permissions required for a UDM administrator. You can add permissions to the above ones if necessary.
Configuring LDAP Settings

After an LDAP Account Unit has been configured for an Active Directory in SmartDashboard, you must configure it also in the UDM. If you have more than one Active Directory configured in SmartDashboard, make sure to configure them here also.

To configure LDAP settings:

1. Log in to the UDM portal with UDM administrator credentials.
2. In the Configuration tab of the UDM portal, below LDAP Settings, click New.
   The New LDAP Account Unit window opens.
3. In Display Name, enter a name for the LDAP account unit in UDM.
4. Select the LDAP Account Unit from the list.
5. Select an LDAP Server that is related with the LDAP Account Unit from the list.
6. Optional: In Base Branch, use the AD syntax to enter a specified branch of users to show. By default, users from the main branch are shown.
   For example: OU=Users,OU=Mexico,DC=ad,DC=checkpoint,DC=com.
   The search will start from Users.Mexico.
7. Optional: In Filter, use the AD syntax to filter the list of users shown by specified criteria.
   For example: (&(!(objectclass=computer))(!(department=*))]
   The search will show AD entities that are not computers and that have a department.
8. Click OK.
   The LDAP object that represents the LDAP Account Unit is added to the table. You can edit it or remove it if necessary.
9. Click Apply.

Configuring a Mail Server

After at least one mail server has been configured in SmartDashboard, you must configure it also in the UDM. This mail server is used to send the emails that contain certificate information.

To configure a mail server:

1. Log in to the UDM portal with UDM administrator credentials.
2. In the Configuration tab of the UDM portal, below Mail Settings, select the applicable Mail Server from the list.
3. In From Address, enter the email address that is shown in the From field in the certificate emails. When replying to an email, the address in this field is used.
4. In Display Name of Sender, enter the name that is shown for the sender in the From Address field. For example, for the From Address field value Jsmith@abc.com, enter John Smith for the sender name.
5. Click Apply.
Configuring an HTTP Proxy

UDM features that require internet access require HTTP Proxy configuration.

To configure HTTP proxy:

1. On the UDM Server, open $UDMDIR/tomcat/webapps/udm_portal/WEB-INF/applicationContext-security.xml
2. In this section:

```xml
<beans:bean id="httpProxyHost"
    class="com.checkpoint.udm_portal.core.infra.Host">
     <!-- <beans:property name="serverAddress"  value="<address>" />
     <beans:property name="port"  value="<port>" /> -->
</beans:bean>
```

Change the values for `serverAddress` and `port` to the details of an http proxy server. For example:

```xml
<beans:bean id="httpProxyHost"
    class="com.checkpoint.udm_portal.core.infra.Host">
    <beans:property name="serverAddress" value="httpproxy.domain.com" />
    <beans:property name="port"  value="8080" />
</beans:bean>
```

3. Save changes.

Configuring the Endpoint Security Management Server

To get information about AD users’ laptops and PCs that run the Endpoint Security client, you must configure connectivity to the Endpoint Security Management Server.

To configure the Endpoint Security Management Server:

1. Log in to the UDM portal with UDM administrator credentials.
2. In the Configuration tab, below Endpoint Settings, click New. The New Endpoint Server window opens.
3. In Display Name, enter a name for the Endpoint Server administrator account.
4. Enter the User Name, Password, and Server Address.
5. Click OK. The Endpoint Security Management Server is added to the table. You can edit it or remove it if necessary.
6. Click Apply. If the user has a laptop or PC that is or was connected to network resources, the Devices table shows the entry. For more information, see Monitoring Devices (on page 29).

>Note - The Devices table shows information for all user repositories, not only a specified search user repository.
Configuring Capsule Cloud

To get information about Capsule Cloud users and to send Capsule Cloud registration codes, configure a Capsule Cloud account.

To configure Capsule Cloud:

1. Log in to the UDM portal with UDM administrator credentials.
2. In the Configuration tab, below Cloud Settings, click New or Edit. The New Cloud Server window opens.
3. Enter:
   - **Display Name** - A name for the Capsule Cloud administrator account.
   - **User Name, Password** - Credentials of a Capsule Cloud administrator
4. Click OK. The display name of the configured account shows under Cloud Settings in the Configuration tab.
5. Click Apply.
Managing Users and Devices

The procedures in this chapter are for Help Desk administrators defined as UDM administrators.

Logging In

Make sure you have the login details that the security administrator has defined in SmartDashboard for your UDM administrator and the IP address or DNS name of the Security Management Server it interacts with. The UDM administrator is defined in the Users and Administrators view in SmartDashboard.

You must also have:

- The IP address of the Endpoint Security Management Server that the UDM interacts with. This is required if it is necessary to connect to the Endpoint Security Management Server.
- The AD username and password credentials. This is required for AD operations (if applicable).

To log in to the UDM:

1. Browse to the UDM application from a web browser.
2. Enter your User name and Password.
3. Enter the Server Name or IP address of the Security Management Server.
4. Click Login.
   The Users & Devices window opens.

Searching for Users

To search for a user:

1. In the Users & Devices tab, enter your search query in the search box. Use this syntax: 
   `<free text>` or `'<column_name>:<value>', '<column_name>:<value>'`
   For example:
   - Entering John Smith in the search box - Searches the user name, display name, full name, and description fields.
   - Entering `username:Jsmith` - Searches the AD user name field for a user record that contains Jsmith in the user name field.
   - Entering `email:jsmith@abc.com` - Searches the AD email field for a user record that contains jsmith@abc.com in the email field.
   - Entering `group:exchange` - Searches the AD group field for records that contain users that belong to groups that contain the string exchange. You can enter a partial group name. The Users Repository table will show all matching users that belong to groups that contain the partial name.

2. By default, all user sources are searched (Any is shown in the Users Repository list). Any includes all defined LDAP Account Units and an Endpoint Security Management Server if configured. To search for a specified LDAP Account Unit or the Endpoint Security Management Server, select it from the list.
3. Click the **Search** icon.

   The Users Repository table shows all matching results. If a user has already connected to resources using remote devices, the Devices table shows the details.

   If the result set is too big, a message is shown. Refine the search to narrow the results.

**To see details for a specified user:**

1. From the entries in the Users Repository table, select the applicable user.
2. Click **View Details** or double-click the user’s entry in the table.

   The user’s details are shown. The window also contains sections for Groups, Certificates, Devices, and Logs. Click the arrow icon next to the section name to expand it.

### Managing Certificates

Check Point Mobile Apps for mobile devices can use certificate-only authentication or two-factor authentication with client certificates and username/password. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.

The certificate management options in UDM include:

- Create, edit, and revoke a certificate for a user
- Create certificates for multiple users
- Customize the instructions template sent to users

Multiple certificates can be created for a user. A user’s certificates are shown in the user’s **Certificates** table.

**To see a user’s certificates:**

1. On the **Users & Devices** tab, search for a user.
2. Double-click a user’s name in the **Users Repository** list.

   The window shows the user’s details, groups, certificates, devices, and logs. Scroll to the **Certificates** section if necessary.

This table summarizes the use of certificates and corresponding statuses:

<table>
<thead>
<tr>
<th>Action</th>
<th>Certificate Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td><strong>Expired</strong> - This status is shown when the certificate has reached its expiration date. In such a case, you must create a new certificate for the user if necessary.</td>
</tr>
<tr>
<td>A UDM administrator creates a new certificate for a user and then sends it to the user.</td>
<td><strong>Pending Enrollment</strong> - This status is shown in the Certificates table until the user connects to the Mobile Access Security Gateway through a client and uses the certificate for authenticating.</td>
</tr>
<tr>
<td>The user connects through the client and enrolls with the certificate details (includes gateway IP address, user name, and registration key).</td>
<td><strong>Valid</strong> - This status is shown if the enrollment is successful. Otherwise, the certificate status continues to be Pending Enrollment until successful connection.</td>
</tr>
</tbody>
</table>
### Action vs. Certificate Status

<table>
<thead>
<tr>
<th>Action</th>
<th>Certificate Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A UDM administrator revokes the certificate to make sure that the device cannot access the organization’s network resources. For example, an employee leaves the company or the device is sold or is no longer in use.</td>
<td>Revoked - This status is shown when the UDM administrator revokes a valid certificate.</td>
</tr>
</tbody>
</table>

### Creating and Editing Certificates

**To create or edit a new certificate:**

1. In the **Users & Devices** tab, search for the user you must create or edit a certificate for.
2. To create a certificate:
   - Below **User Tasks**, click **New Certificate**.
   
   The **New Certificate For User** window opens (where **User** shows the selected user name).
3. To edit a certificate that is pending enrollment:
   - Double-click the user, select the certificate from the **Certificates** list, and click **Edit**.
   
   The **Edit Certificate For User** window opens.
4. In **Remote Access Site**, select the Mobile Access gateway through which the user will access the organization’s network.
5. In **Instructions Template**, select the template that contains the instructions for installing the client app and certificate installation.
   
   If you have to adjust information in the template, see Customizing Instruction Templates (on page 22).
6. Optional: To change the expiration date of the registration key, edit the number of days in the **days** box.
7. Optional: Add a comment that will be shown for the certificate in the Certificates section of the user’s details.
8. Make sure **Send instructions to the user** is selected if an email with connection instructions must be sent.
9. Click **OK**.

   A notification pop-up shows that the email is being sent when applicable. The certificate status in the Certificates table shows Pending Enrollment until the user connects with the client to the gateway and authenticates with the certificate.

### Creating Certificates for Multiple Users

You can create multiple certificates at one time for selected users, user groups, and OU nodes.

**To create multiple certificates:**

1. In the **Users & Devices** tab, click **Certificate Distribution**, under **System Tasks**.
   
   The **Certificate Distribution** window opens.
2. In the **Mail Details** area:
   - **Send instructions to the user** - When selected, users receive an email with instructions to install the mobile app and register the certificate.
• **Remote Access Site** - Select the Mobile Access gateway through which the user will access the organization’s network.
• **Instructions Template** - Select the template that contains the instructions for installing the client app and certificate installation.

3. In the **Certificate Details** area:
   • Optional: To change the expiration date of the registration key, edit the number of days in the **days** box.
   • Optional: Add a comment that will be shown for the certificate in the Certificates section of the user’s details.

4. In the **Select users and groups** area,
   • Click **Add** to select users and groups to receive certificates.
   • Click **OK**.

5. Optional: Select **Download a file that contains all the enrollment keys**. This can be helpful for troubleshooting.

6. Click **Generate**.
   A **Certificate Distribution** window opens with the results of the certificate creation and emails to users.

### Customizing Instruction Templates

When creating or editing a template, you can edit the instruction template that distributes a registration key to a user.

**To edit a template:**

1. In the **New/Edit Certificate For User** window (where **User** shows the selected user name), click **Customize**.
2. In the **Edit** tab, make the necessary corrections.
3. Optional: Click **Preview** to see a preview of how the email will look.
4. Click **OK**.

   **Note** - The changes made are applied only to this instance of the invitation and has no effect on the SmartDashboard templates.

### Revoking Certificates

You can revoke a certificate that is Pending Enrollment or Valid. Revoking a certificate makes it unusable.

- If the status of a certificate is Pending Enrollment, after you revoke it, the certificate does not show in the **Certificates** list.
- If the status of a certificate is Valid, after you revoke it, the certificate stays in the Certificates list and shows the status **Revoked**. You cannot remove it from the table.

When you revoke a certificate that is valid (a device enrolled with this certificate), a **remote wipe** operation is done on the device.

**Remote wipe:**

- Deletes the certificate from the device to disable connectivity from this device.
- Deletes the server from the site list on the device.
After these operations are completed, you can see the remote wipe action in the logs.


**To revoke one certificate:**
1. Select the certificate from the **Certificates** list.
2. Click **Revoke**.
3. Click **OK** in the confirmation message.
   - If the certificate was valid, it shows the status Revoked in the **Certificates** list.

**To revoke all certificates:**
1. Select the certificate or certificates from the **Certificates** list.
2. Click **Revoke All**.
3. Click **OK** in the confirmation message.
   - If the certificates were valid, they show the status Revoked in the **Certificates** list.

### Active Directory Operations

The UDM lets you do several operations directly on the Active Directory. To do AD operations, you must have the AD administrator credentials. After you enter the credentials you can use the UDM to:

- Reset a user’s password
- Unlock a locked account
- Disable an active account or enable a deactivated account
- Manage user groups

The first time you select one of these AD operations in a UDM session, you will be asked to enter AD credentials. After you successfully enter the credentials, you have permissions to do these operations for the remainder of your UDM session.

**To enter Active Directory credentials:**
1. On the **User & Devices** tab, select one of the above AD tasks from the **User Tasks** list.
   - The **AD Admin Credentials** window opens. You must have the appropriate AD permissions for each operation from the list above.
2. Enter the AD **User Name** and **Password**.
3. Click **OK**.

### Resetting Passwords

To do this operation you must enable an SSL connection between the UDM machine and the Active Directory. For more details, see Enabling SSL for Active Directory (on page 25).
To reset a user’s password:

1. In the **Users & Devices** tab, search for the user for which you must reset a password.
2. Below **User Tasks**, click **Reset password**.
3. If you are asked to enter AD credentials, enter them and click **OK**.
   The Reset Password window opens.
4. In **New password**, enter the new password for the user and confirm it.
5. If it is necessary for the user to change this password when logging in, select **User must change password at next logon**.
6. When the **Unlock account** checkbox is selected, the user’s account is locked in the AD. When resetting the user’s password, the account will also be unlocked.
7. Click **OK**.

**Unlocking an Account**

When a user tries to log in many times with an incorrect password, the user is locked out. An end user cannot log in until the account is unlocked.

To unlock a user’s account:

1. In the **Users & Devices** tab, search for the user account to unlock. The More Info field shows that the user is locked.
2. Below **User Tasks**, click **Unlock account**.
3. If you are asked to enter AD credentials, enter them and click **OK**.
   The Unlock Account window opens.
4. Click **OK** in the window.
   The user is unlocked in the Active Directory.

**Disabling and Enabling Accounts**

You can disable the AD account of a user that is not allowed access to the organization’s resources. For example, when a user is no longer employed by your organization. You can also enable accounts that were disabled in the past.

To disable an active account:

1. In the **Users & Devices** tab, search for the user that must be disabled.
2. Below **User Tasks**, click **Disable Account**.
3. If you are asked to enter AD credentials, enter them and click **OK**.
4. Click **OK** in the information window that opens.
   The user’s account is disabled.

To enable an inactive account:

1. In the **Users & Devices** tab, search for the user that must be enabled.
2. Below **User Tasks**, click **Enable Account**.
3. If you are asked to enter AD credentials, enter them and click **OK**.
4. Click **OK** in the information window that opens.
   The user’s account is enabled.
Managing User Groups

UDM lets you associate new and existing users to Active Directory groups. You can also remove a group association when necessary.

- New employees must be added to different user groups to access different network resources.
- Existing employees may require access to different user groups depending on position changes or special projects.

To manage a user’s groups:

1. In the Users & Devices tab, search for the user.
2. Double-click the user.
   The user’s details are shown.
3. To add a user to a group:
   a) In the Groups section, click Add.
   b) If you are asked to enter AD credentials, enter them and click OK.
      The Select Group window opens.
   c) Search for the group in the Query box or select it from the list.
   d) Click OK.
   e) In the confirmation window click OK.
      The user is added to the group and the group is added to the Groups table’s list.
4. To remove a user from a group:
   a) In the Groups section, select the applicable group from the list and click Remove.
   b) If you are asked to enter AD credentials, enter them and click OK.
      The Remove from Group window opens.
   c) Click OK.
      The user is removed from the group and the group is removed from the Groups table’s list.

Enabling SSL for Active Directory

The UDM operation that resets passwords in Active Directory requires configuration of LDAP over SSL.

By default, UDM is set up to use LDAP without SSL.

There are two configuration options:

- Enabling LDAP over SSL (LDAPS) basic configuration - This option does not verify certificate trust.
- Enabling LDAP over SSL (LDAPS) advanced configuration - This option verifies certificate trust.

To enable LDAP over SSL (LDAPS) basic configuration:

1. On the UDM server, go to the file:
   $UDMDIR/conf/udmenv.properties
2. Edit the parameter ldap.communication.ssl = false to:
   ldap.communication.ssl = true
To enable LDAP over SSL (LDAPS) advanced configuration:

1. Do all of the instructions in sk84620
2. On the UDM server, go to the file:
   $UDMDIR/conf/udmenv.properties
3. Edit the parameter ldap.communication.ssl = false to:
   ldap.communication.ssl = true
4. Edit the parameter ldap.communication.sslTrustAllCertificates = true to:
   ldap.communication.sslTrustAllCertificates = false

Sending Cloud Registration Codes

Capsule Cloud registration codes:
- Register the Capsule Connect clients to Check Point Capsule Cloud.
- Are unique for each user.
- Cannot be sent to groups.

When users get a registration email, it contains:
- A Registration Key for use with Windows or Mac Capsule Connect.
- A link and QR code to download the Android Capsule Connect.
- A link and QR code to download the Android Capsule Connect.

To send a registration code:

1. In the Users & Devices tab, select a user.
2. Under User Tasks, select Send Cloud Registration Code.
3. The Cloud Registration Code window shows the registration code. By default, Send instructions to <user> is selected and the user is sent the registration code and instructions by email. Clear the option if no email is necessary.
4. Click OK.

Giving Remote Help to Full Disk Encryption Users

With Remote Help, Endpoint users can access their Full Disk Encryption protected computers if they are locked out. Users call their help desk administrator and they do this challenge/response procedure.

There are two types of Full Disk Encryption Remote Help:
- **One Time Login** - Gives access as an assumed identity for one session, without resetting the password.
- **Remote password change** - This option is for a user who has a password but has forgotten it.

To give Full Disk Encryption Remote Help assistance:

1. In the Users & Devices tab, search for the user that is locked out.
2. In the Devices list, select the device that is locked out.

4. Select the type of help the end-user requires:
   - **One-Time Login** - Gives access for one session without resetting the password. When the user successfully logs in, the user changes the password.
   - **Remote password change** - This option changes the password when forgotten.

5. Click **Generate Response**.

6. Tell the user the response text string. The user should enter it in the Remote Help window on the locked computer. The endpoint computer shows a challenge code.

7. In the **Challenge (from user)** field, enter the challenge code that the user gives you.

8. Click the second **Generate Response** button. Remote Help authenticates the challenge code and generates a response code.

9. Tell the user to enter the **Response Two (to user)** text string in the Remote Help window on the locked computer.

10. Make sure that the user changes the password or has one-time access before ending the Remote Help session.

11. Click **Close**.
Monitoring Logs and Devices

The procedures in this chapter are for Help Desk administrators defined as UDM administrators.

Viewing System Logs

The Logs tab shows you system logs. It lets you browse the last 100 SmartLog log records of the defined Security Management Server that you are connected to. The log table is automatically refreshed.

To load more records, continue to scroll down the page.

**To search for a specified security log:**

1. Click the **Logs** tab.
2. Enter your query in the **Enter search query** box. Use this syntax:
   ```
   '<IP_address>', '<column_name>:<value>','<column_name>:<value>'
   ```
   For example:
   ```
   '203.0.113.64','action:drop'
   ```

**To see the log record for a specified entry:**

1. Select a log entry from the table.
2. Double-click the entry or click **View Details**.
   The Log Details window opens. The log fields shown are different for different types of entries.

**To refresh the system log data:**

In the **Logs** tab, Click the **Refresh** icon.

**To see only Capsule Cloud logs:**

In the **Logs** tab, select **Cloud** from the drop-down menu, instead of **SmartLog**.

Viewing User Logs

You can see the logs generated for a user through the Endpoint Security Management Server on the User Details page.

**To see a user’s logs:**

1. In the **Users & Devices** tab, search for a user.
2. Double-click the user entry in the Users Repository table or click **View Details**.
   The User Details page opens.
3. Scroll to the **Logs** section on the page.
To search for a specified log:
Enter your query in the **Enter search query** box. Use this syntax:

'\(<\text{IP}\_\text{address}\>\), \(<\text{column}\.\text{name}\>:<\text{value}\>\)'

For example:

'203.0.113.64', 'action:drop'

**To see the log record for a specified entry:**

1. Select a log entry from the table.
2. Double-click the entry or click **View Details**.

   The Log Details window opens. The log fields shown are different for different types of entries.

**To refresh the system log data:**

Click the **Refresh** icon.

---

**Monitoring Devices**

If a user has already connected to resources using remote devices, the Devices table on the Users & Devices tab shows the details. The entries shown in this table are created based on logs.

The **Device** column shows two types of devices:

<table>
<thead>
<tr>
<th>Device Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Desktop Icon" /></td>
<td>Represents desktop PCs and laptops</td>
</tr>
<tr>
<td><img src="image" alt="Mobile Icon" /></td>
<td>Represents mobile devices (smartphones and tablets)</td>
</tr>
</tbody>
</table>

Devices can have one of these statuses:

<table>
<thead>
<tr>
<th>Device Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Connected Icon" /></td>
<td>Connected</td>
</tr>
<tr>
<td><img src="image" alt="Disconnected Icon" /></td>
<td>Disconnected</td>
</tr>
</tbody>
</table>

The **Certificate Number** column shows the certificate number that was used to enroll the device.

The **Office Mode IP** column shows the IP address for a device in a VPN environment. When such a device connects with the Mobile VPN application, the device gets an internal IP address for accessing resources.

**Downloading All UDM Logs**

To download a compressed folder that contains all UDM-related log files:

In the **Configuration** tab of the UDM portal, under Log Reporting, click **Download Logs**.
Suspicious Account Activity Monitoring

_Suspicious Account Activity Monitoring_ tracks potential security incidents related to Capsule Workspace or Mobile Access accounts. Users can receive an email or SMS when an incident occurs with their accounts. The incidents that are tracked are:

- **Password Guessing** - Too many consecutive failed logins to the account with the Active Directory password.
- **Passcode Guessing** - Too many consecutive failed attempts to unlock Capsule Workspace.
- **Certificate Sharing** - The same certificates is used on different devices.
- **Unknown Device** - Someone successfully logged in to the account from a new or unknown device.

The email or SMS that users receive contains a link to a page with information about the security incident. The information includes the device name and the time that the incident occurred. Based on the settings you configure, it can also include the location and IP address of the incident. Users can also send an email to an administrator to report the incident.

The email address and phone number for SMS are taken from Active Directory (`mail` and `mobile` fields). Make sure that phone numbers are written in international format.

A **Suspicious Activity Detection** log is created in SmartLog for each suspicious activity.

Before Configuring Suspicious Activity Monitoring

_SmartDashboard Permissions for First Time Configuration_

The first time that you turn on Suspicious Activity Monitoring or the Self Portal in the UDM portal, a new SmartDashboard administrator user is created automatically. The user is `sam_autogenerated_admin` and it is automatically configured with all of the permissions that it requires. The administrator that turns on these features for the first time in the UDM portal must have permission to configure new users in SmartDashboard.

On Multi-Domain Security Management, the first time that you turn on Suspicious Activity Monitoring, the administrator must be a SmartDomain Manager administrator.

Configure an HTTP Proxy

See Configuring an HTTP Proxy (on page 17).

**Define Properties in the UDM Configuration Files**

Define these settings in the `udmenv` properties configuration file, `$UDMDIR/conf/udmenv.properties`:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sam.udm.server.host</code></td>
<td>The UDM server host name. It is the default host name for the email and SMS templates for the alert page URL.</td>
</tr>
<tr>
<td><code>sam.admin.notification.mail.address</code></td>
<td>The email address of the security administrator. Users have an option to report suspicious activity. The report is sent to this email address.</td>
</tr>
</tbody>
</table>
Define this setting in $UDMDIR/conf/url_shortener.properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url_shortener.server.host_name</td>
<td>The server host name. It is the default host name for the shortened Security Incident Page URL feature.</td>
</tr>
</tbody>
</table>

To edit the UDM configuration files:

1. On the UDM server, run: `udmstop`
2. Make the changes in each file.
3. Save the changes.
4. On the UDM server, run: `udmstart`

Configuring Suspicious Activity Monitoring

Configure which suspicious activities on mobile devices trigger logs and user alerts. You can also customize the SMS or email that users receive and the information it contains. Only users on the Users and Groups to Monitor list are monitored and can get alerts.

To configure suspicious activity monitoring:

1. Make sure that SmartDashboard is closed.
2. Log in to the UDM portal with UDM administrator credentials.
3. Open the User Portal & Security tab.
4. In the Suspicious Activities area, for each incident type:
   - Move the slider to show ON to activate it or OFF to deactivate it.
   - Select a notification option
     - Log Only - The activity shows in logs. No alerts are sent to users.
     - Notify Users - Send a message to users. Select Email, SMS, or both.
   - Configure the notification - Click Configure template next to Email or SMS to edit the Email or SMS Notification Template.
5. In Password guessing and Passcode guessing, select how many failed attempts must be made to trigger notification.
6. Users get a link to the Alert Information Page in the email or SMS notification:
   - Select if the Location or IP Address of the incident shows in the Alert Information Page.
   - Link expiration time - Select the expiration time (in minutes) of the link. After this time the alert data is not available from the alert page. Users will see a Link Expired error message.
7. In Users and Groups to Monitor, click Add to add users and groups to the list. The suspicious activity monitoring policy only applies to users on this list.
8. Click Apply.

SMS Provider Settings

If you selected to Notify users by SMS for one or more suspicious activities, configure the SMS Provider Settings for a company that you choose to supply the messages.

If you do not have an SMS provider, you can use the SMS provider trial mode to try out the feature. If you select this option, SMS messages are sent through a Check Point provider for up to 10 days.
Note that the 10 days start from when you select **Use SMS provider trial mode** and click **Apply** to install the new policy. Select the option only if you are sure that you want to use the trial.

The trial ends after 10 days or when you enter settings for an SMS provider.

**Configuring SMS Provider Settings**

To configure SMS Provider Settings:

1. Get this information from the SMS provider:
   - A URL. The URL should contain these placeholders: $APIID, $USERNAME, $PASSWORD, $PHONE, $MESSAGE.
   - A username and password
   - An API ID
2. In the UDM portal, open the **Configuration** tab.
3. In the **SMS Provider Settings** section, click **New**.
   
   A **New SMS Provider** window opens.
4. Enter a **Display Name** that shows the provider’s name.
   - To use the trial mode, select **Use SMS provider trial mode**.
   - To use a specified provider, fill in the fields with the information that you got from the SMS provider.
5. Click **OK**.
6. Click **Apply**.
   
   The settings are active. If you selected to use the trial mode, the trial period begins immediately.

**Advanced Configuration for Suspicious Activity Monitoring**

You can configure advanced settings in the configuration files.

To make changes in the configuration file:

1. On the UDM server, run: `udmstop`
2. Make the changes in each file.
3. Save the changes.
4. On the UDM server, run: `udmstart`

**Defining Suspicious Activities**

You can define these options in `$UDMDIR/conf/udmenv.properties`:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>suspicious.activity.grace.period</td>
<td>New suspicious activity grace period in minutes. If the same suspicious activity occurs during the grace period for the same user, the system does not create a new alert. The default is 60 minutes.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>suspicious.activity.duration.of.failed.password.attemps</td>
<td>The password guessing suspicious activity is triggered when the configured amount of failed logins (configured in <a href="#">User Portal &amp; Security</a>) occurs during this configured duration. The default is 30 minutes.</td>
</tr>
<tr>
<td>suspicious.activity.duration.of.failed.passcode.attemps</td>
<td>The passcode guessing suspicious activity is triggered when the configured amount of failed passcode logins (configured in <a href="#">User Portal &amp; Security</a>) occurs during this configured duration. The default is 30 minutes.</td>
</tr>
<tr>
<td>sam.udm.server.host [required]</td>
<td>The UDM server host name. It is the default host name for the email and SMS templates for the alert page URL.</td>
</tr>
<tr>
<td>sam.admin.notification.mail.address [required]</td>
<td>The email address of the security administrator. Users have an option to report suspicious activity. The report is sent to this email address.</td>
</tr>
</tbody>
</table>

### Defining the Security Incident Page URL

The SMS that users get when an incident occurs contains a link to an alert page with information about the security incident. By default, the URL is shortened. You can change these options in `$UDMDIR/conf/udmenv.properties`:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use.url.shortener</td>
<td>Use a shortened URL or not. If false the full alert page URL is sent in SMS notifications. The default is true. Valid values: true,false.</td>
</tr>
<tr>
<td>validity.time.in.minutes</td>
<td>The validity duration of the shortened URL. After this time the shortened URL will redirect the user to the Self Portal login page instead of the alert page. The default is 10 minutes.</td>
</tr>
<tr>
<td>expiration.time.in.minutes</td>
<td>The expiration time of the shortened URL. After this time the user will get a 404 error code. The default is 2880 minutes (48 hours).</td>
</tr>
</tbody>
</table>

Define this setting in `$UDMDIR/conf/ url_shortener.properties`:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url_shortener.server.host_name</td>
<td>The server host name. It is the default host name for the shortened Security Incident Page URL feature.</td>
</tr>
</tbody>
</table>
The *Self-Service Portal* lets users without administrator privileges:

- See a history of account access activities.
- See a history of account security incidents.
- Send an email to an administrator to report an incident.
- Generate certificates for user’s devices (only works with certificate authentication).
- Revoke the user’s own certificates from devices (only works with certificate authentication).
- Set or change the mobile number for the user’s LDAP account (requires LDAP privileges to change the *mobile* field).

Configure if the self portal is activated and which actions users can do.

The options that users see in the Self Portal are based on what you configure in the UDM *Self Portal* section.

Only users on the *Users and Groups to Monitor* list can use the Self Portal.

### Configuring the Self-Service Portal

To configure the self portal:

1. Log in to the UDM portal with UDM administrator credentials.
2. On the *User Portal & Security* tab, in the *Self Portal* area, move the slider to show *ON* to activate it or *OFF* to deactivate it.
3. Note the URL of the self portal.
4. Select which actions users can do from the self portal:
   - **Revoke device certificates** - Revoke the user’s certificate from a device. For Capsule Workspace, it deletes all content in the Capsule Workspace area of the device.
   - **Generate certificates** - Create a new certificate for a device that lets it connect to Capsule Workspace.
     - Optional: Click *Settings* to configure more self-enrollment settings (*"Configuring More Self-Service Portal Settings"* on page 36).
   - **Set mobile number** - Reset the user’s mobile number in LDAP. The user must have permissions to do this in LDAP.
5. Click *Apply*.
6. In SmartDashboard, create a new Web Application for the Self Portal and create a Mobile Access rule to let users access it.
7. Configure SSO to make the portal available from Capsule Workspace.
8. Configure Reverse Proxy.
Configuring Reverse Proxy on the Mobile Access Gateway

If the UDM Server is internal, a Mobile Access gateway uses Reverse Proxy to make the self-service portal and alert page accessible to users outside of the organization. Users browse to an address (URL) that is resolved to the gateway IP address. Then, the gateway passes the request to the internal UDM server.

Configure reverse proxy on an R77.30.01 or higher Mobile Access gateway.

To configure reverse proxy on the Mobile Access gateway:

1. On the gateway, run:
   ```plaintext
   ReverseProxyCLI add rule udm
   ```
2. Follow the on-screen instructions to create a rule that gives users access to these paths:
   - `/udm_portal/selfservice`
   - `/goto` (for the shortened URL feature)

   Use these values:
   - **External hostname** - The DNS name of the gateway.
   - **Internal hostname** - The UDM server's host name.

   For example:
   ```plaintext
   ReverseProxyCLI add rule udm1
   Please enter external hostname url, for example: https://ext.contoso.com:
   <DNS of the gateway>
   Please enter internal host url, for example: http://int.contoso.com:8080 OR http://1.1.1.1:8080:
   <hostname of the UDM Server>
   Do you want to add allowed paths (y/n)[n]? y
   Please enter the allowed paths, separated by ',' delimiter:
   /udm_portal/selfservice,/goto
   Do you want to add http proxy (y/n)[n]? n
   Do you want to add https proxy (y/n)[n]? n
   ```
3. Run: `ReverseProxyCLI apply config`

To configure reverse proxy on the UDM Server:

1. In the UDM Portal, change the SMS and Email templates that contain a URL to point to the DNS of the Reverse Proxy gateway.
2. On the UDM Server run: `udmstop`
3. In `$UDMDIR/conf/udmenv.properties`
   Change the value of this line to:
   ```plaintext
   sam.udm.server.host=<DNS of the gateway>
   ```
4. If you use the shorten URL feature:
   In `$UDMDIR/conf/url_shortener.properties`:
   Change the value of this line to:
   ```plaintext
   url_shortener.server.host_name=<DNS name of the gateway>
   ```
5. Run: `udmstart`
Troubleshooting Reverse Proxy

You can troubleshoot the Reverse Proxy through standard Check Point monitoring tools, such as SmartView Tracker and SmartLog.

**Note** - The destination is not shown.

For advanced troubleshooting instructions, contact Check Point Technical Support.

**To turn on debugging:**

1. In `/opt/CPcvpn-R77/conf/ReverseProxy_conf/httpd_common.conf` file, change `ReverseProxyHandlerTraceLog` parameter, change **Off** to **On**.
   
   See the log files for the XX Product XX: `/opt/CPcvpn-R77/log/trace_log/`

2. In `/opt/CPcvpn-R77/conf/ReverseProxy_conf/httpd_ssl.conf` file, change `LogLevel` parameter, change **emerg** to **debug**, for HTTPS.
   
   See the log files for HTTPS: `$CVPNDIR/log/reverseproxy_ssl_debug_log`

3. In `/opt/CPcvpn-R77/conf/ReverseProxy_conf/httpd_clear.conf` file, change `LogLevel` parameter, change **emerg** to **debug**, for HTTP.
   
   See the log files for HTTP: `$CVPNDIR/log/reverseproxy_debug_log`

**To enable cvpnd logs:**

1. Run: `cvpnd_admin debug set TDERROR_ALL_ALL=5`

2. See the logs in: `$CVPNDIR/log/cvpnd.elg`

To disable, run: `cvpnd_admin debug off`

**To make sure that the Reverse Proxy processes are running:**

1. Run: `ps -ef | grep httpd`

2. In the output, find: `ReverseProxySSL/httpd.conf` (for HTTPS) and `ReverseProxyClear/httpd.conf` (for HTTP).

Configuring More Self-Service Portal Settings

Select which options are displayed in the Self-Service Portal and how they are displayed. Users can only generate certificates for the Remote Access Sites and Remote Access Clients that are displayed in the Portal.

For each **Remote Access Site** and **Instruction Template** you can edit:

- **Display** - When selected, users see the option in the Self-Service Portal. When cleared, users do not see that option.

- **User Portal Display Name** - The name that users will see in the portal for the site or instruction template.

Advanced Configuration for the Self Portal

To manage correct use of certificate generation in the Self Portal, the amount of pending certificates that one user can have at one time is limited to three. These are certificates that were generated but never enrolled on a device. If users reach this limit and try to generate new certificate, a message shows that the user has too many certificates and instructs them to contact an administrator. The administrator can manage the certificates as necessary.
To change the maximum number of certificates for a user:

1. On the UDM server, run: `udmstop`
2. In the UDM configuration file, `$UDMDIR/conf/udmenv.properties`, edit this property:
   ```plaintext
generate.certificate.action.max.pending.certificates=3
```
   where the value is the maximum number of pending certificates that users can have.
3. Save the changes.
4. On the UDM server, run: `udmstart`
Task Scenarios

This chapter discusses how User and Device Management is used in different task scenarios. The procedures in this chapter are for Help Desk administrators defined as UDM administrators.

Configuring New Employee Options

Scenario
A help desk administrator wants to grant a new employee access to network resources. There are a number of customized actions that can be completed.

What to do:
- Define a user account for the new employee (by an Active Directory administrator).
- Assign the user to the necessary AD groups [“Managing User Groups” on page 25].
- If the user requires remote access from a device, create a certificate and send deployment instructions [“Creating and Editing Certificates” on page 21].

Configuring Existing Employee Options

Scenario
A help desk administrator wants to grant an existing employee access to network resources from a new device. There are a number of customized actions that can be completed.

What to do:
- Assign the user to the necessary AD groups [“Managing User Groups” on page 25].
- Create a certificate and send deployment instructions [“Creating and Editing Certificates” on page 21].
- Revoke certificates for devices that are no longer in use [“Revoking Certificates” on page 22].

Denying Employee Access

Scenario
A help desk administrator wants to deny access to network resources for an employee that is no longer employed in the organization. There are a number of customized actions that can be completed.

What to do:
- The UDM administrator can disable the account [“Disabling and Enabling Accounts” on page 24]. Alternatively, the AD administrator can delete the user account or lock the user account in Active Directory.
Task Scenarios

- Revoke valid certificates to remove organizational data from the user’s devices by remote wipe ("Revoking Certificates" on page 22).

Handling Lost Devices

Scenario
An employee loses a device. There are a number of customized actions that can be completed.

What to do:
- Try to find the device.
- Report the incident.
- Revoke valid certificates to remove organizational data from the user’s devices by remote wipe ("Revoking Certificates" on page 22).
UDM with Mobile Threat Prevention

Working with Mobile Threat Prevention

Mobile Threat Prevention protects mobile devices from advanced threats with the Check Point Protect App for iOS and Android. You can use UDM to view and manage Mobile Threat Prevention users from the UDM portal. Mobile Threat Prevention and UDM can also work with an MDM server.

Administrators cannot make changes to the Mobile Threat Prevention account. You must have a valid Mobile Threat Prevention account configured to use these features.

PII filter works with UDM, Mobile Threat Prevention and MDM to filter out personally identifiable information (PII) from outbound traffic. See UDM PII Filter (on page 42).

When an MDM is configured, you can see all Mobile Threat Prevention information in the Mobile Threat Prevention tab of the UDM portal. See Mobile Threat Prevention Secure Browsing with UDM (on page 43).

A mail server that uses SMTP must be configured for UDM to work with Mobile Threat Prevention.

If you need a proxy server to get to the Mobile Threat Prevention server, see Configuring Proxy Servers (on page 41).

Configuring an Mobile Threat Prevention Account

In the UDM Portal, configure the Mobile Threat Prevention server and administrator credentials. You can also enter the details of a Mobile Device Management (MDM) Server that is used with the Mobile Threat Prevention account.

To configure a Mobile Threat Prevention account in the UDM Portal:

1. Make sure SmartDashboard is closed.
2. In the Configuration tab, below Mobile Threat Prevention Settings, click New or Edit. The New or Edit Mobile Threat Prevention Server window opens.
3. Enter:
   - Display Name - A name for the Mobile Threat Prevention administrator account.
   - User Name, Password - Credentials of a Mobile Threat Prevention administrator.
   - Server URL - The URL of the account.
4. Optional: Click Test Connectivity to test the ability to log in to the Mobile Threat Prevention account.
5. Optional: Enter the details of a Mobile Device Management (MDM) Server that is used with the Mobile Threat Prevention account.
   - User Name, Password - Credentials of an MDM administrator.
   - MDM URL - The URL for the MDM account.
6. In the Device Registration Settings area, select to send registration emails to iOS users, Android users, or both.
7. Click OK.
   The Server URL of the configured account shows under Mobile Threat Prevention Settings in the Configuration tab.

8. Click Apply.
   The display name of the configured account shows under Mobile Threat Prevention Settings in the Configuration tab.

9. Refresh the UDM portal to see the new Mobile Threat Prevention tab.

Configuring Proxy Servers

Configure these proxy-related attributes in the UDM configuration file: $UDMDIR/conf/udmenv.properties

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>pii.proxy.udm.server.host.name</td>
<td>Enables PII proxy functionality. Enter The host name or IP address that UDM resides on</td>
<td>Yes</td>
</tr>
<tr>
<td>pii.proxy.next_proxy.server.address</td>
<td>The IP address of an HTTP proxy that UDM can use for internet connectivity</td>
<td>No</td>
</tr>
<tr>
<td>pii.proxy.next_proxy.server.port</td>
<td>The port of an HTTP proxy that UDM can use for Internet connectivity</td>
<td>No</td>
</tr>
</tbody>
</table>

Configuring a White List for MDM Access

You can create a white list to limit the communication that Mobile Threat Prevention can have with the MDM.

To configure a white list for Mobile Threat Prevention to MDM communication:

1. Contact Check Point technical support to configure the content of the white list.
2. In the UDM configuration file: $UDMDIR/conf/udmenv.properties
   Set pii.proxy.mdm.white.list to true.
3. Save changes.
4. Run: udmstop
5. Run: udmstart

Managing Users and Devices

From the Users & Devices tab you can enroll devices to Check Point Protect, the Mobile Threat Prevention App, and revoke devices from the App.

When a device is enrolled, the user gets an email with instructions to:

- Download Check Point Protect - Use the included link or scan the QR code
- Register to the App - Use the included Registration Key and Mobile Threat Prevention Server Address
To enroll a device:
1. In the **Users & Devices** tab, select a user.
2. Under **User Tasks**, click **Enroll to Mobile Threat Prevention**.
3. Click **OK**.
   A registration email is sent to the user.

To revoke a device:
1. In the **Users & Devices** tab, click a user to see the user’s devices.
2. Right-click on a device and select **Revoke from Mobile Threat Prevention**.

**UDM PII Filter**

The **Personally Identifiable Information (PII)** filter works with UDM, Mobile Threat Prevention and MDM to filter out personally identifiable information from outbound traffic in these scenarios:

- UDM to Mobile Threat Prevention Cloud Services communication
- Mobile Threat Prevention Cloud Service to MDM communication (MDM-bound proxy)
- Mobile Threat Prevention Dashboard UI through the UDM portal (Mobile Threat Prevention-bound proxy)

When you configure Mobile Threat Prevention with an MDM server, the PII filter prevents users’ personal information from staying in the Cloud. Check Point encrypts the information in the cloud so it shows as obfuscated in the Mobile Threat Prevention portal. Instead, it shows clearly in the Mobile Threat Prevention tab of the UDM portal.

You must enable PII proxy functionality. See Configuring Proxy Servers (on page 41)

When a PII field is detected on outbound traffic, the filter encrypts its value using a pre-configured AES encryption key. The result is then formatted to resemble the role of the original field (for example, name, email, or phone number), and is marked in a special way to allow future detection of the field value as a PII value. After such encrypted PII values arrive back at the UDM server as part of inbound traffic, their original values are restored. Internal servers are not involved with the PII replacements.

**Advanced PII Filter Encryption**

The encryption key configuration is crucial to PII’s functionality, because it controls value restoration and replacement. PII values that are encrypted with a different AES key than the one currently installed cannot be restored. Instead, a value of N/A is shown.

The encryption key and initialization vector (IV) file are created when the UDM services are started for the first time. The files are:

- **pii_encryption.key**
- **pii_encryption.iv**

Each time the UDM services are restarted, the PII filter looks for these files. If both files are present and valid, they become effective until the UDM services are restarted again. If not, a new pair of key and IV files is generated.
To back up the encryption key and initialization vector for each UDM installation:

1. Connect to the UDM machine with SCP or WinSCP.
2. Browse to the $UDMDIR/conf/ directory. The default directory is /opt/CPudm-R77/conf/.
3. Copy the files pii_encryption.key and pii_encryption.iv to a safe place.

Alternatively, you can choose to use a predefined set of key and IV files that is common to all UDM installations.

To configure a predefined set of key and IV files to use with all UDM installations:

1. On the UDM server, open this file: $UDMDIR/conf/pii_filter.properties
2. Find this attribute and change the value to true.
   
   pii_filter.encryption.use_predefined_key=true
3. This causes the PII filter to use this set of key and IV files:
   
   pii_encryption_predefined.key
   pii_encryption_predefined.iv

   **Caution:** This setup is equivalent to using value obfuscation instead of encryption, because anyone with access to the predefined key can easily restore all PII values.

**Mobile Threat Prevention Secure Browsing with UDM**

You can see the Mobile Threat Prevention dashboard from within the UDM portal, with all PII values restored. This is done through Mobile Threat Prevention-bound HTTP proxy ("MDM-Bound HTTP Proxy" on page 44) and the PII filter ("UDM PII Filter" on page 42). Administrators can only see the device details and cannot make changes to the Mobile Threat Prevention account.

The feature requires a valid Mobile Threat Prevention account.

See the information in the Mobile Threat Prevention tab of the UDM portal, which only shows if a Mobile Threat Prevention account is configured.

The feature also requires UDM configuration that makes the Gaia WebUI inaccessible.

Mobile Threat Prevention Secure Browsing with UDM is not supported in standalone UDM environments.

**To enable Mobile Threat Prevention Secure Browsing with UDM:**

1. To enable the MTP-bound proxy:
   
   a) Backup and this file on the UDM server:
      
      $UDMDIR/apache/conf/udm_gaia_portal_httpd.conf
   
   b) Uncomment these lines to make them active:
      
      ```
      #ProxyPass               /
      http://127.0.0.1:8081/udm_portal/mtp_proxy/
      #ProxyPassReverse        /
      http://127.0.0.1:8081/udm_portal/mtp_proxy/
      ```
   
   2. Restart the Gaia Web services. On the UDM server, run:
      
      ```
      > tellpm process:httpd2
      > tellpm process:httpd2 t
      ```
MDM-Bound HTTP Proxy

Mobile Threat Prevention-Bound Proxy lets the Mobile Threat Prevention Cloud Service access an on-premises MDM server.

Requirements:
- An MDM account is configured in the UDM portal.
- The Mobile Threat Prevention cloud service trusts the UDM server’s SSL server certificate.
- UDM trusts the MDM server’s SSL server certificate.

**Trusting the UDM Server**

To configure the Mobile Threat Prevention Cloud Service to trust the UDM certificate:

1. If your UDM server resides behind a Firewall with NAT, configure the UDM server with a routable IP Address.
2. Retrieve the UDM self-signed certificate from: /web/conf/server.crt
3. Import the retrieved certificate to the Mobile Threat Prevention dashboard:
   a) Log in to your Mobile Threat Prevention account.
   b) Go to Settings > MDM.
   c) Under Advanced Settings, import the retrieved certificate.
   d) Select your MDM service and configure this URL as your server address:
      `https://<UDM Server FQDN URL>/udm_portal/mdm_proxy/<your MDM tenant ID>`
      The rest of the settings are from your MDM account.

Notes:
- The GAIA certificate is not updated automatically when the server’s IP address is changed. Therefore, the IP address of the server and the one on the certificate will be different. If the IP address changes, generate and set a new certificate as described in sk97648 [http://supportcontent.checkpoint.com/solutions?id=sk97648](http://supportcontent.checkpoint.com/solutions?id=sk97648).

**Trusting the MDM Server**

To make the UDM Server trust the MDM Server (if it does not):

1. Get the MDM’s certificate or its CA as a PEM file.
2. Put the PEM file on the UDM server in /var/tmp/MdmServer.crt
3. On the UDM server, run:
   ```
   $JAVA_HOME/bin/keytool -import -trustcacerts -alias company -file /var/tmp/MdmServer.crt -keystore $JAVA_HOME/lib/security/cacerts -storepass changeit
   ```
4. Restart the UDM services. Run:
   - udmstop
   - udmstart
Troubleshooting Scenarios

The procedures in this chapter are for Help Desk administrators defined as UDM administrators.

Users Cannot Reach Network Resources

Scenario
An employee reports that they cannot get to a network resource. A help desk administrator wants to find a solution to the problem.

What to do:
- Search for the user ("Searching for Users" on page 19).
- See the user’s details:
  - Make sure the user is not locked ("Unlocking an Account" on page 24).
  - Make sure the user is assigned to the correct AD groups ("Managing User Groups" on page 25).
- See the recent logs for the user ("Viewing User Logs" on page 28).
- Make sure the device being used has a valid certificate ("Managing Certificates" on page 20).
- Make sure the Security Gateway is connected and that there are no connectivity issues.

Users are Locked Out of Devices

Scenario
There can be two types of scenarios:
- Endpoint - An employee forgot their FDE password and locked the laptop or computer. A help desk administrator wants to unlock the device remotely.
- AD password - An employee forgot their Active Directory password. An incorrect password was entered too many times and the account became locked. A help desk administrator wants to unlock the account and reset the password.

What to do:
- Search for the user ("Searching for Users" on page 19).
- For the Endpoint issue - help remotely (" Giving Remote Help to Full Disk Encryption Users" on page 26).
- For the AD password - unlock the account and reset the password ("Resetting Passwords" on page 23).
Index

A
Active Directory Operations • 23
Advanced Configuration for Suspicious Activity Monitoring • 32
Advanced Configuration for the Self Portal • 36
Advanced PII Filter Encryption • 42
Authentication Tab • 13

B
Before Configuring Suspicious Activity Monitoring • 30

C
Configuring a Mail Server • 13, 16
Configuring a White List for MDM Access • 41
Configuring an HTTP Proxy • 16
Configuring an Mobile Threat Prevention Account • 40
Configuring Capsule Cloud • 17
Configuring Email Templates • 13
Configuring Existing Employee Options • 38
Configuring LDAP Account Units • 10
Configuring LDAP Settings • 15
Configuring More Self-Service Portal Settings • 36
Configuring New Employee Options • 38
Configuring Proxy Servers • 41
Configuring Reverse Proxy on the Mobile Access Gateway • 34
Configuring SMS Provider Settings • 32
Configuring Suspicious Activity Monitoring • 31
Configuring the Endpoint Security Management Server • 17
Configuring the Self-Service Portal • 34
Creating and Editing Certificates • 21
Creating Certificates for Multiple Users • 21
Customizing Instruction Templates • 22

D
Define Properties in the UDM Configuration Files • 30
Defining a UDM Administrator • 14
Disabling and Enabling Access • 38
Disabling and Enabling Accounts • 24
Downloading All UDM Logs • 29

E
Enabling SmartLog • 10
Enabling SSL for Active Directory • 25

G
General Tab • 11
Giving Remote Help to Full Disk Encryption Users • 26

H
Handling Lost Devices • 39

I
Important Information • 3
Installing UDM • 7
Introduction • 6

L
Logging In • 19

M
Managing Certificates • 20
Managing User Groups • 24
Managing Users and Devices • 19, 41
MDM-Bound HTTP Proxy • 44
Mobile Threat Prevention Secure Browsing with UDM • 43
Monitoring Devices • 29
Monitoring Logs and Devices • 28
Multi-Domain Server Configuration • 8

O
Objects Management Tab • 12

R
Resetting Passwords • 23
Revoking Certificates • 22

S
Searching for Users • 19
Self-Service Portal • 34
Sending Cloud Registration Codes • 26
Servers Tab • 11
Setting Up UDM • 10
SmartDashboard Prerequisites • 10
SMS Provider Settings • 31
Suspicous Account Activity Monitoring • 30

T
Task Scenarios • 38
Troubleshooting Reverse Proxy • 35
Troubleshooting Scenarios • 45
Trusting the MDM Server • 45
Trusting the UDM Server • 44

U
UDM PII Filter • 42
UDM with Mobile Threat Prevention • 40
Unlocking an Account • 24
Users are Locked Out of Devices • 45
Users Cannot Reach Network Resources • 45