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 R77.20.01
For more about this release, see the R77.20.01 home page (http://supportcontent.checkpoint.com/solutions?id=sk105123).

Latest Version of this Document
Download the latest version of this document (http://supportcontent.checkpoint.com/documentation_download?ID=39079).
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 R77.20.01 Administration Guide).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 May 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Chapter 1

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.

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>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>
Chapter 2

Installation

In This Section:

Installing UDM........................................................................................................... 6
Multi-Domain Server Configuration........................................................................... 7

The procedures in this chapter are for security administrators.

In this version, you can enable the UDM Portal as a Management blade in these deployments:

- Part of an R77.20.01 deployment - It can enabled on a Security Management Server or Endpoint Security Management Server.
- Part of an R77.20.01 standalone Security Management Server and gateway deployment.
- On its own dedicated Security Management Server.

The UDM Portal can work with a Multi-Domain Security Management environment.

See the R77.20.01 Release Notes for hardware and software requirements.

Installing UDM

To install the UDM Portal:

1. Use the instructions in the E80.61 and R77.20.01 Release Notes to install R77.20.01.
2. After the installation finishes, open SmartDashboard.
3. Open the Management object.
4. In the General Properties > Management tab, make sure that Management & User Portal is selected.
5. Click OK.
6. Install Database.
7. In a standalone environment, install policy.
8. Make sure that UDM is running. Open a browser and go to this URL:
   https://<UDM server machine address or name>/udm_portal
9. Enter the login credentials and the IP address of your Security Management Server

   

   Notes - On your Management Server, make sure that:
   - The UDM Server is defined as a GUI client.
   - In your Firewall Policy, CPMI is allowed from the UDM Server to the Management Server.
Multi-Domain Server Configuration

You can use your R77.20.01 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. On your UDM Server, open this file:
   
   $UDMDIR/bin/cmas_list.conf

2. Add the Domain Management Server to the file with this syntax:
   
   <Domain Management Server ip_address>:WSPort=<Domain Management Server port>
   
   For example: 192.168.12.10:WSPort=30000

3. Run: udmstop

4. 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 (10.0.0.1)
 )
)
```

- The Domain Management Server IP address is 10.0.0.1
- The Domain Management Server Port is 30000
Chapter 3

Setting Up UDM

In This Section:

- SmartDashboard Prerequisites ................................................................................. 8
- Configuring LDAP Settings ..................................................................................... 13
- Configuring a Mail Server ...................................................................................... 13
- Configuring the Endpoint Security Management Server ........................................ 14
- Configuring Capsule Cloud ..................................................................................... 14
- Enabling SSL for Active Directory ........................................................................... 14

The procedures in this chapter are for security administrators.

SmartDashboard Prerequisites

Before Help Desk administrators can use the UDM Portal, 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 managing permissions

Enabling SmartLog

UDM interacts with SmartLog to show logs. If SmartLog is not already enabled in SmartDashboard, enable it. SmartLog must be enabled to see the user's devices as the UDM uses user logs to build the list.

To enable SmartLog in SmartDashboard:

1. Log in to SmartDashboard with your credentials.
2. From the Network Objects tree, double-click the management object.
   The General Properties page of the object 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/tomcat/webapps/udm_portal/WEB-INF/classes/conf/udmenv.properties
2. Edit 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. The system uses an LDAP account unit interface to query and change items in your User Directory. Each Account Unit represents one or more branches of the data maintained on an LDAP server. When a query about a connection or user is sent to the gateway, it chooses the LDAP server defined for the Account Unit.

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 with your credentials.
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 the settings in the applicable tabs:
   - 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**.
Setting Up UDM

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.

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 Mobile Client 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:
   
   - **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.
   
   The text in **Display Text** is the text that shows on the link.
   
   a. **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.
        
        - **Capsule Workspace** - An app that creates a secure container on the mobile device. This app gives users access to internal websites, file shares, and Exchange servers.
        
        - **Capsule Connect** - A full L3 tunnel app that gives users network access to all mobile applications.
   
   b. **Download Application** - Lets users download a Check Point App for their mobile devices.
      
      - **Select the client device operating system**:
        
        - iOS
        
        - Android
      
      - **Select the client type to download**:
        
        - **Capsule Workspace** - An app that creates a secure container on the mobile device. This app gives users access to internal websites, file shares, and Exchange servers.
        
        - **Capsule Connect** - A full L3 tunnel app that gives users network access to all mobile applications.
      
      - **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.

9. Click **OK**.

10. Optional: Click **Preview in Browser** to see a preview of how the email will look.

11. Click **OK**.

**Defining a UDM Administrator**

Make sure to 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
Setting Up UDM

- User and Device Management Configuration - Read/Write (to enable UDM configuration (LDAP and Exchange settings)

  e) In the Monitoring and Logging tab, select these options to enable seeing 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. In the Configuration tab, below LDAP Settings, click New.
   The New LDAP Account Unit window opens.
2. In Display Name, enter a name for the LDAP account unit in UDM.
3. Select the LDAP Account Unit from the list.
4. Select an LDAP Server that is related with the LDAP Account Unit from the list.
5. 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.
6. 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.
7. 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.
8. 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. In the Configuration tab, below Mail Settings, select the applicable Mail Server from the list.
2. 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.
3. 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.
4. Click Apply.
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. In the Configuration tab, below Endpoint Settings, click New.
   The New Endpoint Server window opens.
2. In Display Name, enter a name for the Endpoint Server administrator account.
3. Enter the User Name, Password, and Server Address.
4. Click OK.
   The Endpoint Security Management Server is added to the table. You can edit it or remove it if necessary.
5. 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 24).

   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 send Capsule Cloud registration codes, configure a Capsule Cloud account.

To configure Capsule Cloud:
1. In the Configuration tab, below Cloud Settings, click New or Edit.
   The New Cloud Server window opens.
2. Enter:
   • Display Name - A name for the Capsule Cloud administrator account.
   • User Name, Password - Credentials of a Capsule Cloud administrator
3. Click OK.
   The display name of the configured account shows under Cloud Settings in the Configuration tab.

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/tomcat/webapps/udm_portal/WEB-INF/classes/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 (http://supportcontent.checkpoint.com/solutions?id=sk84620).
2. On the UDM server, go to the file:
   
   $UDMDIR/tomcat/webapps/udm_portal/WEB-INF/classes/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
Chapter 4

Managing Users and Devices

In This Section:

Logging In ............................................................................................................... 16
Searching for Users ................................................................................................ 16
Managing Certificates ............................................................................................. 17
Active Directory Operations .................................................................................... 19
Sending Cloud Registration Codes ......................................................................... 21
Giving Remote Help to Full Disk Encryption Users ................................................ 22

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>Expired - 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>Pending Enrollment - 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>Valid - This status is shown if the enrollment is successful. Otherwise, the certificate status continues to be Pending Enrollment until successful connection.</td>
</tr>
<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 19).
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 14).

**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.

**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 users 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.
   The User Logon Preboot Remote Help window opens.
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.
Chapter 5

Monitoring Logs and Devices

In This Section:

Viewing System Logs ................................................................. 23
Viewing User Logs ................................................................. 23
Monitoring Devices ................................................................. 24

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 logs 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:
'\<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:
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>![Icon]</td>
<td>Represents desktop PCs and laptops</td>
</tr>
<tr>
<td>![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>![Icon]</td>
<td>Connected</td>
</tr>
<tr>
<td>![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.
Chapter 6

Task Scenarios

In This Section:

- Configuring New Employee Options ................................................................. 25
- Configuring Existing Employee Options ............................................................ 25
- Denying Employee Access .................................................................................. 25
- Handling Lost Devices ......................................................................................... 26

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 21).
- If the user requires remote access from a device, create a certificate and send deployment instructions ("Creating and Editing Certificates" on page 18).

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 21).
- Create a certificate and send deployment instructions ("Creating and Editing Certificates" on page 18).
- Revoke certificates for devices that are no longer in use ("Revoking Certificates" on page 19).

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 20). Alternatively, the AD administrator can delete the user account or lock the user account in Active Directory.
- Revoke valid certificates to remove organizational data from the user's devices by remote wipe ("Revoking Certificates" on page 19).

**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 19).
Chapter 7

Troubleshooting Scenarios

In This Section:

Users Cannot Reach Network Resources .............................................................. 27
Users are Locked Out of Devices ........................................................................... 27

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 16).
- See the user's details:
  - Make sure the user is not locked ("Unlocking an Account" on page 20).
  - Make sure the user is assigned to the correct AD groups ("Managing User Groups" on page 21).
- See the recent logs for the user ("Viewing User Logs" on page 23).
- Make sure the device being used has a valid certificate ("Managing Certificates" on page 17).
- 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 16).
- For the Endpoint issue - help remotely ("Giving Remote Help to Full Disk Encryption Users" on page 22).
- For the AD password - unlock the account and reset the password ("Resetting Passwords" on page 20).
Index

A
Active Directory Operations • 19
Authentication Tab • 10

C
Configuring a Mail Server • 11, 13
Configuring Capsule Cloud • 14
Configuring Email Templates • 11
Configuring Existing Employee Options • 25
Configuring LDAP Account Units • 9
Configuring LDAP Settings • 13
Configuring New Employee Options • 25
Configuring the Endpoint Security Management Server • 14
Creating and Editing Certificates • 18
Creating Certificates for Multiple Users • 18
Customizing Instruction Templates • 19

D
Defining a UDM Administrator • 12
Denying Employee Access • 25
Disabling and Enabling Accounts • 20

E
Enabling SmartLog • 8
Enabling SSL for Active Directory • 14

G
General Tab • 9
Giving Remote Help to Full Disk Encryption Users • 22

H
Handling Lost Devices • 26

I
Important Information • 3
Installation • 6
Installing UDM • 6
Introduction • 5

L
Logging In • 16

M
Managing Certificates • 17
Managing User Groups • 21
Managing Users and Devices • 16
Monitoring Devices • 24
Monitoring Logs and Devices • 23
Multi-Domain Server Configuration • 7

O
Objects Management Tab • 10

R
Resetting Passwords • 20
Revoking Certificates • 19

S
Searching for Users • 16
Sending Cloud Registration Codes • 21
Servers Tab • 10
Setting Up UDM • 8
SmartDashboard Prerequisites • 8

T
Task Scenarios • 25
Troubleshooting Scenarios • 27

U
Unlocking an Account • 20
Users are Locked Out of Devices • 27
Users Cannot Reach Network Resources • 27

V
Viewing System Logs • 23
Viewing User Logs • 23