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.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12674
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 December 2011</td>
<td>In Using 3rd Party Android Mail Clients (on page 16) and Advanced Gateway Configuration (on page 18), changed: MobileAppAndroidAllowClientCertExport to MobileAppAllowClientCertExport</td>
</tr>
<tr>
<td>4 October 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Configuring Mobile Access</td>
<td>6</td>
</tr>
<tr>
<td>Licensing Mobile Access</td>
<td>6</td>
</tr>
<tr>
<td>The Mobile Access Wizard</td>
<td>6</td>
</tr>
<tr>
<td>Step 1: Configure a Web Application</td>
<td>6</td>
</tr>
<tr>
<td>Step 2: Configure Authorized Users</td>
<td>7</td>
</tr>
<tr>
<td>The Mobile Access Wizard is Complete</td>
<td>7</td>
</tr>
<tr>
<td>Configuring Mobile Device Support</td>
<td>8</td>
</tr>
<tr>
<td>Initializing Client Certificates</td>
<td>8</td>
</tr>
<tr>
<td>Configuring ActiveSync Applications</td>
<td>8</td>
</tr>
<tr>
<td>Policy Requirements for ActiveSync Applications</td>
<td>9</td>
</tr>
<tr>
<td>Configuring ESOD for Mobile Apps</td>
<td>10</td>
</tr>
<tr>
<td>Creating Trust for Client Connections</td>
<td>11</td>
</tr>
<tr>
<td>Generating Certificate Signing Request</td>
<td>11</td>
</tr>
<tr>
<td>Installing Signed Certificates</td>
<td>12</td>
</tr>
<tr>
<td>Generating the P12 File</td>
<td>12</td>
</tr>
<tr>
<td>Installing the Signed Certificate</td>
<td>13</td>
</tr>
<tr>
<td>Running the Certificate Signing Utility</td>
<td>13</td>
</tr>
<tr>
<td>System Specific Configurations</td>
<td>14</td>
</tr>
<tr>
<td>iPhone/iPad Configurations</td>
<td>14</td>
</tr>
<tr>
<td>Connecting iPhone/iPad Clients to ActiveSync Applications</td>
<td>14</td>
</tr>
<tr>
<td>Getting Logs from iPhones or iPads</td>
<td>14</td>
</tr>
<tr>
<td>Disabling Client SSO</td>
<td>15</td>
</tr>
<tr>
<td>Android Configurations</td>
<td>15</td>
</tr>
<tr>
<td>Browsing to Servers with Untrusted Server Certificates</td>
<td>15</td>
</tr>
<tr>
<td>Session Timeout for Android Devices</td>
<td>15</td>
</tr>
<tr>
<td>Setting Up Androids for Email Access</td>
<td>16</td>
</tr>
<tr>
<td>Getting Logs from Android Clients</td>
<td>17</td>
</tr>
<tr>
<td>Advanced Gateway Configurations for Mobile Devices</td>
<td>18</td>
</tr>
<tr>
<td>Advanced Gateway Configuration</td>
<td>18</td>
</tr>
<tr>
<td>Tuning Web Security</td>
<td>21</td>
</tr>
<tr>
<td>Using Multiple Exchange Servers</td>
<td>21</td>
</tr>
<tr>
<td>Instructions for End Users</td>
<td>23</td>
</tr>
<tr>
<td>iPhone/iPad End User Configuration</td>
<td>23</td>
</tr>
<tr>
<td>Android End User Configuration</td>
<td>24</td>
</tr>
</tbody>
</table>
Introduction

The Mobile Access Software Blade gives remote access connectivity between Mobile Access clients on hand-held mobile devices and the Security Gateway of your organization. This guide also describes the supplement that adds Android support to Check Point gateways.

This Administration Guide explains how to configure the Mobile Access gateway for hand-held devices. To learn about Mobile Access for web browsers, see the Mobile Access Administration Guide for the relevant version of your Security Management Server.

Before installing and configuring this supplement, read the Mobile Access Supplement - Support for Android Release Notes for your version, see sk65314 (http://supportcontent.checkpoint.com/solutions?id=sk65314) for details.

Do the procedures in order:

1. Set up the gateway ("Configuring Mobile Access" on page 6).
2. Install the Mobile Device supplement on the gateway to support Android devices (see the Release Notes for the relevant devices).
3. Install a server certificate signed by a third-party CA.
4. Configure the gateways for the type of device to support ("System Specific Configurations" on page 14).

Your users download the Check Point client from repositories such as: a custom Web server, Google Market, AppStore.
Chapter 1

Configuring Mobile Access

In This Chapter

Licensing Mobile Access 6
The Mobile Access Wizard 6
Configuring Mobile Device Support 8
Initializing Client Certificates 8
Configuring ActiveSync Applications 8
Policy Requirements for ActiveSync Applications 9
Configuring ESOD for Mobile Apps 10

Licensing Mobile Access

You must get a license for the Mobile Access. From the first policy installation on an enabled Mobile Access, the automatic license begins to count down the 30 evaluation days. This license gives access to 10 users. If an extension is necessary, you can get a new 30-day license from the User Center, for 50 users.

To get a license:
1. Log in to your account on the Check Point User Center.
2. Open your My Products page.
3. Select the Mobile Access license.
4. Click License.
5. Install the license on the Mobile Access Security Gateway manually or with SmartUpdate.
For more about licensing, see the License Guide.

The Mobile Access Wizard

The Mobile Access Wizard enables you to easily configure remote access to your network, enabling users to access an internal site remotely. Alternatively, you can configure access to a Demo application.

The Wizard guides you through:
- Creating a Web Application object
- Creating a user group, selecting an existing user group, or selecting LDAP users or groups
- Troubleshooting connectivity between the Security Gateway and the Web application
- Creating a Mobile Access rule that allows a user group to access the Web application

Step 1: Configure a Web Application

Configure a Web application that users will connect to remotely.

If you have an internal Web application, for example, an organizational intranet site or Microsoft Outlook Web Access, it is recommended to configure access to that site. Enter its URL and, optionally, a display name, which is how the application will appear in the portal, for example, Company Intranet.
Note - Domino Web Access (iNotes) applications cannot be defined as the internal Web application using the First Time Wizard.

After entering the details, you can Test connectivity between the gateway and your internal application. If the gateway cannot reach the Web application, the Wizard will list steps that you can take to enable connectivity. You can automatically accept the suggestions, making troubleshooting quick and easy. You can also choose to configure the DNS and proxy settings manually.

If you do not have an internal site, select the Demo application. The Demo application does not need any further details or connectivity tests.

Step 2: Configure Authorized Users

Configure the user or user groups that are allowed to access the Web application/s that you configured in Step 1.

Make a selection to choose which users or groups can access the configured application:

- **Test user**: Create a test user by entering credentials of an internal user who will be allowed to access the application.
- **Users or groups from Active Directory AD.xxx.com**: Define users and groups from the Active Directory that is already configured to work with your environment. This option only appears if the computer running the Wizard is a member of an Active Directory domain.
- **Users or groups from other Active Directory domain**: Define a new Active Directory and an account that will validate user login.

Configuring Users or Groups from an Active Directory

If you selected one of the Active Directory options above, enter a User name and Password that the Security Gateway can use to gain access into the Active Directory and validate users’ credentials. You may want to create a user account for this specific purpose.

Note - Mobile Access does not support Microsoft Active Directory 2000.

A new page opens in which you specify which users from the AD are authorized to access the application. In effect, you are creating a user group on the AD user gateway that you specify.

Under Authorized Users, select one of the following:

- **Your user**: allows access only to you with your AD credentials
- **All users**: allows access to all users defined in the Active Directory
- **Specific user(s)/group(s)**: manually enter AD users and user groups.

The Mobile Access Wizard is Complete

A summary tells you what you have accomplished using the First Time Wizard.

1. Click Finish to complete the Wizard.
2. Wait while the new objects are created.
3. Click OK on the Security Gateway Properties window. You must install the security policy on the Security Gateway in order for your changes to take effect.

Note that the Mobile Access Wizard is only the beginning of configuring comprehensive secure remote access to internal applications. Configure a complete set of applications, access rules, and security requirements in the Mobile Access tab in SmartDashboard.
Configuring Mobile Device Support

Mobile Access for mobile devices gives two-factor authentication with a client certificate and username/password. Mobile devices use two-factor authentication and the Mobile Access portal uses username/password authentication by default. If your company's security policy requires a higher level of security, you can disable the browser portal using these instructions.

To enable support for hand-held devices on the Mobile Access gateway:
1. Double-click the Mobile Access gateway in the Network Objects tree in SmartDashboard.
2. Select Mobile Access.
3. Select the Smartphone Application Connect using Check Point Mobile for Smartphones option.
4. Click OK.

To enable or disable the Mobile Access portal for browser access:
1. Double-click the Mobile Access gateway in the Network Objects tree in SmartDashboard.
2. Select Mobile Access.
3. To enable browser access, select the Web Portal option.
4. To disable browser access, clear the Web Portal option.
5. Click OK.

Initializing Client Certificates

Check Point Mobile for Android uses two-factor authentication, client certificate and username/password. You must make a registration key for each certificate. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.

Note - If you use LDAP or AD, initiating client certificates does not change the LDAP or AD server. If you get an error message regarding LDAP/AD write access, ignore it and close the window to continue.

If your AD server uses UTF-8 encoding for DN strings or user names, do not use the procedure here. Use the instructions in sk65021 (http://supportcontent.checkpoint.com/solutions?id=sk65021).

To initialize a client certificate:
1. On SmartDashboard, open the properties window of the user.
2. Open Certificates.
3. If a user had a certificate previously, click Revoke to revoke the current client certificate.
4. Select New > Registration Key for certificate enrollment.
   A Registration Key is generated.
   Note - The device may ask the user for the Activation Key. This is the same as the Registration Key.
5. Copy the key and send it to the user.

Configuring ActiveSync Applications

If users connect to the Exchange server for synchronized email, calendar and contacts, define ActiveSync applications in SmartDashboard. ActiveSync for mobile device support is available for Microsoft Exchange Server 2007 SP2 or higher.

To configure ActiveSync on Mobile Access gateways:
1. In SmartDashboard, define a new Web Mail Application in Mobile Access tab > Applications > Web Mail.
The **Web mail service** window opens.

![Web mail service - ActiveSyncAppCP](image)

- **Name** - Enter a name that starts with `ActiveSyncApp`.
- **Outgoing Mail Server (SMTP)** - Select the Exchange server.
- **Incoming Mail Server (IMAP)** - Select the Exchange server.
- **SMTP Service** and **IMAP Service** - Select the Exchange server protocol for ActiveSync (`http` or `https`).
- **Mail domain** - Enter the Exchange server Windows domain.
  
  **Note** - The mail domain and Windows domain may be different. Make sure to enter the Windows domain.

1. **Link in Portal** must be filled, but ignored for the ActiveSync application.
2. Click **OK**.
3. In **Mobile Access** tab > **Policy**, add the new ActiveSyncApp and assign user groups to give users access.
4. Install the policy on the Mobile Access gateway.

### Policy Requirements for ActiveSync Applications

- To access ActiveSync, users must belong to a user group that is allowed to access ActiveSync applications.
- Each user must have an email address defined in the **Email Address** field in the properties of an internal user object, or on an LDAP server (for LDAP users).
- If users are internal, their Check Point client passwords must be the same as their Exchange passwords, otherwise ActiveSync will not work.

You can help users the first time they connect to the Mobile Access Web applications from a mobile device. This is a general list of information to send to users. Note that the exact screens that users see depend on the device and system version.

- Give users the Fully Qualified Domain Name (FQDN) of the Mobile Access gateway. An IP address will connect, but is not trusted. FQDN is recommended.
- Make sure each user has the activation key (registration key) for the client certificate.
• Tell users that the password for the Check Point client is their corporate password.

Configuring ESOD for Mobile Apps

Hand-held devices cannot run ESOD components. If your organization has ESOD configured, mobile apps will not be able to access ESOD enforced applications by default.

You can configure access to these blocked applications by configuring an attribute called MobileAppBypassESODforApps.

Note - Mobile apps are not recognized by their HTTP User-Agent header.

To configure the Security Gateway:

1. On the Security Gateway run:
   ```bash
cvpnd_settings set MobileAppBypassESODforApps "true"
   ```
2. Restart the Mobile Access services: `cvprestart`
3. If you use a cluster, copy the `$CVPNDIR/conf/cvpnd.C` file to all cluster members and restart the services on each.
Chapter 2

Creating Trust for Client Connections

Mobile Access for hand-held devices must trust the gateway. If users are denied access to the gateway, the gateway does not have a server certificate that is signed by a third-party.

In This Chapter

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating Certificate Signing Request</td>
<td>11</td>
</tr>
<tr>
<td>Installing Signed Certificates</td>
<td>12</td>
</tr>
</tbody>
</table>

Generating Certificate Signing Request

Before changing the server certificate in the Change Server Certificate section, follow these steps to generate the required certificate and private-key files.

1. From the gateway command line, type `expert` to enter Expert Mode. Press ENTER.
2. Type the current password, and press ENTER.
3. Type `csr_gen <filename>`, and press ENTER; for example:

   ```bash
csr_gen server1
   ```

   Output:

   ```
   [Expert@cpmodule]# csr_gen server1
csr_gen : Creating Key and Certificate Signing Request based on the following information:
   Key Size: rsa:2048
   Number of days to certify the certificates for : 365
   CSR output filename : server1.csr
   Private Key output filename: server1.key
   OpenSSL config file : /opt/CPcvpn-R75.20/conf/openSSL.cnf
   Do you want to continue (y/n)? [y] :
   ```

4. Press ENTER. Output:

   ```
   Do you want the private key file to be encrypted (recommended, but you'll need to remember the password till you install the signed certificate in Mobile Access) (y/n)? [y]
   ```

5. Press ENTER to accept the default. The script then invokes OpenSSL to create the key and CSR. Output:
Installing Signe

d Certificates

Creating Trust for
Client Connections

Page 12

This message informs you about the creation of the server-key file and requests a password to encrypt it. A password is requested, if you chose to encrypt the private-key file.

6. Enter a password and confirm. Output:

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank. For some fields there will be a default value. If you enter '.', the field will be left blank.

7. Fill in the required data according to the guidelines. All fields are optional. The most important field is the Common Name (CN). This should match the site name or the IP address of the gateway. For example: sslvpn.example.com.

Output:

csr_gen : Operation Succeeded
Your Private Key File is : server1.key
Your CSR File is : server1.csr

Important:
If files with these names (server1.csr and server1.key in the above example) already exist on the machine, they will be overwritten without warning.

1. Pass the CSR file to your CA, and keep the *.key private-key file. Make sure you remember the password (if there is one) for the private-key file.

2. Get the signed certificate for the gateway from the CA (in exchange for a fee and after passing an examination). The certificate must be in PEM format (base64 encoded).

Installing Signed Certificates

After you generate the certificate and send it to be signed, do these next procedures.

Generating the P12 File

After you get the Signed Certificate for the gateway from the CA, generate a P12 file that has the Signed Certificate and the private key.

1. Get the Signed Certificate for the gateway from the CA.
   If the signed certificate is in P12 or P7B format, convert these files to a PEM (Base64 encoded) formatted file with a CRT extension.

2. Make sure that the CRT file has the full certificate chain up to a trusted root CA.
   Usually you get the certificate chain from the signing CA. Sometimes it split into separate files. If the signed certificate and the trust chain are in separate files, use a text editor to combine them into one file. Make sure the server certificate is at the top of the CRT file.

3. From the gateway command line, log in to expert mode.

4. Use the *.crt file to install the certificate with the *.key file that you generated.
Installing Signed Certificates

Creating Trust for Client Connections

Installing Signed Certificates

Installing the Signed Certificate

Install the Third Party signed certificate to create Trust between the Mobile Access Software Blade and the clients.

All portals on the same IP address use the same certificate. Define the IP address of the portal in the Portal Settings page for the blade/feature.

1. Import the new certificate to the gateway in SmartDashboard from a page that contains the Portal Settings for that blade/feature. For example:
   - Gateway Properties > Mobile Access > Portal Settings
   - Gateway Properties > SecurePlatform Settings
   - Gateway Properties > Data Loss Prevention
   - Gateway Properties > Identity Awareness > Captive Portal > Settings > Access Settings
   In the Certificate section, click Import or Replace.

2. Install the policy on the gateway.

   Note - The Repository of Certificates on the IPSec VPN page of the SmartDashboard gateway object is only for self-signed certificates. It does not affect the certificate installed manually using this procedure.

Running the Certificate Signing Utility

On gateways managed by R75.x Security Management Servers, do this:

1. View the certificate: SmartDashboard > View > Details > Copy to file.
2. Select Base-64 encoded X.509 (.CER).
3. Put the resulting file on the Mobile Access gateway at: $CVPNDIR/var/ssl/server.crt
   Rename the file extension to crt, if necessary.
   If you have clusters, copy the file to all cluster members.
   If your environment is Multi-Domain Security Management, run this command on the Domain Management Server.
5. Install the policy.

```bash
  cpopenssl pkcs12 -export -out <output file> -in <signed cert chain file> -inkey <private key file>
```

For example:
```
  cpopenssl pkcs12 -export -out server1.p12 -in server1.crt -inkey server1.key
```

b) Enter the certificate password when prompted.
Chapter 3

System Specific Configurations

This chapter describes system specific configurations for iPhones/iPads and Androids. In some instances, end user configuration is necessary. The instructions are placed both in this chapter and in Instructions for End Users (on page 23).

In This Chapter

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone/iPad Configurations</td>
<td>14</td>
</tr>
<tr>
<td>Android Configurations</td>
<td>15</td>
</tr>
</tbody>
</table>

iPhone/iPad Configurations

Note - OS 3.x iPhones support only one Exchange email account. Before users install the new profile, make sure they remove previously configured profiles (Settings > General > Profiles > Configuration Profiles) and other Exchange accounts.

Connecting iPhone/iPad Clients to ActiveSync Applications

Users who see the Mail Setup item can install the ActiveSync profile. This gives users access to their corporate email.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users (on page 23).

To connect to corporate email:
1. Sign in to the Mobile Access site.
2. Tap Mail Setup.
3. Do the on-screen instructions.

Getting Logs from iPhones or iPads

To resolve issues with client devices, tell the users to send you the logs. The iPhone or iPad must have an email account set up.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users (on page 23).

To configure logs:
1. Tap Information.
   Before login, this is on the top right. After login, this is on the bottom right.
2. Tap Send Logs on the navigation bar.
   If you do not have an email account configured on the iPhone, a message shows that one must be configured. After this is done, you must open Check Point Mobile Access again.
   When an email account is configured, the email page opens. The logs are attached.
Note - The email account that the iPhone uses to send the email is the default account. This might not be your organization's ActiveSync account.

If the iPhone is not configured for a destination email address for logs, the email that opens has an empty To field. You can enter the destination address now, or set up a default destination address for Check Point Mobile logs.

To set up a default destination address:
1. Tap Settings.
2. Scroll down to the Check Point Mobile icon and tap it.
3. In the Mobile global settings, enter the address in Logs email.

Disabling Client SSO

Single Sign On (SSO) lets users in a session connect to the Mobile Access gateway, without authenticating when the client starts. If a user cannot access the gateway while SSO is enabled, disable it.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users (on page 23).

To disable SSO on a client:
1. Tap Settings.
2. Scroll down to the Check Point Mobile icon and tap it.
3. In the Mobile global settings, tap the Single Sign On > Enabled switch.

Android Configurations

Browsing to Servers with Untrusted Server Certificates

When browsing from the Android app to a server with an untrusted server certificate, you are denied access and you get this message:

"Some resources on this page reside on an untrusted host."

In some cases, such as in a staging or demo environment, you can enable browsing to servers with untrusted certificates.

Important - Disabling the server certificate validation in the client app is forbidden for production setups since it allows any 3rd-party to intercept the SSL traffic.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users (on page 23).

To disable the server certificate validation for Web applications:
1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap Settings.
4. Enable Allow connection to untrusted servers.

Note - HTTP (non-SSL) requests are always blocked even when this attribute is disabled.

Session Timeout for Android Devices

For Androids, idle timeout cannot be modified or enforced by the device or the gateway.

The only timeout setting that applies to the device is the active session timeout. It is configured in SmartDashboard: Mobile Access Software Blade > Additional Settings > Session > Re-authenticate users every x minutes option. This setting indicates the maximum session length. When this period is reached, the user must log in again. For example, if re-authentication is set to 120 minutes, a user will need to log in again after 2 hours in an active session.
Setting Up Androids for Email Access

Setting up Androids for email access includes configuration on the Exchange server, the Security Gateway, and the hand-held device.

Since the Android native mail client does not support client certificate authentication, you have two options:

- Configure the Security Gateway to not use client certificate authentication (not recommended as this reduces the security of all mobile devices accessing the gateway).
- Configure a 3rd party Android mail client that uses an exported client certificate to let you read emails from the corporate Exchange mail server.

Preparing the Exchange Server for Android Clients

To view emails, configure the Exchange Server to let Android clients bypass the Exchange Server’s device security policy.

To remove Android users from the Exchange Server device security policy:
1. Open Exchange System Manager.
2. Open Global Settings.
3. Right-click Mobile Services and select Properties.
5. Click Exceptions.
6. Click Add and select all Android device users.
7. Click OK.

Preparing the Gateway for ActiveSync with SSL VPN

Most Android devices do not support client certificate authentication for ActiveSync.

Important - If you want to turn off the client certificate authentication to allow Android clients to use ActiveSync, be aware that this will reduce the security of all mobile devices accessing the gateway.

To configure the gateway to not use client certificate authentication:
1. Disable the Client Certificate requirement on the Security Gateway. Run:
   cvpnd_settings set ActiveSyncClientCertificateNeeded "false"
2. Restart the Mobile Access services: cvpnrestart
3. If you use a cluster, copy the $CVPNDIR/conf/cvpnd.C file to all cluster members and restart the services on each.

Using 3rd Party Android Mail Clients

The Android native mail client does not support client certificate authentication but there are some 3rd party mail clients that do support it. To use 3rd party Android mail clients, you must set a gateway property that lets you transfer the client certificate to the mail application.

Note - Only mail clients using SSL and ActiveSync are supported.

Important - Exporting the certificate allows users to access the gateway from any device. Before allowing the export of client certificates, make sure this complies with the corporate policy.

To configure the Security Gateway:
1. On the Security Gateway run:
   cvpnd_settings set MobileAppAllowClientCertExport "true"
2. Restart the Mobile Access services: cvpnrestart
3. If you use a cluster, copy the $CVPNDIR/conf/cvpnd.C file to all cluster members and restart the services on each.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users (on page 23).

**To transfer the client certificate to the 3rd party mail client:**
1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap **Settings**.
4. From the **Export Certificate** option, tap **Export**. The Export Certificate window opens.
   - If the Export Certificate option is disabled, contact the system administrator.
5. Select the certificate format appropriate for your mail client: P12 or PFX.
6. Select the location to save the certificate.
   - The default path is /sdcard (for devices that have an SD card) or an external resource folder (for devices that do not have an SD card).
7. Tap **OK** to save the certificate to the selected location.
   - A window shows: Export succeeded. Certificate password is: _______
8. You can copy the password to the clipboard. You will need the password when you import the certificate to the third party mail app.

After users export the Check Point certificate, they can import the certificate to an external email client, for example Moxier Mail. The certificate lets them read email from the corporate Exchange mail server via the Security Gateway.

**Getting Logs from Android Clients**

To resolve issues with client devices, tell the users to send you the logs.

The next procedure is for end users to configure on their devices. For all end user configuration procedures, see Instructions for End Users (on page 23).

**To enable logs:**
1. Open the Check Point application.
2. Tap **About**.
3. Press the **Menu** button on the device.
4. Tap Write Logs and then Enable.
5. Enter the email address of the system administrator.
6. Tap **OK**.

**To send logs:**
1. Open the Check Point application.
2. Tap **About**.
3. Press the **Menu** button on the device.
4. Tap Send Logs.
5. Select a way to send the logs.
Chapter 4

Advanced Gateway Configurations for Mobile Devices

Use these instructions only if you have directions from Check Point technical support.

In This Chapter

- Advanced Gateway Configuration 18
- Tuning Web Security 21
- Using Multiple Exchange Servers 21

Advanced Gateway Configuration

You can customize client authentication, device requirements, certificate details, and ActiveSync behavior. Use the CLI commands explained here to change the configuration file:

$CVPNDIR/conf/cvpnd.C

Note - Disable Link Translation Domain on Mobile Access gateways before you connect to them with the Android client.

To apply changes:

Restart the Mobile Access services: cvpnrestart

If you use a cluster, copy the $CVPNDIR/conf/cvpnd.C file to all cluster members and restart the services on each.

To set Mobile Access attributes:

cvpnd_settings set <attribute_name> "<value>"

To get the current value of an attribute:

cvpnd_settings get <attribute_name>

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveSyncAllowed (true)</td>
<td>If access to ActiveSync applications is allowed.</td>
</tr>
<tr>
<td>ActiveSyncExchangeServerAuthenticationMethod</td>
<td>Method of forwarding authentication from the Mobile Access gateway to the internal Exchange server.</td>
</tr>
<tr>
<td>(basic)</td>
<td>Valid values: basic, digest, ntlm</td>
</tr>
<tr>
<td>ActiveSyncClientCertificateNeeded (true)</td>
<td>If ActiveSync access for all mobile devices requires a client certificate. Changing this value affects all mobile devices using the gateway.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>MobileAppAllowActiveSyncProfileConfig (true)</td>
<td>Make the automatic ActiveSync Profile configuration for iPhones and iPads available to users. If true, only users with authorization to access ActiveSync applications see this feature. If false, no user sees this feature.</td>
</tr>
<tr>
<td>MobileAppMinRequiredClientOSVersion (3.1)</td>
<td>Minimum operating system version for iPhones and iPads. If a client fails this requirement, user sees Your OS version must be upgraded</td>
</tr>
<tr>
<td>MobileAppAndroidMinRequiredClientOSVersion (2.1)</td>
<td>Minimum operating system version for Android. If a client fails this requirement, user sees Your OS version must be upgraded</td>
</tr>
<tr>
<td>MobileAppMinRecommendedClientOSVersion (3.1)</td>
<td>Recommended operating system version for iPhones and iPads. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than Required value, or Mobile Access will not start.</td>
</tr>
<tr>
<td>MobileAppAndroidMinRecommendedClientOSVersion (2.1)</td>
<td>Recommended operating system version for Android. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than Required value, or Mobile Access will not start.</td>
</tr>
<tr>
<td>MobileAppMinRequiredClientAppVersion (1.3)</td>
<td>Minimum App version required for iPhones and iPads. If a client fails this requirement, user sees Application Update Required</td>
</tr>
<tr>
<td>MobileAppAndroidMinRequiredClientAppVersion (1.0)</td>
<td>Minimum App version required for Android. If a client fails this requirement, user sees Application Update Required</td>
</tr>
<tr>
<td>MobileAppMinRecommendedClientAppVersion (1.3)</td>
<td>Recommended App version for iPhones and iPads. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than Required value, or Mobile Access will not start.</td>
</tr>
<tr>
<td>MobileAppAndroidMinRecommendedClientAppVersion (1.0)</td>
<td>Recommended App version for Android. If a client fails this recommendation, user sees a message but usage continues. Note: value must be equal to or greater than Required value, or Mobile Access will not start.</td>
</tr>
<tr>
<td>MobileAppMinClientOSVersionForProfileConfig (3.1)</td>
<td>Minimum operating system version for iPhone and iPad to configure ActiveSync with the app. If you want data encryption, change this value from the default to 4.0. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>MobileAppAndroidMinClientOSVersionForProfileConfig (2.1)</td>
<td>Minimum operating system version for Android to configure ActiveSync with the app. If you want data encryption, change this value from the default to 3.0. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption.</td>
</tr>
<tr>
<td>MobileAppIncludeLocationInLogs (false)</td>
<td>A GPS feature. When true, iPhones/iPads send physical location data to the gateway, where it is collected and appears in authentication logs.</td>
</tr>
<tr>
<td>MobileAppClientSideTimeout (0)</td>
<td>Timeout (in seconds), controlled by the device. If the active Web application is idle for this amount of time, the end-user is redirected to the login page. This protects sensitive data that a user could have left open on the device. The default zero (0) means that the timeout is taken from the Mobile Access Session option: Disconnect idle sessions. This attribute is not applicable to Android clients.</td>
</tr>
<tr>
<td>MobileAppBypassESODforApps (false)</td>
<td>When true, mobile apps are allowed access to MAB applications whose protection level requires ESOD compliance. Mobile apps can always access the MAB portal.</td>
</tr>
<tr>
<td>MobileAppAllowClientCertExport (false)</td>
<td>When true, allows mobile app clients to export their client certificates to other apps and devices. See Using 3rd Party Android Mail Clients (on page 16).</td>
</tr>
</tbody>
</table>
Tuning Web Security

We recommend using the local IPS Web Intelligence protections that are automatically configured and activated when you enable the Mobile Access blade. If you want to use the IPS profile that you assign to the Security Gateway instead of the local file, make sure that crucial protections are active so that your Security Gateway stays secure.

To change to a Security Gateway IPS profile configuration for Mobile Access instead of the local configuration:
1. Edit the IPS profile assigned to the Security Gateway to include Mobile Access protections.
2. Run:
   ```bash
   cvpnd_settings set use_ws_local_configuration false
   ```
3. When prompted, backup `$CVNDR/conf/cvpnd.C`
4. Restart the Mobile Access processes: `cvpnd restart`

To switch back to the local, automatic IPS settings for Mobile Access:
1. Run:
   ```bash
   cvpnd_settings set use_ws_local_configuration true
   ```
2. Restart the Mobile Access processes: `cvpnd restart`

Using Multiple Exchange Servers

If you have multiple Exchange servers, you can use them all with ActiveSync, if:
- You use Active Directory for authentication.
- Each Security Management Server User Group is assigned to one Exchange server.

To configure ActiveSync for multiple Exchange servers:
1. Add a new ActiveSyncApp for each Exchange server.
2. In `Policy > Access to Applications`, assign each AD user group to one of these applications.
   Each Exchange Server ActiveSyncApp can have multiple AD user groups assigned to it, but no group can be assigned to more than one server.

   Example:
   Exchange Server 1 is used by ActiveSyncAppCP, and Exchange Server 2 is used by ActiveSyncApp_bck.
   One group, Partners, is assigned to ActiveSyncAppCP. Users in Partners get their email from Exchange Server 1.
   Two groups, Customers and Mobile-vpn-user, are assigned to ActiveSyncApp_bck. Users in these groups get their email from Exchange Server 2.
3. Configure the Security Gateway configuration file with these guidelines:
   - Each attribute must have the same number of elements as the other attributes, in the same sequence.
   - Elements are separated by commas, without spaces.
   - If there is a space in one of the element values, you must use quotes around the full element list.
   - To set an attribute value, run: `cvpnd_settings set <attribute_name> "<value>"
   - To see an attribute value, run: `cvpnd_settings get <attribute_name>`

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileAppProfileNames ()</td>
<td>List of profiles. Each profile name must match a configured ActiveSync application.</td>
</tr>
<tr>
<td></td>
<td>A typical ActiveSync application object is actually a WebMail application object beginning with the name ActiveSyncApp.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MobileAppProfileDisplayNames ()</td>
<td>How the user sees the profiles.</td>
</tr>
<tr>
<td>MobileAppExchangeDomainNames ()</td>
<td>Exchange Server domains of each profile.</td>
</tr>
<tr>
<td>MobileAppSslvpnHostNames ()</td>
<td>Which Mobile Access gateway to use as a proxy for each ActiveSync profile. Even if multiple profiles use the same gateway, it must be listed as many times as there are profiles.</td>
</tr>
</tbody>
</table>

Example:

```plaintext
:MobileAppProfileNames (ActiveSyncApp_1,ActiveSyncApp_2,ActiveSyncApp_3)
:MobileAppProfileDisplayNames ("NY,London,Berlin")
:MobileAppExchangeDomainNames (AD,mydomain.co.uk,ad.example.co.de)
:MobileAppSslvpnHostNames (sslvpn.ex.com,sslvpn.ex.com,sslvpn.ex.com)
```

4. Restart the Mobile Access services: `cvpnrestart`.
   If you use a cluster, copy the `$CVFNDIR/conf/cvpnd.C` file to all cluster members and restart the services on each.

5. Install Policy.
Chapter 5

Instructions for End Users

Give these instructions to end users for configuring their mobile devices to work with Mobile Access.

In This Chapter

iPhone/iPad End User Configuration
Android End User Configuration

iPhone/iPad End User Configuration

Do these procedures on your iPhone/iPad so you can work with Mobile Access.
Before you start, make sure that your administrator gives you:

- The name of the site you will connect to.
- The required Registration key (also called Activation key).

**Important** - Do only the procedures that your network administrator has instructed you to do.

To connect to the corporate site:
1. Get the Check Point Mobile app from the App Store.
2. When prompted, enter the:
   - Site Name
   - Registration key

To connect to corporate email:
1. Sign in to the Mobile Access site.
2. Tap **Mail Setup**.
3. Do the on-screen instructions.
4. When asked for the password, enter the Exchange password.

To configure logs:
1. Tap **Information**.
   Before login, this is on the top right. After login, this is on the bottom right.
2. Tap **Send Logs** on the navigation bar.
   If you do not have an email account configured on the iPhone, a message shows that one must be configured. After this is done, you must open Check Point Mobile Access again.
   When an email account is configured, the email page opens. The logs are attached.

   **Note** - The email account that the iPhone uses to send the email is the default account. This might not be your organization's ActiveSync account.

   If the iPhone is not configured for a destination email address for logs, the email that opens has an empty **To** field. You can enter the destination address now, or set up a default destination address for Check Point Mobile logs.

To set up a default destination address:
1. Tap **Settings**.
2. Scroll down to the **Check Point Mobile** icon and tap it.
3. In the Mobile global settings, enter the address in Logs email.

To disable SSO on a client:
1. Tap Settings.
2. Scroll down to the Check Point Mobile icon and tap it.
3. In the Mobile global settings, tap the Single Sign On > Enabled switch.

Android End User Configuration

Do these procedures on your Android device so you can work with Mobile Access.

Before you start, make sure that your administrator gives you:
- The name of the site you will connect to.
- The required Registration key (also called Activation key).

⚠️ Important - Do only the procedures that your network administrator has instructed you to do.

To connect to the corporate site:
1. Get the Check Point Mobile app from the Android Market.
2. When prompted, enter the:
   - Site Name
   - Registration key

To enable logs:
1. Open the Check Point application.
2. Tap About.
3. Press the Menu button on the device.
4. Tap Write Logs and then Enable.
5. Enter the email address of the system administrator.
6. Tap OK.

To send logs:
1. Open the Check Point application.
2. Tap About.
3. Press the Menu button on the device.
4. Tap Send Logs.
5. Select a way to send the logs.

To disable the server certificate validation for Web applications:
1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap Settings.
4. Enable Allow connection to untrusted servers.

To transfer the client certificate to the 3rd party mail client:
1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap Settings.
   If the Export Certificate option is disabled, contact the system administrator.
5. Select the certificate format appropriate for your mail client: P12 or PFX.
6. Select the location to save the certificate.
   The default path is /sdcard (for devices that have an SD card) or an external resource folder (for devices that do not have an SD card).
7. Tap **OK** to save the certificate to the selected location.
   A window shows: Export succeeded. Certificate password is: _______
8. You can copy the password to the clipboard. You will need the password when you import the certificate to the third party mail app.