R75 Hotfix

Support for Check Point Mobile for iPhone and Application Control Detection of Skype

Release Notes

11 April 2011
© 2011 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.
Important Information

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

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11950
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>11 April 2011</td>
<td>Fixed the uninstall path (&quot;Uninstalling the Hotfix&quot; on page 6).</td>
</tr>
<tr>
<td>27 February 2011</td>
<td>Configuration of support for Check Point Mobile for iPhone and iPad moved to Check Point Mobile for iPhone and iPad R75 Gateway Configuration Instructions (<a href="http://supportcontent.checkpoint.com/documentation_download?ID=11980">http://supportcontent.checkpoint.com/documentation_download?ID=11980</a>)</td>
</tr>
<tr>
<td>27 February 2011</td>
<td>Improved installation instructions (&quot;Installing the Hotfix&quot; on page 5)</td>
</tr>
<tr>
<td>24 February 2011</td>
<td>Improved formatting and document layout; configuration of Client Certificate Authentication moved to sk61060 (<a href="http://supportcontent.checkpoint.com/solutions?id=sk61060">http://supportcontent.checkpoint.com/solutions?id=sk61060</a>)</td>
</tr>
<tr>
<td>14 February 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.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R75 Hotfix Support for Check Point Mobile for iPhone and Application Control Detection of Skype Release Notes).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>In This Document</td>
<td>5</td>
</tr>
<tr>
<td>What’s New</td>
<td>5</td>
</tr>
<tr>
<td>Installation</td>
<td>5</td>
</tr>
<tr>
<td>Installing the Hotfix</td>
<td>5</td>
</tr>
<tr>
<td>Build Numbers</td>
<td>6</td>
</tr>
<tr>
<td>Uninstalling the Hotfix</td>
<td>6</td>
</tr>
<tr>
<td>Configuring Support for Check Point Mobile for iPhone and iPad</td>
<td>7</td>
</tr>
<tr>
<td>Configure the Mobile Access Software Blade</td>
<td>7</td>
</tr>
<tr>
<td>Enabling Mobile Access Software Blade</td>
<td>7</td>
</tr>
<tr>
<td>Licensing the Mobile Access Security Gateway</td>
<td>7</td>
</tr>
<tr>
<td>Configure iPhone Support</td>
<td>8</td>
</tr>
<tr>
<td>Connect Clients to Web Applications</td>
<td>8</td>
</tr>
<tr>
<td>Initializing Client Certificates</td>
<td>8</td>
</tr>
<tr>
<td>Connecting Clients to the Site</td>
<td>9</td>
</tr>
<tr>
<td>Connect Clients to ActiveSync Applications</td>
<td>9</td>
</tr>
<tr>
<td>Configuring ActiveSync Applications</td>
<td>9</td>
</tr>
<tr>
<td>Configuring Users to Access ActiveSync Applications</td>
<td>9</td>
</tr>
<tr>
<td>Connecting Clients to ActiveSync Applications</td>
<td>9</td>
</tr>
<tr>
<td>Advanced Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Advanced Gateway Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Customizing ActiveSync Profiles</td>
<td>12</td>
</tr>
<tr>
<td>Using Multiple Exchange Servers</td>
<td>12</td>
</tr>
<tr>
<td>Supporting ActiveSync for Symbian Devices</td>
<td>13</td>
</tr>
<tr>
<td>Tuning Web Security</td>
<td>13</td>
</tr>
<tr>
<td>Creating Trust for Client Connections</td>
<td>14</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>15</td>
</tr>
<tr>
<td>Getting Logs from Clients</td>
<td>15</td>
</tr>
<tr>
<td>Disabling Client SSO</td>
<td>15</td>
</tr>
<tr>
<td>Known Limitations</td>
<td>16</td>
</tr>
</tbody>
</table>
In This Document

This Release Notes document provides essential operating requirements and describes known issues for R75 Hotfix Support for Check Point Mobile for iPhone and Application Control Detection of Skype. Review this information before setting up R75 Hotfix Support for Check Point Mobile for iPhone and Application Control Detection of Skype.

What's New

This hotfix provides support for:

- Mobile Access Software Blade: Supports Check Point Mobile for iPhone and iPad
  - Access to Web applications
  - Access to email, calendar, and contacts
- Two-factor authentication with client certificate and username/password

This hotfix can only be installed on R75 Security Management servers and Security Gateways.

Installation

Before you install this hotfix, make sure that you have R75 installed on the Security Gateway and Security Management server.

Check Point Mobile for iPhone and iPad

Before you install the hotfix, make sure that the Mobile Access Software Blade is installed on the Security Gateway.

To configure a Security Gateway to accept connections from Check Point Mobile for iPhone and iPad, you must:

1. Install this hotfix ("Installing the Hotfix" on page 5) on a SecurePlatform Security Gateway and on a SecurePlatform, Windows, Linux or Solaris Security Management server.
2. Do the instructions in the Check Point Mobile for iPhone and iPad R75 Gateway Configuration Instructions. ([http://supportcontent.checkpoint.com/documentation_download?ID=11980](http://supportcontent.checkpoint.com/documentation_download?ID=11980))

Skype Detection

To detect Skype traffic, you must:

1. Enable the Application Control Software Blade on a SecurePlatform, Windows or IPSO Security Gateway.
2. Install this hotfix ("Installing the Hotfix" on page 5) on the Security Gateway.
3. After you install the hotfix, make sure that you have the latest online package for Application Control.

Installing the Hotfix

To install this hotfix on SecurePlatform, Linux, Solaris or Windows from the CLI:

1. Backup the following directories:
   - $CVPNDIR (For SecurePlatform Security Gateways only)
   - $FWDIR
2. Download the installation file for your platform:
Installation File

<table>
<thead>
<tr>
<th>Platform</th>
<th>Installation File</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform and Linux (Open Servers and Appliances)</td>
<td>Check_Point_R75_iPhone_Skype.linux.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11951">http://supportcenter.checkpoint.com/file_download?id=11951</a>)</td>
</tr>
<tr>
<td>Windows</td>
<td>Check_Point_R75_iPhone_Skype.windows.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11953">http://supportcenter.checkpoint.com/file_download?id=11953</a>)</td>
</tr>
<tr>
<td>Solaris</td>
<td>Check_Point_R75_iPhone_Skype.solaris2.tgz (<a href="http://supportcenter.checkpoint.com/file_download?id=11954">http://supportcenter.checkpoint.com/file_download?id=11954</a>)</td>
</tr>
</tbody>
</table>

3. Copy the hotfix to a temporary directory.
4. Extract the hotfix and run:
   - For SecurePlatform, Linux, or Solaris: ./UnixInstallScript
   - For Windows: setup.exe
5. At the end of the installation, reboot the machine.

To install this hotfix on IPSO from the CLI:

1. Download the hotfix for IPSO: Check_Point_R75_iPhone_Skype.IPSO6.2.tgz (http://supportcenter.checkpoint.com/file_download?id=11952)
2. Copy the hotfix to a temporary directory.
3. Extract the hotfix and run the executable file.
4. At the end of the installation, run the `cpstop` and `cpstart` commands.

Build Numbers

This table contains the software products updated in this release and their build numbers. To confirm that the hotfix is installed, run the version command for each product. If the command returns the build number listed, the hotfix is installed.

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Build No.</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>012</td>
<td><code>fw ver -k</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is Check Point VPN-1(TM) &amp; FireWall-1(R) - Build 012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>kernel: - Build 012</td>
</tr>
<tr>
<td>Mobile Access</td>
<td>005</td>
<td><code>cvpn_ver</code></td>
</tr>
</tbody>
</table>

Uninstalling the Hotfix

To uninstall this hotfix on SecurePlatform, Linux, Solaris or Windows from the CLI:

2. Run: `cd /opt/CPUninstall/R75.00.003/`
3. Run: `./UnixUninstallScript`
4. Reboot.
   If you have a problem during the uninstall, restore the directories that you backed up during the installation process and contact the Check Point Support Center for assistance.

To uninstall this hotfix on IPSO from the CLI:

- Run: `/opt/CPsuite-R75/UnixUninstallScript`
Configuring Support for Check Point Mobile for iPhone and iPad

To connect from the Check Point Mobile app to the Security Gateway, do this workflow:

1. Set up the gateway. ("Configure the Mobile Access Software Blade" on page 7)
2. Enable support for iPhone and iPad on the gateway ("Configure iPhone Support" on page 8).
3. Connect clients:
   - to Web Applications ("Connect Clients to Web Applications" on page 8)
   - to ActiveSync Applications. ("Connect Clients to ActiveSync Applications" on page 9)
4. Install a server certificate signed by a third-party. ("Creating Trust for Client Connections" on page 14)

Configure the Mobile Access Software Blade

Before you enable Check Point Mobile for iPhone and iPad, you must set up the Mobile Access Software Blade.

Enabling Mobile Access Software Blade

When you enable the Mobile Access Software Blade, a wizard opens. In the wizard you set up Web applications and configure user access. When you are done, Mobile Access gets an automatic 30-day evaluation license. For more details about licensing, refer to the R75 Mobile Access Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11673).

Licensing the Mobile Access Security Gateway

You must get a license for the Mobile Access Software Blade. After the first policy installation on an enabled Mobile Access blade, 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.
Configure iPhone Support

You can enable support for iPhone and iPad to allow these devices to access Web applications and ActiveSync with the Check Point Mobile for iPhone and iPad.

When you enable the Mobile Access Software Blade, all users can authenticate to the gateway with the iPhone app and with the Mobile Access portal. To change the authentication method for the Mobile Access portal, refer to the R75 Mobile Access Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11673). Or, you can disable the Mobile Access portal.

To enable support for iPhone and iPad on the Mobile Access gateway:

1. On the Mobile Access gateway, run:
   cvpnd_settings set MobileAppAllowed "true"
2. Restart the Mobile Access Software Blade services: cvpnrestart

To disable the Mobile Access portal for all other remote access traffic:

- Run: toggleCvpnPortal off

To enable the portal for all remote access traffic:

- Run: toggleCvpnPortal on

Note - If you use a cluster, repeat each of these actions for all members of a cluster.

Connect Clients to Web Applications

Web applications configured for the Mobile Access Software Blade are also available to users of Check Point Mobile for iPhone and iPad. For more details about Mobile Access, refer to the R75 Mobile Access Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11673).

Initializing Client Certificates

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

You can only have one certificate at a time for a single user.

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. Click Initiate to initiate a registration key for a new client certificate.
   A Registration Key is generated.
5. Copy the key and send it to the user.

Note - The device may ask the user for the Activation Key. This is the same as the Registration Key.

Note - If you use LDAP or AD, when you initiate client certificates it does not make changes to the LDAP or AD server. If you get a message that says otherwise, close the window with the close (X) button.
Connecting Clients to the Site
You can help users the first time they connect to the Mobile Access Web applications from Check Point Mobile for iPhone and iPad.

- Make sure the users have the FQDN of the Mobile Access gateway. An IP address will connect, but is not trusted. Therefore, we recommend the FQDN only.
- Make sure each user has the activation key (registration key) for the client certificate.
- If the users see a server certificate warning, and you did not yet install a trusted server certificate signed by a third-party CA, you can tell the users to tap Accept.
- Make sure that each user knows the password for the app is the same password that they use to access the Mobile Access portal.

After a successful sign-in, the user will see the Web applications to which the user has permissions.

Connect Clients to ActiveSync Applications

Configuring ActiveSync Applications
If users connect to the Exchange server for synchronized email, calendar and contacts, define ActiveSync applications in SmartDashboard.

ActiveSync for iPhone and iPad 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.
   - 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.
   - 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.

Configuring Users to Access ActiveSync Applications
- To access ActiveSync, users must belong to a user group that is allowed to access an ActiveSync application (configured in the previous section).
- Each user must have an email address defined in one of these places:
  - The Email Address field in the properties of an internal user object.
  - On an LDAP server (for LDAP users).
- If users are internal users, their Check Point passwords must be identical to their Exchange passwords, otherwise ActiveSync will not work.

Connecting Clients to ActiveSync Applications
Users who see the Mail Setup item can install the ActiveSync profile. This gives users access to their corporate email.
Note - OS 3.x iPhones support only one Exchange profile. Before users install the new profile, make sure they remove previously configured profiles (Settings > General > Profiles > Configuration Profiles).

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

Advanced Configuration

In This Section

- Advanced Gateway Configuration
- Customizing ActiveSync Profiles
- Using Multiple Exchange Servers
- Supporting ActiveSync for Symbian Devices
- Tuning Web Security
- Creating Trust for Client Connections

Advanced Gateway Configuration

You can customize client authentication, device requirements, certificate details, and ActiveSync behavior.

Note - The Link Translation Domain feature is not supported with iPhones. Disable Link Translation Domain on Mobile Access gateways before you connect to them with the iPhone app.

To configure the Mobile Access gateway:
1. For each attribute that you want to configure, run:
   `cvpnd_settings set <attribute_name> "<value>"

   Note - To check the current value of an attribute run:
   `cvpnd_settings get <attribute_name>`

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileAppAllowed (default value: false)</td>
<td>Change to true to enable Check Point Mobile for iPhone and iPad features.</td>
</tr>
<tr>
<td>MobileAppMinRequiredClientOSVersion (default value: 3.1)</td>
<td>Minimum operating system version for iPhone/iPad. If a client fails this requirement, user sees Your OS version must be upgraded.</td>
</tr>
<tr>
<td>MobileAppMinRecommendedClientOSVersion (default value: 3.1)</td>
<td>Recommended operating system version for iPhone/iPad. 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>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MobileAppMinRequiredClientAppVersion (default value: 1.2)</td>
<td>Minimum App version required for iPhone/iPad. If a client fails this requirement, user sees Application Update Required</td>
</tr>
<tr>
<td>MobileAppMinRecommendedClientAppVersion (default value: 1.2)</td>
<td>Recommended App version for iPhone/iPad. If a client fails this recommendation, user sees a message but usage continues. <strong>Note</strong>: value must be equal to or greater than Required value, or Mobile Access will not start.</td>
</tr>
<tr>
<td>MobileAppClientCertificateNeeded (default value: true)</td>
<td>Enforce certificate requirement to connect to the Mobile Access gateway.</td>
</tr>
<tr>
<td>MobileAppAllowActiveSyncProfileConfig (default value: true)</td>
<td>Make the automatic ActiveSync Profile configuration available to users. If this is true, only users with authorization to access ActiveSync applications see this feature. If this is false, no user sees this feature.</td>
</tr>
<tr>
<td>MobileAppMinClientOSVersionForProfileConfig (default value: 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 <strong>4.0</strong>. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption.</td>
</tr>
<tr>
<td>MobileAppClientSideTimeout (default value: 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.</td>
</tr>
<tr>
<td>MobileAppIncludeLocationInLogs (default value: 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>ActiveSyncAllowed (default value: true)</td>
<td>Enable ActiveSync features.</td>
</tr>
<tr>
<td>ActiveSyncClientCertificateNeeded (default value: true)</td>
<td>If true, ActiveSync access requires a client certificate.</td>
</tr>
<tr>
<td>ActiveSyncClientCertMatchUserName (default value: true)</td>
<td>If a client certificate is used, and this attribute is true, the certificate must belong to the ActiveSync user.</td>
</tr>
<tr>
<td>ActiveSyncExchangeServerAuthenticationMethod (default value: basic)</td>
<td>Method of forwarding authentication from the Mobile Access gateway to the internal Exchange server. <strong>Valid values</strong>: basic, digest, ntlm</td>
</tr>
</tbody>
</table>

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

Customizing ActiveSync Profiles

ActiveSync Exchange features are configured by an iPhone Configuration Profile. Check Point Mobile for iPhone and iPad automatically creates an individual profile for each user, with an embedded client certificate. It uses the parameters of the ActiveSync application objects that you define.

You can customize the profile. For example, if you have multiple Exchange servers, you can configure multiple profiles. We use this example to show how to customize profiles with the ActiveSync parameters. To do a simpler customization (for example, to change the profile names), do only the steps that tell how to change the configuration file.

Using Multiple Exchange Servers

If you have multiple Exchange servers, you can use them all with ActiveSync, if:

- You use Active Directory.
- Each group of users 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 group to one of these applications.
   Each Exchange Server ActiveSyncApp can have multiple AD groups assigned to it, but no group can be assigned to more than one server.
   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 profiles and Exchange server domains. Set the attributes below according to 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.
   - For each attribute that you want to configure, run:
     cvpnd_settings set <attribute_name> "<value>"
   The attributes are described in the table below.

   **Note** - To check the current value of an attribute 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. A typical ActiveSync application object is actually a WebMail application object beginning with the name ActiveSyncApp.</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>
</tbody>
</table>
### Attribute | Description
--- | ---
MobileAppSslvpnHostNames () | 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.

Example:

```
: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)
```

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

5. Install Policy.

### Supporting ActiveSync for Symbian Devices

Mobile devices with the Symbian OS behave differently than iPhones and iPads. A Symbian device presents its client certificate automatically only if the first URL it accesses on the gateway demands the certificate. If the URL does not request the certificate, the device never presents it. This is an issue because this supplement enforces client certificate authentication by default.

To make sure Symbian devices can use ActiveSync:

1. Use `sysconfig` to define a dedicated virtual IP address on the Mobile Access gateway.
2. Define a dedicated FQDN for Symbian clients. For example: `symbian.sslvpn.example.com`
3. Configure the DNS servers to map the dedicated FQDN to the virtual IP.
4. On the gateway, back up `/etc/rc.local` and open it.
5. Add these `fw ctl` commands to `/etc/rc.local`:

   ```
   # The force_client_cert_auth flag enables Symbian support.
   fw ctl set int force_client_cert_auth 1
   # The IP address below is an example of the virtual IP.
   fw ctl set string client_cert_auth_dest_ip 192.0.2.40
   ```

6. Run the script or reboot the gateway.

### 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:

   ```
   cvpnd_settings set use_ws_local_configuration false
   ```
3. When prompted, backup `$CVPNDIR/conf/cvpnd.C`
4. Restart the Mobile Access processes: `cvpnstop, cvpnstart`

To switch back to the local, automatic IPS settings for Mobile Access:

1. Run:

   ```
   cvpnd_settings set use_ws_local_configuration true
   ```
2. Restart the Mobile Access processes: `cvpnstop, cvpnstart`
Creating Trust for Client Connections

Check Point Mobile clients must trust the gateway. If users see a message that the server is not trusted, the gateway does not have a server certificate that is signed by a third-party.

Make sure that the server certificate of the Mobile Access gateway is signed by a trusted third-party Certification Authority (for example, EnTrust). This CA must be also trusted by the device. The certificate must replace the self-signed (ICA) certificate.

Generating the Certificate Signing Request

First, generate a Certificate Signing Request (CSR). The CSR is for a server certificate, because the gateway acts as a server to the clients.

Note - This procedure creates private key files. If private key files with the same names already exist on the machine, they are overwritten without warning.

1. From the gateway command line, log in to expert mode.
2. Run:

```
copenssl req -new -out <CSR file> -keyout <private key file> -config $CPDIR/conf/openssl.cnf
```

This command generates a private key. You see this output:

```
Generating a 2048 bit RSA private key
.
.
.
writing new private key to 'server1.key'
Enter PEM pass phrase:
```

3. Enter a password and confirm. You see this message:

```
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.
```

Fill in the data.

- The Common Name field is mandatory. This field must have the Fully Qualified Domain Name (FQDN). This is the site that users access. For example: portal.example.com.
- All other fields are optional.

4. Send the CSR file to a trusted certificate authority. Make sure to request a Signed Certificate in PEM format. Keep the .key private key file.

Installing the Signed Certificate

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

To install the signed certificate:

1. Get the Signed Certificate for Mobile Access from the certificate authority.
   If the signed certificate is in P12 or P7B format, convert these files to PEM format.
   - To convert a P12 File to PEM format: Run the `$CVPNDIR/bin/p12ToPem` script. See sk30997.
   - To convert a P7B File to PEM format: Run the `$CVPNDIR/bin/p7bToPem` script. See sk31589.
2. Install the *.crt file with the *.key file that was generated by CSR_gen.
   a) If you already have a signed certificate file, back up this directory from a gateway or cluster member: `$CVPNDIR/var/ssl`
   b) Run: `$CVPNDIR/bin/InstallCert <certfile> <keyfile> '<passwd>'`
   c) Run: `cvpnrestart`
3. If you use clusters:
   a) Copy all $CVPNDIR/var/ssl/server* files to the same path on all other cluster members.
   b) On each member that the files are copied to, run: cvpnrestart
4. Run: certificate_signing_utility -upgrade
   If your environment is Multi-Domain Security Management, run this command on the Domain Management Server.
5. Install the policy.
6. Make sure that the new certificate is presented by the gateway portal to clients.
   
   **Note** - You may have to do Install Policy more than once.

You can also use the SmartDashboard to import a P12 certificate for the Mobile Access portal to use.

**To import a certificate in the SmartDashboard:**
- In the gateway properties, go to Mobile Access > Portal Settings and click Import.

---

**Troubleshooting**

**Getting Logs from Clients**

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

**Tell the user to:**
1. Tap the Information icon. (Before login, this is on the top right. After login, this is on the bottom right.)
2. Tap the Send Logs button on the navigation bar.
   - If the user does not have an email account configured on the iPhone, a message shows the user that one must be configured. After this is done, the user 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. The user 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 the iPhone Settings icon.
   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 application is invoked again. If a user cannot access the gateway while SSO is enabled, disable it.

**To disable SSO on a client, tell the user to:**
1. Tap the iPhone Settings icon.
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.
## Known Limitations

### Check Point Mobile for iPhone and iPad

<table>
<thead>
<tr>
<th>ID</th>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>00624534</td>
<td>The Link Translation Domain feature is not supported with iPhones. Disable Link Translation Domain on Mobile Access gateways before you connect to them with the iPhone App.</td>
</tr>
<tr>
<td>00597730</td>
<td>Interactive Simultaneous Login Prevention (SLP) is not supported.</td>
</tr>
<tr>
<td>00568280</td>
<td>Application protection levels that include authentication settings are not supported.</td>
</tr>
<tr>
<td>00644551</td>
<td>After you configure your mail settings, the Mail Setup application is removed from the Check Point Mobile application list. If you need to configure the mail settings again, tap the Options icon in the bottom-left corner of the Check Point Mobile application and set &quot;Enable Mail Settings&quot; to On. Now the Mail Setup application is listed again in the Check Point Mobile application list.</td>
</tr>
<tr>
<td>00643766</td>
<td>Internal user passwords can be up to 8 ASCII characters.</td>
</tr>
</tbody>
</table>

### Skype Detection in Application Control

<table>
<thead>
<tr>
<th>ID</th>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>00641021</td>
<td>Skype versions 3 and 4 are detected. Skype version 5 is not detected.</td>
</tr>
<tr>
<td>00641055</td>
<td>You must allow UDP traffic in order to detect Skype traffic. If UDP traffic is blocked, Skype traffic is not detected.</td>
</tr>
</tbody>
</table>
| 00643231 | During installation on IPSO, you see this error message:  
/ opt/CPsuite-R75/bin/hook_fw1_HOTFIX_FOXX_SSLVPN_IPHONE_HF_002:  
/bin/chown: not found  
You can ignore this message. The hotfix installs successfully. |