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=24851)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R77.30 home page

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 April 2015</td>
<td><strong>New for R77.30 Gateways:</strong></td>
</tr>
<tr>
<td></td>
<td>Session Visibility and Management Utility (on page 167)</td>
</tr>
<tr>
<td></td>
<td>Kerberos Constrained Delegation (on page 70)</td>
</tr>
<tr>
<td></td>
<td>Certificate Attribute Forwarding (on page 72)</td>
</tr>
<tr>
<td></td>
<td>Configuring Link Translation Domains in SmartDashboard (on page 43)</td>
</tr>
<tr>
<td></td>
<td>Configuring a SAML Web Application (on page 41)</td>
</tr>
<tr>
<td></td>
<td><strong>Updated:</strong> Names of Check Point Mobile Apps throughout the document</td>
</tr>
<tr>
<td></td>
<td>Managing Capsule Workspace Settings (on page 103)</td>
</tr>
<tr>
<td></td>
<td>Push Notifications (on page 106)</td>
</tr>
<tr>
<td>10 July 2014</td>
<td>Corrected the note in SSL Network Extender Application Mode (on page 74)</td>
</tr>
<tr>
<td></td>
<td>Added note to Push Notifications (on page 106).</td>
</tr>
<tr>
<td>26 June 2014</td>
<td><strong>New for R77.20 Gateways:</strong></td>
</tr>
<tr>
<td></td>
<td>Configuring a TLS/SSL Version for an Application (on page 97)</td>
</tr>
<tr>
<td></td>
<td>Configuring SSO Name Format (on page 61)</td>
</tr>
<tr>
<td></td>
<td>SSO for Native Applications (on page 63)</td>
</tr>
<tr>
<td></td>
<td>Updated Push Notifications (on page 106)</td>
</tr>
<tr>
<td>01 June 2014</td>
<td>Added information to Capsule Workspace Mail Applications (on page 95)</td>
</tr>
<tr>
<td></td>
<td>Updated Kerberos Authentication Support (on page 67)</td>
</tr>
<tr>
<td>12 March 2014</td>
<td>Updated Push Notifications (on page 106)</td>
</tr>
<tr>
<td>05 March 2014</td>
<td>Updated Kerberos configuration (&quot;Kerberos Authentication Support&quot; on page 67)</td>
</tr>
<tr>
<td></td>
<td>Updated fwpush (on page 192)</td>
</tr>
<tr>
<td></td>
<td>Updated Anti-Virus and Anti-malware Blade (on page 172)</td>
</tr>
<tr>
<td></td>
<td>Updated Push Notifications (on page 106)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>06 February 2014</td>
<td>Updated MDM Cooperative Enforcement (on page 109) with link to sk98447 for iOS 7 configuration with Check Point Apps</td>
</tr>
<tr>
<td>23 January 2014</td>
<td>Updated MDM Cooperative Enforcement (on page 109) Corrected IPv6 support information in Remote Access Solution Comparison (on page 20)</td>
</tr>
<tr>
<td>15 January 2014</td>
<td>New for R77.10 gateways:</td>
</tr>
<tr>
<td></td>
<td>• Added VSX support (&quot;Deployments with VSX&quot; on page 28)</td>
</tr>
<tr>
<td></td>
<td>• Added IPV6 support (&quot;Mobile Access Applications&quot; on page 11)</td>
</tr>
<tr>
<td></td>
<td>• Push Notifications (on page 106)</td>
</tr>
<tr>
<td></td>
<td>• Multiple Realms (on page 131)</td>
</tr>
<tr>
<td></td>
<td>• WebSockets (on page 58)</td>
</tr>
<tr>
<td></td>
<td>• MDM Cooperative Enforcement (on page 109)</td>
</tr>
<tr>
<td></td>
<td>• Remote Wipe (on page 102)</td>
</tr>
<tr>
<td></td>
<td>• fwpush (on page 192)</td>
</tr>
<tr>
<td></td>
<td>Updated Remote Access Solution Comparison (on page 20)</td>
</tr>
<tr>
<td></td>
<td>Corrected menu options in Portal Protection Settings (on page 157) and User Experience Settings (on page 157)</td>
</tr>
<tr>
<td>01 August 2013</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 Mobile Access R77 Versions Administration Guide).
# Contents

## Important Information

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Mobile Access</td>
<td>3</td>
</tr>
<tr>
<td>Mobile Access Applications</td>
<td>11</td>
</tr>
<tr>
<td>Mobile Access Management</td>
<td>12</td>
</tr>
<tr>
<td>SSL Network Extender</td>
<td>12</td>
</tr>
<tr>
<td>SSL Network Extender Network Mode</td>
<td>12</td>
</tr>
<tr>
<td>SSL Network Extender Application Mode</td>
<td>13</td>
</tr>
</tbody>
</table>

## Commonly Used Concepts

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>13</td>
</tr>
<tr>
<td>Authorization</td>
<td>13</td>
</tr>
<tr>
<td>Endpoint Compliance Scanner</td>
<td>13</td>
</tr>
<tr>
<td>Secure Workspace</td>
<td>13</td>
</tr>
<tr>
<td>Protection Levels</td>
<td>14</td>
</tr>
<tr>
<td>Session</td>
<td>14</td>
</tr>
</tbody>
</table>

## Mobile Access Security Features

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Side Security Highlights</td>
<td>14</td>
</tr>
<tr>
<td>Client Side Security Highlights</td>
<td>14</td>
</tr>
</tbody>
</table>

## User Workflow for Mobile Access Portal

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing In</td>
<td>15</td>
</tr>
<tr>
<td>First time Installation of ActiveX and Java Components</td>
<td>15</td>
</tr>
<tr>
<td>Language Selection</td>
<td>16</td>
</tr>
<tr>
<td>Initial Setup</td>
<td>16</td>
</tr>
<tr>
<td>Accessing Applications</td>
<td>16</td>
</tr>
</tbody>
</table>

## Security Gateway Portals

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providing Secure Remote Access</td>
<td>18</td>
</tr>
<tr>
<td>Types of Solutions</td>
<td>18</td>
</tr>
</tbody>
</table>

## Check Point Remote Access Solutions

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-Based vs. Clientless</td>
<td>19</td>
</tr>
<tr>
<td>Secure Connectivity and Endpoint Security</td>
<td>19</td>
</tr>
</tbody>
</table>

## Remote Access Solution Comparison

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary of Remote Access Options</td>
<td>20</td>
</tr>
</tbody>
</table>

## Getting Started with Mobile Access

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Deployments</td>
<td>26</td>
</tr>
<tr>
<td>Simple Deployment</td>
<td>26</td>
</tr>
<tr>
<td>Deployment in the DMZ</td>
<td>27</td>
</tr>
<tr>
<td>Cluster Deployment</td>
<td>28</td>
</tr>
<tr>
<td>Deployments with VSX</td>
<td>28</td>
</tr>
<tr>
<td>SmartDashboard Toolbar</td>
<td>30</td>
</tr>
<tr>
<td>Basic SmartDashboard Configuration</td>
<td>30</td>
</tr>
</tbody>
</table>
Configuring Microsoft Active Directory for Mobile Access ........................................... 68
Manual Configuration for Kerberos ......................................................................... 69
Kerberos Constrained Delegation ......................................................................... 70
Configuring Kerberos Constrained Delegation .................................................. 70
Configuring a Delegate User on the AD Server ............................................... 71
Configuring Support on the Mobile Access Gateway ...................................... 71
Troubleshooting ................................................................................................. 71
Certificate Attribute Forwarding ......................................................................... 72
Configuring Certificate Attribute Forwarding .................................................. 72
Native Applications for Client-Based Access .................................................... 73
Accessing Native Applications ........................................................................... 73
SSL Network Extender ...................................................................................... 73
SSL Network Extender Network Mode ........................................................... 74
SSL Network Extender Application Mode ....................................................... 74
Configuring VPN Clients ................................................................................... 76
Office Mode ....................................................................................................... 76
Configuring Office Mode ................................................................................... 77
IP Pool Optional Parameters .............................................................................. 78
Configuring SSL Network Extender Advanced Options .................................... 78
Deployment Options ......................................................................................... 78
Encryption ......................................................................................................... 78
Launch SSL Network Extender Client ............................................................... 78
Endpoint Application Types ............................................................................... 79
Application Installed on Endpoint Machine .................................................... 79
Application Runs Via a Default Browser ........................................................ 79
Applications Downloaded-from-Gateway ....................................................... 79
Configuring Authorized Locations per User Group ......................................... 80
Ensuring the Link Appears in the End-User Browser ...................................... 81
Configuring a Simple Native Application ....................................................... 81
General Properties ........................................................................................... 81
Authorized Locations ......................................................................................... 81
Applications on the Endpoint Computer ......................................................... 81
Completing the Native Application Configuration ........................................ 82
Configuring an Advanced Native Application ............................................... 82
Configuring Connection Direction ................................................................. 82
Multiple Hosts and Services ............................................................................. 83
Configuring the Endpoint Application to Run Via a Default Browser ............. 83
Automatically Starting the Application ......................................................... 83
Making an Application Available in Application Mode .................................... 84
Automatically Running Commands or Scripts ................................................ 84
Protection Levels for Native Applications ...................................................... 85
Defining Protection Levels ............................................................................... 86
Adding Downloaded-from-Gateway Endpoint Applications ......................... 86
Downloaded-from-Gateway Application Requirements .................................... 86
Adding a New Application ............................................................................... 87
Example: Adding a New SSH Application ....................................................... 88
Example: Adding a New Microsoft Remote Desktop Profile............................ 89
Configuring Downloaded-from-Gateway Endpoint Applications .................... 91
Configuring the Telnet Client (Certified Application) ....................................... 92
Configuring the SSH Client (Certified Application) .......................................... 92
Configuring the TN3270 Client (Certified Application) .................................... 92
Configuring the TN5250 Client (Certified Application) .................................... 92
Configuring the Remote Desktop Client (Add-On Application) .................... 93
Configuring the PuTTY Client (Add-On Application) ...................................... 94
Configuring the Jabber Client (Add-On Application) ...................................... 94
Configuring the FTP Client (Add-On Application) .......................................... 94
Exchange Mail Applications for Smartphones and Tablets ............................ 95
Capsule Workspace Mail Applications ................................................................. 95
ActiveSync Applications .................................................................................. 96
Mobile Access for Smartphones and Tablets ................................................. 99
  Overview of Mobile Access for Smartphones and Tablets .......................... 99
  Certificate Authentication for Handheld Devices ...................................... 99
  Managing Client Certificates ..................................................................... 100
    Creating Client Certificates ................................................................. 100
    Creating Templates for Certificate Distribution ..................................... 101
  Remote Wipe .............................................................................................. 102
  Managing Capsule Workspace Settings ...................................................... 103
    Creating and Editing Mobile Profiles ...................................................... 104
    Passcode Profiles .................................................................................... 105
  Push Notifications ....................................................................................... 106
    Configuring Push Notifications ............................................................. 106
    Customizing Push Notifications ............................................................ 107
    Exchange Server and Gateway Communication ....................................... 108
    Monitoring Push Notification Usage ...................................................... 108
  ESOD Bypass for Mobile Apps .................................................................... 109
  MDM Cooperative Enforcement .................................................................. 109
    Configuring MDM on the Security Gateway ............................................ 110
    Testing MDM .......................................................................................... 114
    Advanced Testing .................................................................................... 114
  System Specific Configuration ..................................................................... 114
    iPhone and iPad Configuration ............................................................... 114
    Android Configurations ........................................................................... 115
  Instructions for End Users .......................................................................... 116
    iPhone/iPad End User Configuration ....................................................... 116
    Android End User Configuration ............................................................. 117
  Advanced Gateway Configuration for Handheld Devices ........................... 118
  User Authentication in Mobile Access ......................................................... 121
  User Authentication to the Mobile Access Portal ...................................... 121
    Configuring Authentication ...................................................................... 121
    Requiring Certificates for Mobile Devices ............................................. 122
    How the Gateway Searches for Users ...................................................... 122
  Two-Factor Authentication with DynamicID .............................................. 123
    How DynamicID Works .......................................................................... 123
    The SMS Service Provider ...................................................................... 123
    SMS Authentication Granularity ............................................................. 123
    Basic DynamicID Configuration for SMS or Email .................................. 124
    Advanced Two-Factor Authentication Configuration .............................. 126
    Configuring Resend Verification and Match Word ................................... 128
    Two-Factor Authentication per Gateway .................................................. 129
    Two-Factor Authentication per Application .............................................. 129
    Two-Factor Authentication for Certain Authentication Methods .......... 130
  Multiple Realms ......................................................................................... 131
    Workflow ................................................................................................ 131
    Creating New Realms ............................................................................. 131
    Configuring Authentication Schemes ....................................................... 131
    Defining Fetch Directories ...................................................................... 132
    Applying New Realms ............................................................................ 133
    Two-Factor Authentication for Certain Authentication Methods .............. 134
  Session Settings ......................................................................................... 135
    Session Timeouts .................................................................................... 135
    Roaming .................................................................................................. 135
    Tracking .................................................................................................. 135
    Securing Authentication Credentials ..................................................... 135
    Simultaneous Logins to the Portal ......................................................... 136
  Endpoint Security On Demand ..................................................................... 138
    Endpoint Compliance Enforcement ......................................................... 138
Chapter 1

Introduction to Mobile Access

Check Point Mobile Access blade is a simple and comprehensive remote access solution that delivers exceptional operational efficiency. It allows mobile and remote workers to connect easily and securely from any location, with any Internet device to critical resources while protecting networks and endpoint computers from threats. Combining the best of remote access technologies in a software blade provides flexible access for endpoint users and simple, streamlined deployment for IT.

This software blade option simply integrates into your existing Check Point gateway, enabling more secure and operationally efficient remote access for your endpoint users. The data transmitted by remote access is decrypted and then filtered and inspected in real time by Check Point’s award-winning gateway security services such as antivirus, intrusion prevention and web security. The Mobile Access blade also includes in-depth authentications, and the ability to check the security posture of the remote device. This further strengthens the security for remote access.

Mobile Access Applications

Mobile Access provides the remote user with access to the various corporate applications, including, Web applications, file shares, Citrix services, Web mail, and native applications.

- A Web application can be defined as a set of URLs that are used in the same context and that is accessed via a Web browser, for example inventory management, or HR management.
- A file share defines a collection of files, made available across the network by means of a protocol, such as SMB for Windows, that enables actions on files, such as opening, reading, writing and deleting files across the network.
- Mobile Access supports Citrix client connectivity to internal XenApp servers.
- Mobile Access supports Web mail services including:
  - Built-in Web mail: Web mail services give users access to corporate mail servers via the browser. Mobile Access provides a front end for any email server that supports the IMAP and SMTP protocols.
  - Other Web-based mail services, such as Outlook Web Access (OWA) and IBM Lotus Domino Web Access (iNotes). Mobile Access relays the session between the client and the OWA server.
- iPhone and iPad support
  - Access to Web applications
  - Access to email, calendar, and contacts
  - Two-factor authentication with client certificate and user name/password
Mobile Access supports IPv6 on the following:
- The Mobile Access portal
- Capsule Workspace

This feature is supported in R77.10 and higher. Notes:
- SSL Network Extender is not supported with IPv6
- IPv6 is supported on external interfaces only

SSL Network Extender support for MacOS as part of Capsule Workspace Access

Mobile Access supports any native application, via SSL Network Extender. A native application is any IP-based application that is hosted on servers within the organization. When a user is allowed to use a native application, Mobile Access launches SSL Network Extender and allows users to employ native clients to connect to native applications, while ensuring that all traffic is encrypted.

Remote users initiate a standard HTTPS request to the Mobile Access gateway, authenticating via user name/password, certificates, or some other method such as SecurID. Users are placed in groups and these groups are given access to a number of applications.

For information about Web applications, file shares, Citrix services, Web mail see Applications for Clientless Access.

For information about native applications, see Native Applications for Client-Based Access (on page 73).

Mobile Access Management

- Mobile Access enabled gateways are managed by the Security Management Server that manages all Check Point gateways.
- All Mobile Access related configuration can be performed from the Mobile Access tab of SmartDashboard.
- Mobile Access users are shown in SmartConsole, along with real-time counters, and history counters for monitoring purposes.

SSL Network Extender

The SSL Network Extender client makes it possible to access native applications via Mobile Access.

SSL Network Extender is downloaded automatically from the Mobile Access portal to the endpoint machines, so that client software does not have to be pre-installed and configured on users' PCs and laptops. SSL Network Extender tunnels application traffic using a secure, encrypted and authenticated SSL tunnel to the Mobile Access gateway.

SSL Network Extender Network Mode

The SSL Network Extender Network Mode client provides secure remote access for all application types (both Native-IP-based and Web-based) in the internal network via SSL tunneling. To install the Network Mode client, users must have administrator privileges on the client computer.

After installing the client, an authenticated user can access any authorized internal resource that is defined on Mobile Access as a native application. The user can access the resource by launching the client application, either directly from the desktop or from the Mobile Access portal.
SSL Network Extender Application Mode

The SSL Network Extender Application Mode client provides secure remote access for most application types (both Native (IP-based) and Web-based) in the internal network via SSL tunneling. Most TCP applications can be accessed in Application Mode. The user does not require administrator privileges on the endpoint machine.

After the client is installed the user can access any internal resource that is defined on Mobile Access as a native application. The application must be launched from the Mobile Access portal and not from the user's desktop.

Commonly Used Concepts

This section briefly describes commonly used concepts that you will encounter when dealing with Mobile Access.

Authentication

All remote users accessing the Mobile Access portal must be authenticated by one of the supported authentication methods. As well as being authenticated through the internal database, remote users may also be authenticated via LDAP, RADIUS, ACE (SecurID), or certificates. You can also configure two factor authentication with a DynamicID one time password.

Authorization

Authorization determines how remote users access internal applications on the corporate LAN. If the remote user is not authorized, access to the services provided by the Mobile Access gateway is not granted.

After being authenticated, the user can open an application:

- If the user belongs to a group with access granted to that application.
- If the user satisfies the security requirements of the application (such as authentication method and endpoint health compliance).

Endpoint Compliance Scanner

The Check Point Endpoint Security On Demand scanner enforces endpoint compliance by scanning the endpoint to see if it complies with a pre-defined endpoint compliance policy. For example, an endpoint compliance policy would make sure that the endpoint clients have updated Anti-Virus signatures and an active firewall. If the endpoint is compliant with the endpoint compliance policy, the user is allowed to access the portal.

When end users access the Mobile Access Portal for the first time, an ActiveX component scans the client computer. If the client computer successfully passes the scan, the user is granted access to the Mobile Access portal. The scan results are presented to the Mobile Access gateway and to the end user.

When Endpoint Security on Demand detects a lack of security, it either rejects the connection or allows the user to choose whether or not to proceed, according to the Endpoint Compliance policies. The system administrator defines policies that determine which types of threats to detect and what action to take upon their detection.

Secure Workspace

End-users can utilize Check Point's proprietary virtual desktop that enables data protection during user-sessions, and enables cache wiping, after the sessions have ended. Secure Workspace protects all session-specific data accumulated on the client side. It uses protected disk space and file encryption to secure files created during the access session. Afterwards, it cleans the protected session cache, eliminating any exposure of proprietary data that would have been inadvertently left on public PCs.
Protection Levels

Protection Levels balance between connectivity and security. The Protection Level represents a security criterion that must be satisfied by the remote user before access is given. For example, an application may have a Protection Level, which requires users to satisfy a specific authentication method. Out of the box, Mobile Access has three pre-defined Protection Levels — Permissive, Normal, and Restrictive. It is possible to edit Protection Level settings, and define new Protection Levels.

Session

After being authenticated, remote users are assigned a Mobile Access session. The session provides the context in which Mobile Access processes all subsequent requests until the user logs out, or the session ends due to a time-out.

Mobile Access Security Features

Greater access and connectivity demands a higher level of security. The Mobile Access security features may be grouped as server side security and client side security.

Server Side Security Highlights

Mobile Access enabled gateways are fully integrated with and benefit from the same security features as other Security Gateways. In addition, Mobile Access gateways have numerous security features to enable secure remote access. The following list outlines the security highlights and enhancements available on Mobile Access gateways:

1. **IPS:** Protects organizations from all known, and most unknown network attacks using intelligent security technology.
   - The Web Intelligence component of IPS enables protection against malicious code transferred in Web-related applications: worms, various attacks such as Cross Site Scripting, buffer overflows, SQL injections, Command injections, Directory traversal, and HTTP code inspection.

2. **IPS Service:** Downloads new defense mechanisms to the IPS console, and brings existing defense mechanisms up-to-date.

3. **Anti-Virus:** Many Anti-Virus settings enabled on the Security Gateway also apply to Mobile Access traffic, preventing viruses from reaching end users and the enterprise.

4. **Granular authorization policy:** Limits which users are granted access to which applications by enforcing authentication, encryption, and client security requirements.

5. **Web Application support over HTTPS:** All traffic to Web-based applications is encrypted using HTTPS. Access is allowed for a specific application set rather than full network-level access.

6. **Encryption:** SSL Network Extender, used by Mobile Access, encrypts traffic using the 3DES or the RC4 encryption algorithm.

Client Side Security Highlights

The following list outlines the security highlights and enhancements available on the client side:

1. **Endpoint Compliance for Mobile Access on the endpoint machine:** Prevents threats posed by endpoint clients that do not have updated protection, for example, updated anti-virus and firewall applications (see "Endpoint Compliance Enforcement" on page 138).

2. **Secure Workspace protects all session-specific data, accumulated on the client side.** End-users can utilize Check Point's proprietary virtual desktop that prevents data leakage, by encrypting all files and wiping it at the end of the user session. The administrator can configure Mobile Access (via Protection Levels) to force end users to use Secure Workspace when accessing the user portal or sensitive applications.

3. **Controls browser caching:** You can decide what Web content may be cached by browsers, when accessing Web applications. Disabling browser caching can help prevent unauthorized access to sensitive information, thus contributing to overall information security ("Web Application — Protection Level Page" on page 39).
4. **Captures cookies sent to the remote client by the internal Web server:** In most configurations, Mobile Access captures cookies and maintains them on the gateway. Mobile Access simulates user/Web server cookie transmission by appending the cookie information, stored on Mobile Access, to the request that Mobile Access makes to the internal Web server, in the name of the remote user.

5. **Supports strong authentication methods:** For example, using SecurID tokens, SSL client certificates, and two factor authentication utilizing DynamicID.

---

**User Workflow for Mobile Access Portal**

The user workflow includes these steps:

1. Sign in and select the portal language.
2. On first-time use, install ActiveX and Java Components.
3. Initial setup.
4. Access applications.

---

**Signing In**

In a browser, the user types in the URL assigned by the system administrator for the Mobile Access gateway.

*Note -* Some popup blockers can interfere with aspects of portal functionality. You should recommend to users that they configure popup blockers to allow pop-ups from Mobile Access.

If the Administrator has configured Secure Workspace to be optional, users can choose to select it on the sign in page.

Users enter their authentication credentials and click **Sign In.** Before Mobile Access gives access to the applications on the LAN, the credentials of remote users are first validated. Mobile Access authenticates the users either through its own internal database, LDAP, RADIUS or RSA ACE/Servers. Once the remote users have been authenticated, and associated with Mobile Access groups, access is given to corporate applications.

*Note -* If the Endpoint Compliance Scanner is enabled, the user may be required to pass a verification scan on his/her computer, before being granted access to the Mobile Access **Sign In** page, which ensures that his/her credentials are not compromised by 3rd party malicious software.

---

**First time Installation of ActiveX and Java Components**

Some Mobile Access components such as the endpoint Compliance Scanner, Secure Workspace and SSL Network Extender require either an ActiveX component (for Windows with Internet Explorer machines) or a Java component to be installed on the endpoint machine.

When using one of these components for the first time on an endpoint machine using Windows and Internet Explorer, Mobile Access tries to install it using ActiveX. However, Internet Explorer may prevent the ActiveX installation because the user does not have Power User privileges, or display a yellow bar at the top of the page asking the user to explicitly allow the installation. The user is then instructed to click the yellow bar, or if having problems doing so, to follow a dedicated link. This link is used to install the required component using Java.

After the first of these components is installed, any other components are installed in the same way. For example, if the Endpoint compliance Scanner was installed using Java on Internet Explorer, Secure Workspace and SSL Network Extender are also installed using Java.

*Note -* To install using ActiveX after a component was installed using Java, delete the browser cookies.
Language Selection
The user portal can be viewed in several languages. The default language is English. Supported languages include:

- Bulgarian
- Chinese — Simplified
- Chinese — Traditional
- English
- Finnish
- French
- German
- Italian
- Japanese
- Polish
- Romanian
- Russian
- Spanish

You can turn on automatic detection of the local language or let users select a language ("Localization Features" on page 174).

Initial Setup
The user may be required to configure certain settings, such as application credentials. In addition, the user can define additional favorites for commonly used applications.

Accessing Applications
After the remote users have logged onto the Mobile Access gateway, they are presented with a portal. The user portal enables access to the internal applications that the administrator has configured as available from within the organization, and that the user is authorized to use.

Security Gateway Portals
The Security Gateway runs a number of web-based portals over HTTPS:

- Mobile web access portal
- SecurePlatform WebUI
- Gaia WebUI
- Identity Awareness (Captive Portal)
- DLP portal
- SSL Network Extender portal
- UserCheck portal
- Endpoint Security portals (CCC)

All of these portals can resolve HTTPS hosts to IPv4 and IPv6 addresses over port 443.
These portals (and HTTPS inspection) support the latest versions of the TLS protocol. In addition to SSLv3 and TLS 1.0 (RFC 2246), the Security Gateway supports:

- TLS 1.1 (RFC 4346)
- TLS 1.2 (RFC 5246)

Support for TLS 1.1 and TLS 1.2 is enabled by default but can be disabled in SmartDashboard (for web-based portals) or GuiDBedit (for HTTPS Inspection).

To configure TLS protocol support for portals:

1. In SmartDashboard, open Global Properties > SmartDashboard Customization.
2. In the Advanced Configuration section, click Configure.
   The Advanced Configuration window opens.
3. On the Portal Properties page, set minimum and maximum versions for SSL and TLS protocols.

To Configure TLS Protocol Support for HTTPS inspection:

1. In GuiDBedit, on the Tables tab, select Other > ssl_inspection.
2. In the Objects column, select general_confs_obj.
3. In the Fields column, select the minimum and maximum TLS version values in these fields:
   - **ssl_max_ver** (default = TLS 1.2)
   - **ssl_min_ver** (default = SSLv3)
Chapter 2

Check Point Remote Access Solutions

In This Section:

Providing Secure Remote Access ................................................................. 18
Types of Solutions ....................................................................................... 18
Remote Access Solution Comparison ......................................................... 20
Summary of Remote Access Options ......................................................... 21

Providing Secure Remote Access

In today's business environment, it is clear that workers require remote access to sensitive information from a variety of locations and a variety of devices. Organizations must also make sure that their corporate network remains safe and that remote access does not become a weak point in their IT security.

This chapter:
- Gives you information about Check Point's secure remote access options.
- Helps you decide which remote access client or clients best match your organization's requirements.
- Shows you where to get more information.

Types of Solutions

All of Check Point's Remote Access solutions provide:
- Enterprise-grade, secure connectivity to corporate resources.
- Strong user authentication.
- Granular access control.

Factors to consider when choosing remote access solutions for your organization:
- **Client-Based vs. Clientless** - Does the solution require a Check Point client to be installed on the endpoint computer or is it clientless, for which only a web browser is required. You might need multiple solutions within your organization to meet different needs.
- **Secure Connectivity and Endpoint Security** - Which capabilities does the solution include?
  - **Secure Connectivity** - Traffic is encrypted between the client and VPN gateway. After users authenticate, they can access the corporate resources that are permitted to them in the access policy. All Check Point solutions supply this.
  - **Endpoint Security** - Endpoint computers are protected at all times, even when there is no connectivity to the corporate network. Some Check Point solutions supply this.
**Client-Based vs. Clientless**

Check Point remote access solutions use IPsec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:

- **Client-based** - Client application installed on endpoint computers and devices. Clients are usually installed on a managed device, such as a company-owned computer. The client supplies access to most types of corporate resources according to the access privileges of the user.

- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.

- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

**Secure Connectivity and Endpoint Security**

You can combine secure connectivity with additional features to protect the network or endpoint computers.

- **Secure Connectivity** - Traffic is encrypted between the client and VPN gateway and strong user authentication is supported. All Check Point solutions supply this. These solutions require licenses based on the number of users connected at the same time.

- **Security Verification for Endpoint computers** - Makes sure that devices connecting to the gateway meet security requirements. Endpoint machines that are not compliant with the security policy have limited or no connectivity to corporate resources. Some Check Point solutions supply this.

- **Endpoint Security:**
  - **Desktop Firewall** - Protects endpoint computers at all times with a centrally managed security policy. This is important because remote clients are not in the protected network and traffic to clients is only inspected if you have a Desktop Firewall. Some Check Point solutions supply this.
  
  - **More Endpoint Security Capabilities** - Check Point solutions can include more Endpoint Security capabilities, such as anti-malware, disk encryption and more. These solutions require licenses based on the number of clients installed.
## Remote Access Solution Comparison

Details of the newest version for each client and a link for more information are in sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

### SSL VPN Portal and Clients

<table>
<thead>
<tr>
<th>Name</th>
<th>Supported Operating Systems</th>
<th>Client or Clientless</th>
<th>Encryption Protocol</th>
<th>Security Verification for Endpoint Devices</th>
<th>Desktop Firewall on Endpoint Devices</th>
<th>IPv6 Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Access Web Portal</td>
<td>Windows, Linux, Mac OS, iOS, Android</td>
<td>Clientless</td>
<td>SSL</td>
<td>☑</td>
<td>☑ R77.10 and higher</td>
<td></td>
</tr>
<tr>
<td>SSL Network Extender for Mobile Access Blade</td>
<td>Windows, Linux, Mac OS</td>
<td>On-demand Client through Mobile Access Portal)</td>
<td>SSL</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Capsule Workspace for iOS</td>
<td>iOS</td>
<td>Client</td>
<td>SSL</td>
<td>☑ Jailbreak &amp; Root Detection MDM Cooperative Enforcement (sk98201)</td>
<td>☑ R77.10 and higher</td>
<td></td>
</tr>
<tr>
<td>(previously Mobile Enterprise)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capsule Workspace for Android</td>
<td>Android</td>
<td>Client</td>
<td>SSL</td>
<td>☑ Jailbreak &amp; Root Detection MDM Cooperative Enforcement (sk98201)</td>
<td>☑ R77.10 and higher</td>
<td></td>
</tr>
<tr>
<td>(previously Mobile Enterprise)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Layer-3 VPN Tunnel Clients

<table>
<thead>
<tr>
<th>Name</th>
<th>Supported Operating Systems</th>
<th>Client or Clientless</th>
<th>Encryption Protocol</th>
<th>Security Verification for Endpoint Devices</th>
<th>Desktop Firewall on Endpoint Devices</th>
<th>IPv6 Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capsule Connect for iOS (previously Mobile VPN)</td>
<td>iOS</td>
<td>Client</td>
<td>IPsec / SSL</td>
<td>MDM Cooperative Enforcement (sk98201)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capsule VPN for Android (previously Mobile VPN)</td>
<td>Android</td>
<td>Client</td>
<td>IPsec/SSL</td>
<td>MDM Cooperative Enforcement (sk98201)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check Point VPN Plugin for Windows 8.1</td>
<td>Windows 8.1</td>
<td>Pre-installed client</td>
<td>SSL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check Point Mobile for Windows</td>
<td>Windows</td>
<td>Client</td>
<td>IPsec</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Layer-3 VPN Tunnel Clients Integrated with Endpoint Security

<table>
<thead>
<tr>
<th>Name</th>
<th>Supported Operating Systems</th>
<th>Client or Clientless</th>
<th>Encryption Protocol</th>
<th>Security Verification for Endpoint Devices</th>
<th>Desktop Firewall on Endpoint Devices</th>
<th>IPv6 Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security VPN for Windows</td>
<td>Windows</td>
<td>Client</td>
<td>IPsec</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Security VPN for Mac</td>
<td>Mac OS</td>
<td>Client</td>
<td>IPsec</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Security Suite Remote Access VPN Blade</td>
<td>Windows, Mac OS</td>
<td>Client</td>
<td>IPsec</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Additional Remote Access Solutions

<table>
<thead>
<tr>
<th>Name</th>
<th>Supported Operating Systems</th>
<th>Client or Clientless</th>
<th>Encryption Protocol</th>
<th>Security Verification for Endpoint Devices</th>
<th>Desktop Firewall on Endpoint Devices</th>
<th>IPv6 Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecuRemote</td>
<td>Windows</td>
<td>Client</td>
<td>IPsec</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check Point GO VPN</td>
<td>Windows</td>
<td>Clientless - Requires a Check Point GO device</td>
<td>SSL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Summary of Remote Access Options

Below is a summary of each Remote Access option that Check Point offers. All supply secure remote access to corporate resources, but each has different features and meets different organizational requirements.
Details of the newest version for each client and a link for more information are in sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

**Mobile Access Web Portal**

The Mobile Access Portal is a clientless SSL VPN solution. It is recommended for users who require access to corporate resources from home, an internet kiosk, or another unmanaged computer. The Mobile Access Portal can also be used with managed devices.

It provides:

- Secure Connectivity
- Security Verification

The Mobile Access Portal supplies access to web-based corporate resources. You can use the on-demand client, SSL Network Extender, through the Portal to access all types of corporate resources.

**Required Licenses**: Mobile Access Software Blade on the gateway.

**Supported Platforms**: Windows, Mac OS X, Linux, iOS, Android

**Where to Get the Client**: Included with the Security Gateway. See sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

**SSL Network Extender**

SSL Network Extender is a thin SSL VPN on-demand client installed automatically on the user’s machine through a web browser. It supplies access to all types of corporate resources.

SSL Network Extender has two modes:

- **Network Mode** - Users can access all application types (Native-IP-based and Web-based) in the internal network. To install the Network Mode client, users must have administrator privileges on the client computer.
  
  **Supported Platforms**: Windows, Mac OS X, Linux

- **Application Mode** - Users can access most application types (Native-IP-based and Web-based) in the internal network, including most TCP applications. The user does not require administrator privileges on the endpoint machine.
  
  **Supported Platforms**: Windows

**Required Licenses**:

Mobile Access Software Blade on the gateway

**Where to Get the Client**: Included with the Security Gateway. See sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

**Capsule Workspace for iOS**

Capsule Workspace for iOS is an SSL VPN client. It supplies secure connectivity and access to web-based corporate resources and Microsoft Exchange services. It also gives secure access to Capsule Docs protected documents. It was previously called Mobile Enterprise.

Capsule Workspace is ideal for mobile workers who have privately-owned smart phones or tablets. It protects only the business data inside the App and does not require device-level security measures, such as device-lock or device-wipe.

**Required Licenses**: Mobile Access Software Blade on the gateway

**Supported Platforms**: iOS

**Where to Get the Client**: Apple App Store
**Capsule Workspace for Android**

Capsule Workspace for Android is an SSL VPN client. It supplies secure connectivity and access to web-based corporate resources and Microsoft Exchange services. It also gives secure access to Capsule Docs protected documents. It was previously called Mobile Enterprise.

Capsule Workspace for Android is ideal for mobile workers who have privately-owned smart phones or tablets. It protects only the business data inside the App and does not require device-level security measures, such as device-lock or device-wipe.

**Required Licenses:** Mobile Access Software Blade on the gateway  
**Supported Platforms:** Android  
**Where to Get the Client:** Google Play Store

**Capsule Connect for iOS**

Capsule Connect is a full L3 tunnel app that gives users network access to all mobile applications. It supplies secure connectivity and access to all types of corporate resources. It was previously called Mobile VPN.

**Required Licenses:** Mobile Access Software Blade on the gateway  
**Supported Platforms:** iOS 6.0 +  
**Where to Get the Client:** Apple App Store

**Capsule VPN for Android**

Capsule VPN for Android devices is an L3 VPN client. It supplies secure connectivity and access to corporate resources using L3 IPSec/SSL VPN Tunnel. It was previously called Mobile VPN.

**Required Licenses:** Mobile Access Software Blade on the gateway  
**Supported Platforms:** Android 4+ (ICS+)

**Where to Get the Client:** Google Play Store

**Check Point VPN Plugin for Windows 8.1**

Check Point VPN Plugin for Windows 8.1 is an L3 VPN client. It supplies secure connectivity and access to corporate resources using L3 SSL VPN Tunnel.

**Required Licenses:** Mobile Access Software Blade on the gateway  
**Supported Platforms:** Windows 8.1  
**Where to Get the Client:** Pre-installed with Windows.

**Check Point Mobile for Windows**

Check Point Mobile for Windows is an IPsec VPN client. It is best for medium to large enterprises that do not require an Endpoint Security policy.

It provides:

- Secure Connectivity  
- Security Verification

**Required Licenses:** IPsec VPN and Mobile Access Software Blades on the gateway  
**Supported Platforms:** Windows  
**Where to Get the Client:** Check Point Support Center - sk67820  
**Endpoint Security VPN**

Endpoint Security VPN is an IPsec VPN client that replaces SecureClient. It is best for medium to large enterprises.

It provides:

- Secure Connectivity
- Security Verification
- Endpoint Security that includes an integrated Desktop Firewall, centrally managed from the Security Management Server.

**Required Licenses:** The IPsec VPN Software Blade on the gateway, an Endpoint Container license, and an Endpoint VPN Software Blade license on the Security Management Server.

**Supported Platforms:** Windows

**Where to Get the Client:** Check Point Support Center - sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

*Note* - Endpoint Security VPN on Mac OS X includes a Desktop Firewall but not Security Verification.

**Endpoint Security VPN for Mac**

Endpoint Security VPN combines Remote Access VPN with Endpoint Security in a client that is installed on endpoint computers. It is recommended for managed endpoints that require a simple and transparent remote access experience together with desktop firewall rules. It includes:

- Enterprise Grade Remote Access Client that replaces SecureClient for Mac.
- Integrated Desktop Firewall, centrally managed from the Security Management Server.

**Required Licenses:** The IPsec VPN Software Blade on the gateway, an Endpoint Container license, and an Endpoint VPN Software Blade license on the Security Management Server.

**Supported Platforms for Users:** Mac OS X

**Where to Get the Client:** Check Point Support Center - sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

**Endpoint Security Suite**

The Endpoint Security Suite simplifies endpoint security management by unifying all endpoint security capabilities in a single console. Optional Endpoint Security Software Blades include: Firewall, Compliance Full Disk Encryption, Media Encryption & Port Protection, and Anti- Malware & Program Control. As part of this solution, the Remote Access VPN Software Blade provides full, secure IPsec VPN connectivity.

The Endpoint Security suite is best for medium to large enterprises that want to manage the endpoint security of all of their endpoint computers in one unified console.

**Required Licenses:** Endpoint Security Container and Management licenses and an Endpoint VPN Software Blade on the Security Management Server.

**Supported Platforms:** Windows, Mac OS X

**Where to Get the Client:** Check Point Support Center - sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).
**SecuRemote**

SecuRemote is a secure, but limited-function IPsec VPN client. It provides secure connectivity.

**Required Licenses:** IPsec VPN Software Blade on the gateway. It is a free client and does not require additional licenses.

**Supported Platforms:** Windows

**Where to Get the Client:** Check Point Support Center - sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

**Check Point GO**

Check Point GO is a portable workspace with virtualized Windows applications, on a secure and encrypted USB Flash Drive. Users insert the USB device into a host PC and securely access their workspace and corporate resources through SSL VPN technology.

Check Point GO is ideal for mobile workers, contractors, and disaster recovery. The virtual workspace is segregated from the host PC and controls the applications and data that can run in Check Point GO.

It provides:

- Secure Connectivity
- Security Verification

**Required Licenses:** IPsec VPN Software Blade on the gateway and Check Point GO devices.

**Supported Platforms:** Windows

**Where to Get the Client:** Check Point Support Center - sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).
Chapter 3

Getting Started with Mobile Access

In This Section:

- Recommended Deployments ............................................................. 26
- SmartDashboard Toolbar ................................................................. 30
- Basic SmartDashboard Configuration .............................................. 30
- Sample Mobile Access Workflow ................................................... 31
- Mobile Access Wizard ..................................................................... 31
- Setting up the Mobile Access Portal ............................................... 33
- Configuring Mobile Access Policy .................................................. 33
- Preparing for Capsule Workspace .................................................. 34
- Preparing for Capsule Connect ....................................................... 34
- Preparing for Desktop Clients ......................................................... 35

Recommended Deployments

Mobile Access can be deployed in a variety of ways depending on an organization's system architecture and preferences.

**Simple Deployment**

In the simplest Mobile Access deployment, one Mobile Access enabled Security Gateway inspects all traffic, including all Mobile Access traffic. IPS and Anti-Virus can be active on all traffic as well. The Security Gateway can be on the network perimeter.
This is the recommended deployment. It is also the least expensive and easiest to configure as it only requires one gateway machine for easy and secure remote access.

Deployment in the DMZ

When a Mobile Access enabled Security Gateway is placed in the DMZ, traffic initiated both from the Internet and from the LAN to Mobile Access is subject to firewall restrictions. By deploying Mobile Access in the DMZ, the need to enable direct access from the Internet to the LAN is avoided. Remote users initiate an SSL connection to the Mobile Access Gateway. The firewall must be configured to allow traffic from the user to the Mobile Access server, where SSL termination, IPS and Anti-Virus inspection, authentication, and authorization take place. Requests are then forwarded to the internal servers via the firewall.
**Cluster Deployment**

If you have large numbers of concurrent remote access users and continuous, uninterrupted remote access is crucial to your organization, you may choose to have Mobile Access active on a cluster. A cluster can be deployed in any of the deployments described above.

![Cluster Deployment Diagram](image)

Each cluster member has three interfaces: one data interface leading to the organization, a second interface leading to the internet, and a third for synchronization. Each interface is on a different subnet.

In a simple deployment with the Mobile Access cluster in the DMZ, two interfaces suffice; a data interface leading to the organization and the internet, and a second interface for synchronization.

**Deployments with VSX**

You can enable the Mobile Access Software Blade on VSX Virtual Systems. This feature is supported in R77.10 and higher.

You can use a VSX deployment to support different Mobile Access scenarios. Each Virtual System can have a Mobile Access portal with different applications, access policies, authentication requirements, and mobile clients.

For example, in the picture below, a VSX Gateway has four Virtual Systems with Mobile Access enabled. Each Virtual System has Mobile Access configured with different settings to meet the company’s needs for different users.
### Item | Description | Example Mobile Access Portal URL
---|---|---
1 | Virtual System 1 with Mobile Access enabled | https://dev.company.com/sslvpn
2 | Virtual System 2 with Mobile Access enabled | https://sales.company.com/sslvpn
3 | Virtual System 3 with Mobile Access enabled | https://finance.company.com/sslvpn
4 | Virtual System 4 with Mobile Access enabled | https://guest.company.com/sslvpn
5 | Virtual switch | |
6 | VSX Gateway | |
7 | Router | |
8 | Internet | |
9 | Remote users | |

This table shows an example of different settings that you can have on each Virtual System.

<table>
<thead>
<tr>
<th>Virtual System</th>
<th>Users</th>
<th>Clients Allowed</th>
<th>Authentication Schemes</th>
<th>Endpoint Health Checks</th>
<th>Applications Configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual System 1</td>
<td>Development team</td>
<td>Mobile Access Portal, SSL Network Extender, Capsule Workspace</td>
<td>Certificate + AD Password</td>
<td>Mobile Access Portal ESOD check for company Endpoint Security requirements Jail broken or rooted devices not allowed</td>
<td>Development applications</td>
</tr>
</tbody>
</table>
### SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="list_icon.png" alt="List" /></td>
<td>Open the SmartDashboard menu. When instructed to select menu options, click this button to show the menu. For example, if you are instructed to select Manage &gt; Users and Administrators, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td><img src="save_icon.png" alt="Save" /></td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td><img src="folder_icon.png" alt="Folder" /></td>
<td>Open a policy package, which is a collection of Policies saved together with the same name.</td>
</tr>
<tr>
<td><img src="refresh_icon.png" alt="Refresh" /></td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td><img src="database_icon.png" alt="Database" /></td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td><img src="change_icon.png" alt="Change" /></td>
<td>Change global properties.</td>
</tr>
<tr>
<td><img src="verify_icon.png" alt="Verify" /></td>
<td>Verify Rule Base consistency.</td>
</tr>
<tr>
<td><img src="install_icon.png" alt="Install" /></td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
<tr>
<td><img src="smartconsole_icon.png" alt="SmartConsole" /></td>
<td>Open SmartConsole.</td>
</tr>
</tbody>
</table>

### Basic SmartDashboard Configuration

The steps required in SmartDashboard before working with Mobile Access are:


   **Note** - The Mobile Access blade can only be enabled on Security Gateways running on the SecurePlatform and Gaia operating systems.
2. When you enable the Mobile Access blade:
   - You are automatically given a 30 day trial license for 10 users.
   - The Mobile Access Wizard opens. Follow the instructions to configure remote access to your network.

3. Configure your firewall access rules to permit Mobile Access traffic. The actual rules needed depend on your configuration. Implied rules are automatically added to the Rule Base to allow:
   - HTTPS (TCP/443) traffic.
   - HTTP (TCP/80). Requests are redirected to HTTP (TCP/443).
   - The DNS servers and WINS servers configured on the gateway.

   The Security Gateway might also need access to: LDAP, RADIUS, or ACE servers for authentication, and an NTP server for clock synchronization.

4. Configure the authentication scheme that the Mobile Access gateway will accept from remote users. Do this in Gateway Properties > Mobile Access > Authentication.

Sample Mobile Access Workflow

This is a high-level workflow to configure remote access to the internal applications and resources.

1. Use SmartDashboard to enable the Mobile Access Software Blade on the Security Gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
   - Select mobile device access clients
   - Define the Mobile Access portal
   - Define the web applications, for example Outlook Web App
   - Connect to the AD server for user information
3. For VPN clients, add Firewall rules to allow the mobile device connections.
4. Optional: Distribute client certificates to authenticate the mobile users.
   For R76 and higher, use the Certificate Creation and Distribution Wizard.
5. Users download the Check Point Mobile app.
6. Users open the Check Point Mobile app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.

Mobile Access Wizard

The Mobile Access Wizard runs when you enable the Mobile Access blade on a gateway. It lets you quickly allow selected remote users access to internal web or mail applications, through a web browser, mobile device, or remote access client.

See Check Point Remote Access Solutions (on page 18) to understand more about the remote access clients mentioned in the wizard. Many of the settings in the wizard are also in Gateway Properties > Mobile Access.
Going through the wizard:

1. **Mobile Access Methods** - Select from where users can access the Mobile Access applications:
   - **Web** - Through a browser on any computer. SSL Network Extender can be downloaded by users when necessary to access native applications.
   - **Mobile Devices** - Through an iOS or Android Mobile device. Devices must have a Check Point app installed.
     - **Capsule Workspace** - Use Check Point Capsule Workspace - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
     - **Capsule Connect/VPN** - A full L3 tunnel app that gives users network access to all mobile applications.
   - **Desktops/Laptops** - Through a remote access client installed on a desktop computer. Select the clients to allow:
     - **Endpoint Security VPN** - Endpoint Security VPN for Windows or Mac. Includes desktop firewall and security compliance verification.
     - **Mobile** - Check Point Mobile for Windows. Includes security compliance verification.
     - **SecuRemote** - SecuRemote for Windows.

2. **Web Portal** - Enter the primary URL for the Mobile Access portal. The default is the https://<IP address of the gateway>/sslvpn. You can use the same IP address for all portals on the gateway with a variation in the path. You can import a p12 certificate for the portal to use for SSL negotiation. All portals on the same IP address use the same certificate.

3. **Applications** - Select the applications that will be available to web or mobile device users:
   - **Web Applications** - Select the web applications to show on the Mobile Access portal.
     - **Demo web application (world clock)** - Select while testing Mobile Access, to have a web application show as it will when you are in production.
     - **Custom web application** - Enter the URL of the web application that you want users to be able to open when they connect with Mobile Access. For example, you can set the home page of your intranet site.
   - **Mail/Calendar/Contacts** - Enter the Exchange server that mobile devices work with and select which applications mobile device users can access.
     - **Capsule Workspace Mail**
     - **ActiveSync Applications**
     - **Outlook Web App**

4. **Active Directory Integration** - Select the AD domain, enter your credentials and test connectivity. If you do not use AD, select **I don't want to use active directory now**.

5. **Users** - Select users and groups from Active Directory or internal users. You can also create a test user that will get access to the configured applications.

6. **What's Next?** - This window helps you understand steps that are required to complete the automatic configuration done by the Mobile Access wizard. Depending on the selections you made, you might see these steps:
   - **Edit the Firewall policy and add a rule for Remote Access Community** - To work with Desktop Remote Access Clients or Capsule Connect clients, the Mobile Access Wizard automatically includes this gateway in the Remote Access VPN community. Remote Access Clients get access rules from the Firewall Rule Base. See Preparing for Desktop Clients (on page 35).
   - **Install policy on this security gateway** - When you install policy, the changes made by the Mobile Access Wizard become active.
   - **Log in to the Web portal (usually https://<ip address>/sslvpn)** - This is the web portal that you configured. Log in to see and use it. See Setting up the Mobile Access Portal.
   - **Install Check Point Capsule Workspace App and Desktop VPN client** - Install an App or VPN client to start using it. See Preparing for Mobile Devices ("Preparing for Capsule Workspace" on page 34) and Preparing for Desktop Clients (on page 35).
   - **Easily deploy client certificates to your users with the new client certificates tool** - If you use authentication with client certificates, see Managing Client Certificates (on page 100).
Setting up the Mobile Access Portal

Each Mobile Access-enabled Security Gateway leads to its own Mobile Access user portal. Remote users log in to the portal using an authentication scheme configured for that Security Gateway.

Remote users access the portal from a Web browser with https://<Gateway_IP>/sslvpn, where <Gateway_IP> is one of these:
- FQDN that resolves to the IP address of the Security Gateway
- IP address of the Security Gateway

Remote users that use HTTP are automatically redirected to the portal using HTTPS.

Note - If Hostname Translation is the method for link translation, FQDN is required.

Set up the URL for the first time in the Mobile Access First Time Wizard.

You can change the URL of the portal and the look and feel:
- To change the IP address used for the user portal: From the properties of the Gateway object, select Mobile Access > Portal Settings.
- To configure the look and feel of the portal in the Portal Customization page: Go to Mobile Access tab > Portal Settings > Portal Customization.

Configuring Mobile Access Policy

The Mobile Access policy applies to the Mobile Access portal and Capsule Workspace. It does not apply to Desktop clients or Capsule Connect.

Users can access applications remotely as defined by the policy rules. Configure Mobile Access policy in the Policy page of the Mobile Access tab. Create rules that include:
- Users and User Groups.
- Applications that the users can access.
- The gateways that the rule applies to.

Users and applications have multiple properties that you can choose to configure. However, you can add objects to a rule quickly and configure more detailed properties at a different time.

Settings related to what users can access from mobile devices are also defined in the Mobile Settings Profile: Mobile Access tab > Mobile Settings.

To create rules in the Mobile Access Rule Base:

1. In the Policy page of the Mobile Access tab, click one of the add rule buttons.
2. In the Users column, click the + sign, or right-click and select Add Users.
3. In the User Viewer that opens, you can:
   - Select a user directory, either internal or an Active Directory domain.
   - Search for and select individual users, groups, or branches.
4. In the Applications column, click the + sign, or right-click and select Add Applications.
5. In the Application Viewer that opens, you can:
   - Select an application from the list.
   - Click New to define a new application.
6. If you create a New application:
   a) Select the type of application.
   b) In the window that opens enter a Display Name that end-users will see, for example, Corporate Intranet.
   c) Enter the URL or path to access the application according to the example shown.
7. In the **Install On** column, click the + sign, or right-click and select **Add Objects** and select the gateways that the rule applies to.
8. Install the Policy (**Policy** > **Install**).

### Preparing for Capsule Workspace

**To enable devices to connect to the gateway with Capsule Workspace:**

1. Enable and configure Mobile Access on the gateway.
2. In the Mobile Access wizard or in **Gateway Properties > Mobile Access**, select **Mobile Devices** and **Capsule Workspace**.
3. In **Gateway Properties > Mobile Access > Authentication**, select how users authenticate to the mobile device.
   - If you use Certificates, in the **Mobile Access** tab, select **Client Certificates** to create and distribute certificates for authentication between the devices and the gateway ("Managing Client Certificates" on page 100).
5. Make sure you have rules in the Firewall Rule Base that allow traffic from mobile devices. For example, access to Exchange and application servers from the gateway.
6. Download a Capsule Workspace App from the App Store or Google Play to mobile devices.
7. Give users instructions to connect including the:
   - Site Name
   - Registration key (if you use certificate authentication)
   - If you use certificate authentication, we recommend that you include this information in the client certificate distribution email.

### Preparing for Capsule Connect

**To enable devices to connect to the gateway with Capsule Connect:**

1. Enable and configure Mobile Access on the gateway.
2. In the Mobile Access wizard or in **Gateway Properties > Mobile Access**, select **Mobile Devices** and **Secure VPN Client**.
3. In **Gateway Properties > VPN Clients > Authentication**, select how users authenticate to the mobile device.
   - If you use Certificates, in the **Mobile Access** tab, select **Client Certificates** to create and distribute certificates for authentication between the devices and the gateway ("Managing Client Certificates" on page 100).
4. Make sure you have rules in the Firewall Rule Base that allow traffic from mobile devices. For example:
   - Remote Access VPN Community access.
   - Access to Exchange and application servers from the gateway.
5. Download a Check Point App from the AppStore or Google Play Market to mobile devices.
6. Give users instructions to connect including the:
   - Site Name
   - Registration key (if you use certificate authentication)
   - If you use certificate authentication, we recommend that you include this information in the client certificate distribution email.
Preparing for Desktop Clients

- See Check Point Remote Access Solutions (on page 18) to understand which desktop clients are available, which Software Blades and licenses they require, and where to get the client and its documentation.

- Read the documentation for your client and make sure the required configuration is done. Most required gateway settings are configured automatically when you select Desktop Clients in the Mobile Access Wizard or in Gateway Properties > VPN Clients.

- Configure an authentication method in Gateway Properties > VPN Clients > Authentication. Make sure users have the required information to connect.

- In SmartDashboard a Remote Access Community object represents the users and gateways that can connect to each other through IPsec VPN tunnels. This object is in the Firewall Objects Tree > VPN Communities.

If you use a desktop VPN client, use the Remote Access Community object in the Firewall Rule Base to remote access traffic. Add it in the VPN column. For example:

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access</td>
<td>Capsule</td>
<td>Connect Users</td>
<td>Any</td>
<td>Remote Access</td>
<td>HTTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
Chapter 4

Applications for Clientless Access

In This Section:

Protection Levels ................................................................. 36
Web Applications ................................................................. 37
File Shares ........................................................................ 49
Citrix Services ..................................................................... 51
Web Mail Services ................................................................. 54
Native Applications ............................................................... 56
DNS Names ........................................................................... 56
WebSockets ........................................................................... 58

Giving remote users access to the internal network exposes the network to external threats. A balance needs to be struck between connectivity and security. In all cases, strict authentication and authorization is needed to ensure that only the right people gain access to the corporate network. Defining an application requires deciding which internal LAN applications to expose to what kind of remote user.

Mobile Access provides the remote user with access to the various corporate applications, including, Web applications, file shares, Citrix services, Web mail, and native applications.

Protection Levels

Protection Levels are predefined sets of security settings that offer a balance between connectivity and security. Protection Levels allow Mobile Access administrators to define application protections for groups of applications with similar requirements.

Mobile Access comes with three default Protection Levels — Normal, Restrictive, and Permissive. You can create additional Protection Levels and change the protections for existing Protection Levels.

Using Protection Levels

Protection Levels can be used in the definition of Mobile Access Web applications, file shares, Citrix applications, or Web mail service. On Mobile Access gateways of version R71 and higher, protection levels can also be set for each native application. Every application of one of these types can have a Protection Level associated with it. A single Protection Level can be assigned for all native applications.

When defining an application, in the Protection Level page of the application object, you can choose:

- **Security Requirements for Accessing this Application:**
  - **This application relies on the security requirements of the gateway**
    Rely on the gateway security requirement. Users who have been authorized to the portal, are authorized to this application. This is the default option.
  - **This application has additional security requirements specific to the following protection level**
    Associate the Protection Level with the application. Users are required to be compliant with the security requirement for this application in addition to the requirements of the portal.
Defining Protection Levels

To access the Protection Level page from the Mobile Access tab:

1. From the Mobile Access tab in SmartDashboard, select the Additional Settings > Protection Levels page from the navigation tree.
2. Click New to create a new Protection Level or double-click an existing Protection Level to modify it. The Protection Levels window opens, displaying the General Properties page.

To access the Protection Level page from a Mobile Access application:

1. From the Properties window of a Mobile Access application, select Additional Setting > Protection Level.
2. To create a new Protection Level, select Manage > New.
3. To edit the settings of a Protection Level, select the Protection Level from the drop down list and then select Manage > Details. The Protection Levels window opens, displaying the General Properties page.

To define a Protection Level:

1. In the General Properties page, enter a unique name for the Protection Level (for a new Protection Level only), select a display color and optionally add a comment in the appropriate fields.
2. Click on Authentication in the navigation tree and select one or more authentication methods from the available choices. Users accessing an application with this Protection Level must use one of the selected authentication schemes.
3. If required, select User must successfully authenticate via SMS.
4. Click Endpoint Security in the navigation tree and select one or both of the following options:
   - Applications using this Protection Level can only be accessed if the endpoint machine complies with the following Endpoint compliance policy. Also, select a policy. This option allows access to the associated application only if the scanned client computer complies with the selected policy.
   - Applications using this Protection Level can only be accesses from within Secure Workspace. This option requires Secure Workspace to be running on the client computer.
5. Click OK to close the Protection Level window
6. Install the Security Policy.

Web Applications

A Web application can be defined as a set of URLs that are used in the same context and are accessed via a Web browser, for example, inventory management or human resource management.

Mobile Access supports browsing to websites that use HTML and JavaScript. Browsing to websites with VBScript, Java, or Flash elements that contain embedded links is supported using SSL Network Extender, by defining the application as a native application.

Additionally, some sites will only work through a default browser, and therefore cannot be defined as a Web application. If that is the case, use a native application.

Web Applications of a Specific Type

It is possible to configure a Web Application with a specific type as a Domino Web Access (iNotes) application or as an Outlook Web Access application.

Domino Web Access

IBM Lotus Domino Web Access (previously called iNotes Web Access) is a Web application that provides access to a number of services including mail, contacts, calendar, scheduling, and collaboration services.

Domino Web Access requires its files to be temporarily cached by the client-side browser. As a result, the endpoint machine browser caching settings of the Mobile Access Protection Level do not apply to these
files. To allow connectivity, the cross site scripting, command injection and SQL injection Web Intelligence protections are disabled for Domino Web Access.

Note - To make Domino Web Access work through the Mobile Access portal, you must work with Hostname Translation (see "Configuring HT" on page 44).

These Domino Web Access features are not supported:
- Working offline
- Notebooks with attachments.
- Color button in the Mail Composition window.
- Text-alignment buttons in the Mail Composition window.
- Decline, Propose new time and Delegate options in meeting notices.
- Online help- partial support is available.

Outlook Web Access
Outlook Web Access (OWA) is a Web-based mail service, with the look, feel and functionality of Microsoft Outlook. Mobile Access supports Outlook Web Access versions 2000, 2003 SP1, 2007, and 2010.

Configuring Web Applications
To configure a Web Application:
1. In the Mobile Access tab navigation tree, select Applications > Web Applications.
2. Click New. The Web Application window opens.
   The following sections explain the fields in each page.

Web Application — General Properties Page
1. Go to the General Properties page.
2. Fill in the fields on the page:
   - Name is the name of the application. Note that the name of the application that appears in the user portal is defined in the Link in Portal page.
   - This application has a specific type: Select this option if the Web application is of one of the following types:
     - Domino Web Access is a Web application that provides access to a number of services including mail, contacts, calendar, scheduling, and collaboration services.
       Note -
       Domino Web Access requires its files to be temporarily cached by the client-side browser. As a result, the endpoint machine browser caching settings of the Mobile Access Endpoint Compliance Profile do not apply to these files.
       To allow connectivity, the cross site scripting, command injection and SQL injection Web Intelligence protections are disabled for Domino Web Access.
     - Outlook Web Access (OWA) is a Web-based mail service, with the look, feel and functionality of Microsoft Outlook. OWA functionality encompasses basic messaging components such as email, calendaring, and contacts.
Web Application — Authorized Locations Page

1. Go to the **Authorized Locations** page.
2. Fill in the fields on the page:
   - **Host or DNS name** on which the application is hosted.
   - **Allow access to any directory** gives the user access to all locations on the application server defined in **Servers**.
   - **Allow access to specific directories** restricts user access to specific directories. For example /finance/data/. The paths can include $$user$$, which is the name of the currently logged-in user.

   **Note** -

For an application that is defined as an Outlook Web Access application, the following are set as the allowed directories:

- Private Mailboxes: /exchange/
- Graphics and Controls: /exchweb/
- Client access: /owa/
- Public Folders: /public/

When two or more overlapping applications are configured (for example, one for any directory and one for a specific directory on the same host), it is undefined which application settings take effect. If one of the overlapping applications is OWA or iNotes, it will take precedence.

- **Application paths are case sensitive** improves security. Use this setting for UNIX-based Web servers that are case sensitive.
- **Services** that are allowed are typically HTTP for cleartext access to the Web application, and HTTPS for SSL access.

On R77.20 and higher gateways you can select which SSL version to use with HTTPS. Select an option from the list. The default is **Automatic**.

Web Application — Link in Portal Page

1. Go to the Link in Portal page.
2. Fill in the fields on the page:
   - **Add a link to this Web application/file share in the Mobile Access portal** *(Web Application without a specific type)*. If you do not enter a link, users will be able to access the application by typing its URL in the user portal, but will not have a pre-configured link to access it.
   - **This application requires a link in the Mobile Access portal** *(Web Application with a specific type)*, otherwise it cannot be accessed.

   - **Link text** *(multi-language)* is shown in the Mobile Access Portal. Can include $$user$$, which represents the user name of the currently logged-in user. If more than one link is configured with the same (case insensitive) name, only one of them will be shown in the portal.

   - **URL** is the link to the location of the application. Can include $$user$$, which represents the user name of the currently logged-in user. For example, a URL that is defined as http://host/$$user$$ appears for user aa as http://host/aa and for user bb as http://host/bb.

   - **Tooltip** *(multi-language)* for additional information about the application. Can include $$user$$, which represents the user name of the currently logged-in user. The text appears automatically when the user hovers the mouse pointer over the link and disappears when the user clicks a mouse button or moves the pointer away from the link.

Web Application — Protection Level Page

1. Go to the **Protection Level** page.
2. Select an option for **Security Requirements for Accessing this Application**:
   - Allow access to this application to any endpoint machine that complies with the security requirements of the gateway,
Applications for Clientless Access

3. Select an option for **Browser Caching on the Endpoint Machine**, to control caching of web application content in the remote user's browser.

- **Allow caching of all content** is the recommended setting when using the host name Translation method of Link Translation. This setting allows Web sites that use ActiveX and streaming media to work with Hostname Translation.

- **Prevent caching of all content** improves security for remote users accessing a Web Application from a workstation that is not under their full control, by making sure that no personal information is stored on the endpoint machine. But this setting prevents users from opening files that require an external viewer application (for example, a Word or a PDF file), and may cause some applications that rely on file caching to malfunction.

**Configuring Web Content Caching**

Protection Levels let administrators prevent browsers from caching Web content. The caching feature in most browsers presents a security risk because cache contents are easily accessible to hackers.

When the **Prevent caching of all content** option is enabled, users may not be able to open files that require an external viewer application (for example, a Word or PDF file). This requires the user to first save the file locally.

**To let users open external files:**

1. Set the Protection Level to **Allow caching of all content**.
2. To allow caching Microsoft Office documents, add them to the HTML caching category.
   a) Run: cvpnstop
   b) Backup the Apache configuration file: $CVPNDIR/conf/http.conf
   c) In this file, uncomment the CvpnCacheGroups directives related to Microsoft Office documents.
   d) In cluster setups, repeat these steps for all cluster members.
   e) Run: cvpnstart
3. Install Policy.

**Web Application — Link Translation Page**

1. Go to the **Link Translation** page.
2. Choose the Link Translation method used by Mobile Access to access this application.
   - **Use the method specified on the gateway through accessing this application** - Uses the method configured in the: Additional Settings > Link Translation page, in the Link Translation Settings on Mobile Access Gateways section.
   - **Using the following method** - Select the Link translation method (*"Link Translation" on page 42*) that will be used for this application.
     - **Path Translation** - Default for new installations.
     - **URL Translation** - Supported by the Mobile Access gateway with no further configuration
     - **Hostname Translation** - Requires further configuration see *"Configuring HT" on page 44*.

**Using the Login Name of the Currently Logged in User**

Mobile Access applications can be configured to differ depending on the user name of the currently logged-in user. For example, portal links can include the name of the user, and a file-share can include the user’s home directory. For this purpose, the **$$user** directive is used. During a Mobile Access session, $$user resolves to the login name of the currently logged-in user.

For such personalized configurations, insert the $$user string into the relevant location in the definitions of Web applications, file shares, and native applications.

For example, a Web application URL that is defined as **http://host/**$$user** appears for user aa as http://host/aa and for user bb as http://host/bb.**
If the user authenticates with a certificate, $$\text{user}$$ resolves during the user’s login process to the user name that is extracted from the certificate and authorized by the directory server.

For its use in configuring File Shares, see Using the $$\text{user}$$ Variable in File Shares (on page 51).

### Completing the Configuration of the Web Application

2. In the Policy page, associate:
   - User groups.
   - Applications that the users in those user groups are allowed to access.
   - Install On indicates the Mobile Access gateways and gateway clusters that users in those user groups are allowed to connect to.
3. From the SmartDashboard main menu, choose Policy > Install and install the policy on the Mobile Access gateways.

### Configuring a SAML Web Application

The Cloud Connector uses the SAML protocol to let users log in to SaaS (Software as a Service) applications with their corporate credentials. For more information, see sk98811 (http://supportcontent.checkpoint.com/solutions?id=sk98811).

In R77.30 and higher, you can configure a SaaS application as a Mobile Access Web application. To do this you must have the Cloud Connector feature enabled on the Security Management Server. Users can then access the SaaS application with just their corporate credentials from the Mobile Access portal or Capsule Workspace, based on the Mobile Access policy.

**To configure a SaaS application as a Mobile Access Web Application:**

1. In the Mobile Access tab, create a new Web Application.
2. On the Link in Portal page, URL field, enter the URL from the Sign-in or Log-in page URL of the SaaS app.
   - Get this URL from the Cloud Connector tab in SmartDashboard when you click on the configured application.
3. On the Single Sign-on page:
   a) Make sure that Turn on Single Sign-on for this application is selected.
   b) Select Advanced and click Edit.
   c) Select This application reuses the portal credentials. Users are not prompted.
   d) Click OK.
4. Click OK.
5. Install policy.

### Configuring a Proxy per Web Application

It is possible to define an HTTP or HTTPS proxy server per Web application. This configuration allows additional control of access to Web resources allowed to users. For configuration details see sk34810 (http://supportcontent.checkpoint.com/solutions?id=sk34810).

### Configuring Mobile Access to Forward Customized HTTP Headers

For proprietary Web applications that do not support a standard HTTP authentication method, the CvpnAddHeader directive can be used to forward end-user credentials (user name and IP address) that are carried in the HTTP header.
To configure Mobile Access to automatically forward a customized HTTP header, with a specified value, such as the user name or the client IP address:

1. Edit `$CVPNDIR/conf/http.conf`. For a Mobile Access cluster, edit all members.
2. Add or edit the line containing `CvpnAddHeader` according to the following syntax:
   ```
   CvpnAddHeader "customized_header_name" "customized_header_value"
   ```

You can use the following two macros for the `customized_header_value` string:

- `$CLIENTIP`, which is resolved to the actual IP address of the end-user’s client machine.
- `$USER NAME` which is resolved to the user name entered as a credential in the login page

Examples:

- `CvpnAddHeader "CustomHTTPHeaderName" "MyCustomHTTPHeaderValue"
- `CvpnAddHeader "CustomIPHeader" "$CLIENTIP"
- `CvpnAddHeader "CustomUsernameHeader" "$USER NAME"

### Link Translation

Mobile Access ensures secure VPN connectivity by converting HTTP requests into secure HTTPS requests and by changing the port to 443. To accomplish this, Mobile Access translates the source URL into an HTTPS URL that routes traffic to its destination via the Mobile Access gateway. The translated URL is returned to the browser and is visible to the user.

**What is Link Translation?**

Link Translation is the process by which Mobile Access converts internal URLs to public URLs that are valid on the Internet, so that internal resources become accessible via any Internet-connected browser.

Mobile Access supports different methods of Link Translation:

- **URL Translation (UT)** the original link translation method, maintained for backward compatibility.
- **Hostname Translation (HT)** provides dramatically improved performance for Mobile Access gateways and end users, resulting in faster Web access and fewer connectivity issues. It gives access a wider range of websites, with enhanced support for HTML pages, JavaScript, VBscript, and Web applications (such as the SAP Portal).
- **Path Translation (PT)** is the newest Link Translation method. It offers the same connectivity level as Hostname Translation, without the more difficult and costly configurations. (Hostname Translation requires a more expensive server certificate.)

**How Translated URLs Appear in a Browser**

A translated URL appears to users in their browser differently, for the different Link Translation methods.

<table>
<thead>
<tr>
<th>Translated</th>
<th>UT</th>
<th>HT</th>
<th>PT</th>
</tr>
</thead>
</table>

Note that the seemingly random character string, `c-dslq-itfgpae7oq`, represents the destination URL.
Link Translation Per Gateway or Per Application

Some sites work better (or only) with a specific Link Translation method. If you can choose, each method has its advantages and disadvantages.

Check Point gateway versions support these methods:

<table>
<thead>
<tr>
<th>Supporting Gateways</th>
<th>UT</th>
<th>all gateways, all versions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HT</td>
<td>R66.x and higher</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires configuration to be supported.</td>
</tr>
<tr>
<td></td>
<td>PT</td>
<td>R71.40, R75.20 and higher</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(It is the default method for R75.20 new installations.)</td>
</tr>
</tbody>
</table>

You can choose a different method for different applications. You can set the default Link Translation method used by Mobile Access applications in the gateway. And Mobile Access applications can be configured override the default translation method.

SmartDashboard Configuration of Link Translation

Link Translation can be configured to accommodate the distinctive requirements of the application (a Web application or a Citrix service) or the gateway through which the applications are accessed. For example, you can configure a particular Mobile Access application to work with URL Translation, while all other applications supplied by the gateway use Path Translation.

- You can set the default Link Translation method for all applications of a gateway - only applications that have a different specified method will not use the default method.
- You can set the default Link Translation method of a specific application - this Web application will be accessed using the selected method, even if another method is default on the gateways.
- You can configure which domains are translated. This option is in SmartDashboard for R77.30 and higher gateways. To enable this feature, you must install the R77.30 Add-on. See the Release Notes for more information.

Configuring Link Translation Domains in SmartDashboard

On R77.30 and higher gateways, configure which domains use link translation in SmartDashboard > Mobile Access tab > Additional Settings > Link Translation > Link Translation Domains.

Link Translation Domains

The options are:

- **Translate all domains** - This is the default behavior. Link translation is active for all traffic.
- **Manually configure domains to translate** - Add internal domains to the list. Only domains on the list are translated. You can also add exceptions from within a domain,. We recommend that you use this setting to improve performance. To keep communication secure, make sure all internal domains are on the list.
- **Do not translate any domain** - This is relevant for companies that do not have internal domains.

To manually configure domains to translate:

1. In the Mobile Access tab > Additional Settings > Link Translation > Link Translation Domains area, select **Manually configure domains to translate**.
2. Click **Add Domain** to add a whole domain or host (URL) to be translated.
3. Click **Add Exception** to configure a part of a domain or host within a domain that will not be translated.
4. Install policy.
Configuring UT

URL Translation is supported by all versions of gateways.

To configure UT as default method for gateways:

1. In the Mobile Access tab, click Additional Settings > Link Translation.
2. Select a gateway and click Edit.
3. Under Supported Translation Methods, leave URL Translation (always supported) selected.
5. Click OK.

To configure UT as default method for an application:

1. In the Mobile Access tab, click Additional Settings > Link Translation.
2. Select an application and click Edit.
   The Link Translation page of the Mobile Access application opens.
3. Select URL Translation.
4. Click OK.

Configuring HT

Hostname Translation enhances security by replacing the destination host name with a seemingly random character string in the URL, as it appears in the client browser.

You must configure the DNS server to resolve wildcard hostnames, to enable HT.

⚠️ Warning - If the DNS server is not configured to resolve wildcard Mobile Access host names, users will be unable to connect to Mobile Access, because the portal changes to a sub-domain: portal.ssl.example.com.

If you use Hostname Translation as your method for link translation, users must enter an FQDN as the portal URL and not an IP address.

To configure the DNS server for HT:

1. Add a record to the DNS server, to resolve Mobile Access sub-domains to the Mobile Access IP address: *.domain
   For example, assume ssl.example.com is the gateway. Configure the DNS to resolve
   *.ssl.example.com to the gateway IP address. This wildcard includes all sub-domains of the parent domain, such as a.ssl.example.com and b.ssl.example.com.
2. Define the parent domain (ssl.example.com) as a separate DNS record, to resolve Mobile Access IP address.
   This lets users access the Mobile Access portal directly, with its FQDN.
3. Use a wildcard server certificate to make sure clients can access Web applications in sub-domains behind the gateway without warnings ("Generating Wildcard Certificates for Hostname Translation " on page 177).

To configure HT as default method for gateways:

1. In the Mobile Access tab, click Additional Settings > Link Translation.
2. Select a gateway and click Edit.
   The Link Translation page of the gateway opens.
3. Click Portal Settings.
   If this message appears, clear Hostname Translation, for now:
   Hostname Translation requires Portal URL to be defined in the following format: 'https://hostname/'
4. In the Portal Settings page > Main URL, enter the portal URL of the Mobile Access gateway.
5. In the Link Translation page > under Supported Translation Methods, select Hostname Translation.
Leave **URL Translation (always supported)** selected.

If the gateway is of a version earlier than R75.20:

a) Enter the FQDN of the Mobile Access gateway in the **Link Translation** page.

b) Create or select a DNS Name object for the parent DNS names of the Mobile Access gateway. Do not include the wildcard prefix (".*") in the DNS name. For example, enter "ssl.example.com" as the DNS Name object.

6. Under **Default Translation Method**, select **Hostname Translation**.

7. Click **OK**.

**To configure HT as default method for an application:**

1. In the Mobile Access tab, click **Additional Settings > Link Translation**.

2. Select an application and click **Edit**.

   The Link Translation page of the Mobile Access application opens.

3. Select **Hostname Translation**.

4. Click **OK**.

5. Click **Advanced Hostname Translation Settings**.

6. Select a **Cookies Handling Mode**:
   - **On the gateway** - Default. All HTTP cookies that are sent to clients by internal Web servers are stored on Mobile Access, and are not passed on to the client’s browser.
   - **On the endpoint machine** - If the default setting causes the JavaScript (from the internal servers that run on the client browser) that handles HTTP cookies to fail, select this option. Mobile Access passes HTTP cookies to the browser.

7. Click **OK**.

**Statically Obscuring DNS Host Names**

By default an obscured host is always the same for each user. This utilizes the browser cache and optimizes Web browsing.

To turn off Static Obscure Key, run the following command from the Mobile Access CLI in expert mode:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C set useStaticObscureKey false
```

To turn on Static Obscure Key (the default setting), run the following command from the Mobile Access CLI in expert mode:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C set useStaticObscureKey true
```

You will be asked whether to first back up the current `$CVPNDIR/conf/cvpnd.C` file. It is recommended to do so. Follow the instructions on screen.

After making and saving the changes, run `cvpnrestart` to activate the settings.

If the Mobile Access gateway is part of a cluster, be sure to make the same changes on each cluster member.

**Configuring PT**

Path Translation is a new method, selected by default for newly installed gateways.

**To support PT on R71.40 and higher R71-series gateways:**

1. Enter expert mode.

2. Run: `cvpnPT on`

   This changes the link translation method for all applications that use the gateway default setting.

To revert the method, run `cvpnPT off`. In a cluster environment, run the cvpnPT command on all members.

**To configure PT as default method for gateways:**

1. In the Mobile Access tab, click **Additional Settings > Link Translation**.
2. Select a gateway and click Edit.
3. Under Supported Translation Methods, leave Path Translation (always supported) selected.
5. Click OK.

To configure PT as default method for an application:
1. In the Mobile Access tab, click Additional Settings > Link Translation.
2. Select an application and click Edit.
   The Link Translation page of the Mobile Access application opens.
3. Select Path Translation.
4. Click OK.

Link Translation Issues
These Link Translation configuration tips apply to Web applications.
- For Web sites that use ActiveX and streaming media, configure Mobile Access Web applications to Allow caching of all content. This is configured in the Protection Level page of the Web application.
- Domain cookies created in JavaScript are not supported. For example, if you create a cookie with the following JavaScript code:
  ```javascript```
document.cookie=Name=Value; domain=.example.com,
  ```javascript```
The client browser cannot send the cookie to Mobile Access and the Web server if Mobile Access is not located under the domain .example.com.
Note that domain cookies created in HTTP headers are supported, as long as they are not manipulated by JavaScript code.
- With Hostname Translation, the URL shown in the client browser is:
  ```https://<obscured destination host name>.<Mobile Access FQDN>/path```
  (For an explanation, see How Hostname Translation Works (see "Configuring HT" on page 44)). The maximum number of characters in each part of the host name (between https:// and the /path) is limited to 63 (see RFC 1034 - Domain names - concepts and facilities). Therefore, the entire internal host name, including the protocol and the port, must not exceed 63 characters.
- Hostnames displayed in client browsers appear as a seemingly random character string, instead of the complete destination path.
- Signing out from Outlook Web Access, from Domino Web Access (iNotes), or from Microsoft SharePoint may disconnect the Mobile Access session as well.

Link Translation Domain
Defining a Link Translation Domain for Web applications:
- Improves connectivity to external sites. For example, links to external sites displayed in emails are not broken, because they are not translated by Mobile Access.
- Reduces the load on the Mobile Access machine, thereby increasing performance.
- Saves the administrator the trouble of defining all external content as Web applications.
For R77.30 and higher gateways, configure link translation domains in SmartDashboard > Mobile Access tab > Additional Settings > Link Translation.
For R77.20 and lower gateways use the instructions in this section.

Configuring the Link Translation Domain
These instructions are for R77.20 and lower gateways. For R77.30 and higher gateways see Configuring Link Translation Domains in SmartDashboard (on page 43).
The Link Translation Domain is configured in GuiDBedit, the Check Point Database Tool. Select Connectra_Global_Properties and search for translation_domain.
Applications for Clientless Access

Link Translation Domain can be enabled or disabled. Domains and hosts can be added to or excluded from the Link Translation Domain.

After making changes, save the changes in GuiDBedit and install policy on the Security Management Server.

To configure the link translation Domain, you must define Mobile Access’s internal Link Translation domain. Only URLs in the Link Translation Domain are translated by Mobile Access. URLs from outside the Link Translation Domain are directed to their original destination.

You should include all Web resources defined as Web applications in the Link Translation Domain. You can also add additional domains or hosts to the Link Translation Domain.

To enable or disable Link Translation Domain in the Connectra_Global_Properties table:

- To enable: Set enable_translation_domain to true.
- To disable: Set enable_translation_domain to false.

To add each domain or host to the Link Translation Domain:

In the Connectra_Global_Properties table, in the domains_to_translate parameter, enter host names or domain names.

- Host names should be in the format, www.example.com
- Domain names should begin with “.”, for example, .example.com

Note - Add all DNS aliases of host names. For example, if intranet is an alias for www.example.com, you must add intranet to the Link Translation Domain.

You can exclude hosts or sub-domains that are included in the Link Translation Domain but have public access.

To exclude a host or sub-domain:

In the connectra_global_properties table, in the domains_to_exclude parameter, enter host names or domain names.

- Host names should be in the format, www.example.com
- Domain names should begin with “.”, for example, .example.com

You can add or exclude as many domains or hosts as you want.

Web Application Features

Mobile Access contains various features to make working with Web Applications efficient and secure. Some of these are described in the following sections.

Reuse TCP Connections

The Reuse TCP Connections feature enhances performance by letting the network reuse TCP connections that would otherwise be closed. To enable Reuse TCP Connections, make a change to the gateway configuration files.

Note - We strongly recommend that you back up configuration files before you make changes.

In the General Properties page of a Web application, there is a section called Application Type. In this section, you can define the application as having a specific type, either Domino Web Access or Outlook Web Access.

In previous versions, if you chose one of these Application Type options, the TCP connections for the application are closed after each request. However, if you enable Reuse TCP Connections, the connections are reused. This leads to a boost in performance as the three-way handshake does not have to be renewed and the optimized authorization cache feature can be fully utilized.
By default, Reuse TCP Connections is enabled. To turn off Reuse TCP Connections, change the following line in the `$CVPNDIR/conf/http.conf` configuration file from:

```
CvpnReuseConnections On
```

to:

```
CvpnReuseConnections Off
```

After making and saving the changes, run `cvpnrestart` to activate the settings.

If your Mobile Access gateway is part of a cluster, be sure to make the same changes on each cluster member.

**Website Certificate Verification**

In this version, Mobile Access includes the option to validate website security certificates, and either warn the user about problems, ignore any problems, or block websites with certificate problems.

By default, Website Certificate Verification is set to "monitor" this means that a record is entered in SmartView Tracker and there is no effect on end-users. The setting can also be set to "warn" so that users are alerted to any potential security issues and can then decide what steps to take. The setting can also be set to "block," which blocks any website that has a problem with its SSL server certificate, or "ignore", to ignore any issues with a website’s security. All settings create a record in SmartView Tracker except for "ignore".

You must restart Mobile Access services after changing the website certificate verification setting.

You can configure Website Certificate Verification per gateway and per application.

Website Certificate Verification is configured in GuiDBedit, the Check Point Database Tool.

**To change the Website Certificate Verification default behavior for Web applications on the gateway:**

1. In GuiDBedit, go to the table of the gateway > `Connectra_settings`.
2. Search for `certificate_verification_policy`. Enter `block`, `warn`, `monitor` or `ignore` as the value. The default is monitor.

If your internal web servers do not use a commonly known certificate (such as an internal CA), then either change the default setting, or add a trusted Certificate Authority for Website certification to Mobile Access.

If the Mobile Access gateway is part of a cluster, be sure to make the same changes on each cluster member.

**To change the Website Certificate Verification default behavior per Web application:**

1. In GuiDBedit, go to the table of the Web application in `Network Objects > network_objects`.
2. Search for `certificate_verification_policy`. Type `block`, `warn`, or `ignore` as the value.
3. For the `use_gateway_settings` parameter:
   - Enter `true` to use the gateway settings.
   - Enter `false` to use the setting configured for the application.
4. Save the changes in GuiDBedit.
5. Install policy on the Security Management Server using SmartDashboard.

**Adding a Trusted Certificate Authority for Website Certification**

You can add specific Certificate Authorities that Mobile Access does not recognize by default, such as your organization’s internal CA, to your trusted certificates. The list of default Certificate Authorities recognized by Mobile Access is the same as the list recognized by common browsers. To add CAs to this list, copy the certificate to a `.pem` file and then move the file to your Mobile Access gateway. If your Mobile Access gateway is part of a cluster, be sure to make the same changes on each cluster member.
Saving a Trusted Certificate in .pem Format

The procedure for saving a trusted certificate as a .pem file is similar for all browsers and versions with slight differences. Below is an example procedure, using Internet Explorer 7.0.

To save a trusted certificate in .pem format using Internet Explorer 7.0:
1. Using your browser, View the certificate of a website that uses the Certificate Authority you want to add. Be sure to choose the Certificate Authority certificate: In the Certification Path tab, choose the CA and click View Certificate.
2. Select the Details tab and click Copy to File. The Certificate Export Wizard opens.
3. In the Export File Format page, select Base-64 encoded.
4. In the File to Export page, type the File name under which you want to save the certificate information with a .pem file extension.
5. Click Finish.

Moving the CA Certificate to the Mobile Access Gateway

To move the CA Certificate to the Mobile Access Gateway:
1. Move the .pem file to your Mobile Access gateway, into a directory called: $CVPNDIR/var/ssl/ca-bundle/
2. Run the following command: rehash_ca_bundle
   The Certificate Authority should now be accepted by the Mobile Access gateway without any warnings. You do not need to restart Mobile Access services for the change to take effect.

Deleting a Certificate Authority from a Trusted List

To delete a Certificate Authority from your trusted Certificate Authorities:
1. Delete the .pem file from the $CVPNDIR/var/ssl/ca-bundle/ file of the Mobile Access gateway.
2. Run the following command: rehash_ca_bundle
   You do not need to restart Mobile Access services for the change to take effect.

File Shares

A file share defines a collection of files, made available across the network by means of a protocol, such as SMB for Windows, that enables actions on files, including opening, reading, writing and deleting files across the network.

File Share Viewers

Two file share viewers are available. For end-users using Microsoft Internet Explorer, the administrator can allow the end-user to choose the file share viewer:

- **Web-based file viewer** is browser-based, browser-independent, and therefore multi-platform. Note that when using this viewer, extremely large files (bigger than 2GB) cannot be viewed or accessed.
- **Windows Explorer** user interface is for Windows file shares, and requires Internet Explorer 6 or higher. It is based on Microsoft Web Folders and the WebDAV extension of HTML, and uses the familiar Windows file and folder handling model. However, the capabilities of this viewer depend on the version of Web Folders installed on the endpoint machine, and the viewer must be restarted if the user’s credentials become out of date.

Configuring File Shares

To configure a File Share Application:
1. In the Mobile Access tab navigation tree, select Applications > File Shares.
2. Click **New**. The **File Share Application** window opens. The following subsections explain the fields in each page.

**File Share Application — General Properties Page**

Go to the **General Properties** page of the **File Share Application** object. **Name** is the name of the SmartDashboard object.

**File Share Application - Authorized Locations Page**

1. Go to the **Authorized Locations** page of the **File Share Application** object.
   
   This page allows you to configure the file shares that users are authorized to access. These settings take effect whenever a user attempts access, no matter what interface is used, whether by manually typing a path in the portal, browsing using the file viewer, clicking a user-defined file favorite, or clicking the predefined file favorite path defined by the administrator in the **Link in Portal** page.

2. Fill in the fields on the page:
   - **Servers** are the machine(s) or DNS Name(s) on which the file server is hosted. Choose either a single **Host or DNS name**, or **Multiple hosts**.
   - **Allow access to any file share** gives the users access to all locations on the file server defined in Servers.
   - **Allow access to specific file shares** restricts user access to specific shares. For example **My_Share**. Use only the name of a share, such as **My_share$$user**, or **My_share$$user** without any slashes. Do not specify a subdirectory inside a share. The **$$user** variable represents the name of the currently logged-in user. This variable provides personalized authorization for users. If **$$user** is defined as a file share, then if the user currently logged-in is **alice**, **alice** will be allowed access to the share named **alice** defined on the server, such as **\myserv\alice**.

   If you configure two or more overlapping file share applications (for example, one for Any Share and one for a specific share on the same host), the application settings that are in effect are undefined.

**File Share Application — Link in Portal Page**

This page allows you to configure one predefined favorite link. This link is displayed in the Mobile Access portal. By clicking the link the user is able to directly access the specified path. Note that you must authorize access to this location in the **Authorized Locations** page.

1. Go to the **Link in Portal** page of the **File Share Application** object.

2. Fill in the fields on the page:
   - **Add a link to this file share in the Mobile Access portal**. If you do not enter a link, users will be able to access the application by manually typing its link in the portal, but will not have a pre-configured link to access it.
   - **Link text (multi-language)** is shown in the Mobile Access Portal. Can include **$$user**, which represents the user name of the currently logged-in user. If more than one link is configured with the same (case insensitive) name, only one of them will be shown in the portal.
   - **Path** is the full file path that the link will attempt to access, specified using UNC syntax. It can be either a location of a share, or any path under the share. Can include **$$user**, which represents the user name of the currently logged-in user. For example, a path that is defined as **\host\Pub\users\$$user** appears for user **alice** as **\host\Pub\users\alice** and for user **Bob** as **\host\Pub\users\Bob**.

   **Note** - The **host** defined here is the same host that is defined in the **Authorized Locations** page. The IP address of the host is resolved by the DNS Server that is defined on Mobile Access (not by the Mobile Access management).

   - **Tooltip (multi-language)** for additional information. Can include **$$user**, which represents the user name of the currently logged-in user. The text appears automatically when the user pauses the mouse pointer over the link and disappears when the user clicks a mouse button or moves the pointer away from the link.
Applications for Clientless Access

File Share Application — Single Sign-On Page

To configure Single Sign On:

1. Go to the Single Sign On page of the File Share Application object.
2. Select Turn on single Sign On for this application.
3. Configure the sign on method for the application. The default option is: Prompt the users for their credentials and store them for future use.

File Share Application — Protection Level Page

1. Go to the Protection Level page of the File Share Application object.
2. Fill in the fields on the page:
   - Security Requirements for Accessing this Application allows you to:
     - Allow access to this application to any endpoint machine that complies with the security requirements of the gateway.
     - Make access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile.

Completing the Configuration of the File Share Application

1. Go to the Access to Application page of the Mobile Access tab.
2. In the Access to Application page, associate:
   - User groups.
   - Applications that the users in those user groups are allowed to access.
   - Install On are the Mobile Access gateways and gateway clusters that users in those user groups are allowed to connect to.
3. From the SmartDashboard main menu, choose Policy > Install... and install the policy on the Mobile Access gateways.

Using the $$user Variable in File Shares

You can configure personalized user locations that use the login name of the currently logged in user. To do this, use the $$user variable (see "Using the Login Name of the Currently Logged in User" on page 40) wherever you need to specify the name of the user. The $$user variable is resolved during the Mobile Access session to the login name of the currently logged-in user.

For example, a UNC file path that is defined as \host\Pub\$$user is resolved for user Alice as \host\Pub\Alice and for user Bob as \host\Pub\Bob.

Citrix Services

Mobile Access supports Citrix client connectivity to internal Presentation servers. In this type of deployment, Mobile Access functions as a Secure Gateway.

You do not need to use Secure Ticketing authority (STA) servers because Mobile Access implements its own STA engine. But, you can install Mobile Access in a topology with STA and Citrix Secure Gateway (CSG) servers.

Citrix Deployments Modes - Unticketed and Ticketed

Unticketed Mode

In the recommended Unticketed Mode scenario:

- The remote access user logs into the Mobile Access user portal.
- Using the Mobile Access Web interface, the user is directed to the Citrix Web Interface server and then has access to the Presentation server.
Ticketed Mode
In the Ticketed Mode scenario:

- The remote access user logs into the Mobile Access user portal.
- Using the Mobile Access Web interface, the user is directed to the Citrix Web Interface server.

The user logs into the Citrix Web Interface server and is assigned a secure ticket by the Secure Ticket Authority. This ticket allows the user to access the Presentation server once it is verified by the Mobile Access Web Security Gateway.

You do not need to use Secure Ticketing authority (STA) servers because Mobile Access implements its own STA engine.

Configuring Citrix Services

To configure a Citrix Service:
1. In the Mobile Access tab navigation tree, select Applications > Citrix Services.
2. Click New. The Citrix Services window opens.

Before Configuring Citrix Services

The server certificate for Mobile Access must be based on a FQDN (Fully Qualified Domain Name) and issued to the Mobile Access FQDN. For example www.sample.com.

Before you configure Citrix Services, change the Mobile Access server certificate to one that was issued to the FQDN. This is necessary to comply with the Citrix standards for server certificates. Additionally, end-users must browse to Mobile Access using the FQDN that is routable from their network.

Note - Make sure that the certificate is installed on the server (see "Server Certificates" on page 176).

If your Web Interface server is configured to deploy ICA Web clients and the Mobile Access server certificate is issued by a private CA, the certificate’s public key must be installed on the client side browser for the ICA Web Client to function properly. The Mobile Access certificate public key is located under: $CVPNDIR/var/ssl/server.crt

Citrix Service — Web Interface page
1. Go to the Web Interface page of the Citrix Service object.
2. Fill in the fields on the page:
   - Servers are the machine(s) or DNS Name(s) on which the Web Interface server is hosted. Choose either a single Host or DNS name, or Multiple hosts. In order to keep the environment simple, it is recommended to configure a single Web Interface server per Citrix Application.
   - Services must match the settings on the Web Interface server. Select http or https, as required. Other services are NOT supported.

Citrix Service — Link in Portal Page
1. Go to the Link In Portal page of the Citrix Service object.
2. Fill in the fields on the page:
   - Link text (multi-language) is shown in the Mobile Access Portal. If more than one link is configured with the same (case insensitive) name, only one of them will be shown in the portal.
   - URL is the link to the location of the application, or to a subdirectory of the application.
   - Tooltip (multi-language) for some additional information. The text appears automatically when the user pauses the mouse pointer over the link and disappears when the user clicks a mouse button or moves the pointer away from the link.
Citrix Service — STA Servers Page
1. Go to the STA servers page of the Citrix Service object.
2. Get the Host from the current settings on the Web Interface (WI) server.
3. Get the STA ID from the Secure Ticketing Authority (STA) servers.

Note - Mobile Access implements its own Secure Ticketing authority (STA) engine. STA servers are not necessary.

To get the host name or IP address:
1. Login to the Web Interface Citrix administration page.
2. Click Server-Side Firewall.
3. Scroll to the Secure Ticket Authority list.
   • If the field is blank, you are in unticketed mode and you do not need to define any STA Servers on Mobile Access.
   • If the field contains entries, you are in ticketed mode. Each entry in this list is a URL containing the IP or FQDN of a Citrix server. Every entry in the Secure Ticket Authority list must be separately entered into Mobile Access.

To get the STA ID:
1. Login to the STA server.
2. From the Windows Start menu, select Programs > Citrix > Citrix Secure Gateway > Secure Ticket Authority Configuration.
3. Click Next.
The STA ID is shown in the Enter the STA ID field.

Citrix Service — MetaFrame Servers Page
Go to the MetaFrame servers page of the Citrix Service object. In this page you can allow access to all Presentation Servers, or restrict access to defined MetaFrame servers.

If you select Restrict access to these servers only:
• Define the servers using an IP address or Fully Qualified Domain Name (FQDN).
• Make sure that the definition matches the configuration made on the XenApp server farm. If you do not, Mobile Access may not authorize the connection. The Presentation server configuration affects one of the parameters in the ICA file that is received by the client.

Citrix Service — Single Sign On Page
Single Sign On increases application security.

To configure Single Sign On:
1. Go to the Single Sign On page of the File Share Application object.
2. Select Turn on single Sign On for this application.
   Configure the sign on method for the application.

Citrix Service — Protection Level Page
1. Go to the Protection Level page of the Citrix Service object.
2. Enter data in these fields:
   Security Requirements for Accessing this Application lets you:
   • Allow access to this application to any endpoint that complies with the security requirements of the gateway.
   • OR make access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile.
Note - The Citrix architecture requires ICA files and ActiveX executables to be temporarily cached by the client-side browser. As a result, Mobile Access's Protection Level settings do not apply to these files.

3. Get the Host and the STA ID of the Secure Ticketing Authority (STA) servers from the current settings on the Web Interface (WI) server.
   Note - Mobile Access implements its own Secure Ticketing authority (STA) engine. STA servers are not necessary.

To get the hostname or IP address:
1. Login to the Web Interface Citrix administration page.
2. Click Server-Side Firewall.
3. Scroll to the Secure Ticket Authority list.
   - If the field is blank, you are in unticketed mode and you do not need to define any STA Servers on Mobile Access.
   - If the field contains entries, you are in ticketed mode. Each entry in this list is a URL containing the IP or FQDN of a Citrix server. Every entry in the Secure Ticket Authority list must be separately entered into Mobile Access.

To get the STA ID:
1. Login to the STA server.
2. From the Windows Start menu, select Programs > Citrix > Citrix Secure Gateway > Secure Ticket Authority Configuration.
3. Click Next.
   The STA ID is shown in the Enter the STA ID field.

Completing the Configuration of the Citrix Service
1. Go to the Access to Application page of the Mobile Access tab.
2. In the Access to Application page, associate:
   - User groups.
   - Applications that the users in those user groups are allowed to access.
   - Install On are the Mobile Access gateways and gateway clusters that users in those user groups are allowed to connect to.
3. From the SmartDashboard main menu, click Policy > Install and install the policy on the Mobile Access gateways.

Web Mail Services

Mobile Access supports built-in Web mail. Web mail provides a simple way for remote users, through a web browser interface, to access their email. Employees can access their email from any computer that has access to the Internet, such as a computer in a library, or Internet cafe. There is no need to install special email or remote access software. This is helpful for employees who work outside the office on a regular basis.

Note - The traffic log does not show actions done by the user through the Web mail interface.

Mobile Access also supports the IBM Lotus Domino Web Access (DWA, formerly known as iNotes) and Outlook Web Access (OWA). DWA and OWA are configured in Mobile Access as Web Applications.
**Web Mail Services User Experience**

Remote users login to Mobile Access and authenticate themselves in order to gain access to the portal. They can then click a link to access the Web mail application. Mobile Access can be configured to reuse the login credentials when authenticating to the IMAP account on the mail server. If the reused credentials are incorrect, Mobile Access again presents the user with a login page. Valid credentials are saved for future logins.

Once authenticated to the mail application, users can:
- Compose, send and receive email.
- Create, delete, rename, and manipulate mail folders.
- Index messages in various ways.
- Stores addresses.
- Search emails according to various criteria, such as body text, subject and sender’s address.
- Highlight messages with different background colors, enabling quick differentiation.
- Display preferences.

**Incoming (IMAP) and Outgoing (SMTP) Mail Servers**

Mobile Access provides a Web front-end for any email application that uses the IMAP protocol for incoming mail, and SMTP for outgoing mail.

Email stored on the IMAP server is manipulated through the browser interface without having to transfer the messages back and forth. Users can connect to several mail servers depending on their authorization.

**Configuring Mail Services**

To configure a Web Mail application:
1. In the Mobile Access tab navigation tree, select **Applications > Web Mail**.
2. Click **New**. The Web mail service window opens. The following sections explain the fields on each page.

**Web Mail Service — General Properties Page**

1. Go to the **General Properties** page of the Web mail service object.
2. Fill in the fields on the page:
   - **Name** for the mail service, for example, my_mail_server
   - **Outgoing Mail Server (SMTP)**
     - **Host or DNS Name**, for example, smtp.example.com
     - **Service** is normally the standard predefined SMTP service.
   - **Incoming Mail Server**
     - **IMAP server type**
     - **Host or DNS Name**, for example, smtp.example.com
     - **Service** is normally the standard predefined IMAP service.

**Web Mail Service — Link in Portal Page**

1. Go to the **Link In Portal** page of the Web mail service object.
2. Fill in the fields on the page:
   - **Link text (multi-language)** is shown in the Mobile Access Portal. If more than one link is configured with the same (case insensitive) text, only one of them will be shown in the portal.
   - **Tooltip (multi-language)** for additional information. The text appears automatically when the user pauses the mouse pointer over the link and disappears when the user clicks a mouse button or moves the pointer away from the link.
Web Mail Service — Single Sign-On Page
1. Go to the Single Sign On page of the Web mail service object.
2. Select the sign on method for the application.
For more information, see Single Sign On.

Web Mail Service — Protection Level Page
1. Go to the Protection Level page of the Web mail service object.
2. Fill in the fields on the page:
   - Security Requirements for Accessing this Application allows you to
     - EITHER allow access to this application to any endpoint machine that complies with the security requirements of the gateway,
     - OR make access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile.

Completing the Configuration of the Web Mail Service
1. Go to the Access to Application page of the Mobile Access tab.
2. In the Access to Application page, associate:
   - User groups.
   - Applications that the users in those user groups are allowed to access.
   - Install On are the Mobile Access gateways and gateway clusters that users in those user groups are allowed to connect to.
3. From the SmartDashboard main menu, choose Policy > Install and install the policy on the Mobile Access gateways.

Enabling LDAP Contacts Search in Web Mail Applications
By default, the contact search in Web Mail applications works only for internal users that are defined on the Mobile Access gateway. To enable search on contacts that are defined on an LDAP server, see sk34997 (http://supportcontent.checkpoint.com/solutions?id=sk34997).

Native Applications
Native applications are not clientless. They require the SSL Network Extender client on the endpoint machine. See Native Applications for Client-Based Access (on page 73).

DNS Names
If an internal application is hosted on a server inside the organization, using a DNS Name object in the definition of the Mobile Access application makes it possible to change the IP address of the server without having to change the definition of the host object in the Mobile Access application.

For example, if "myhost.example.com" is used in the definition of a Mobile Access application, Mobile Access resolves the IP address of "myhost" when authorizing access to the application.

If an internal application is hosted on multiple replicated servers, a single DNS Name object can be used in the definition of the Mobile Access application, instead of having to individually define each host.

The DNS server that is specified on Mobile Access resolves the DNS names. To set or change the DNS server, use the sysconfig command.
DNS Names and Aliases

A DNS name can have a number of aliases. For example, www.example.com, www.example.co.uk and www.example.co.fr could be aliases of the same DNS name.

In the definition of the DNS Name object, use the format "a.b ... x.y.z", where each section of the DNS name is demarcated by a period. For example, mail.example.com or www.example.co.uk.

Wildcards can be used at the beginning of a domain name, but not at the end. For example, *.example.com includes www.example.com and mail.example.com. On the other hand, www.example.* is NOT valid.

Where DNS Name Objects are Used

DNS objects are used when defining hosts for Mobile Access Web applications, file share applications, Citrix services, and Web mail services. They are also used when configuring support for Hostname Translation.

DNS Name objects cannot be used in the Security Rule Base.

Defining the DNS Server used by Mobile Access

The DNS server that resolves the IP addresses of the DNS Name objects must be defined in one of these locations:

1. In SmartDashboard, in the Mobile Access tab, go to the Additional Settings > Network Accessories > Name Resolution page.
2. From the Mobile Access Security Gateway do these procedures with the command line or the Web User Interface:

<table>
<thead>
<tr>
<th>SecurePlatform</th>
<th>Using the Console</th>
<th>Using the Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run sysconfig.</td>
<td>Select Domain Name Servers.</td>
<td>Go to the SecurePlatform Administration Portal in your browser.</td>
</tr>
<tr>
<td>Select Domain Name Servers.</td>
<td>Configure the DNS.</td>
<td>Go to the Network &gt; DNS page.</td>
</tr>
<tr>
<td>Configure the DNS.</td>
<td></td>
<td>Configure the DNS.</td>
</tr>
</tbody>
</table>

| Gaia | Run set dns primary <ip_address> | Connect your browser to the Gaia WebUI. |
| Optional: Run set dns suffix VALUE. | Go to the Interface Management > Hosts and DNS page. | Configure the DNS. |
| An example of VALUE is example.com | Run save config | |

Configuring DNS Name Objects

To create a DNS Name object:

1. In SmartDashboard, select Network and Resources > DNS Names.
2. Click New.
   The DNS Name window opens.
3. Give the DNS Name object a Name.
4. Click DNS Names.
   The DNS Names window opens.
5. Click Add.
   The Edit DNS Name window opens.
6. Type the DNS name.
7. Click OK three times.
   The DNS Name window closes.
Using the Login Name of the Currently Logged in User

Mobile Access applications can be configured to differ depending on the user name of the currently logged-in user. For example, portal links can include the name of the user, and a file-share can include the user’s home directory. For this purpose, the $$user directive is used. During a Mobile Access session, $$user resolves to the login name of the currently logged-in user.

For such personalized configurations, insert the $$user string into the relevant location in the definitions of Web applications, file shares, and native applications.

For example, a Web application URL that is defined as http://host/$$user appears for user aa as http://host/aa and for user bb as http://host/bb.

If the user authenticates with a certificate, $$user resolves during the user's login process to the user name that is extracted from the certificate and authorized by the directory server.

For its use in configuring File Shares, see Using the $$user Variable in File Shares (on page 51).

WebSockets

WebSockets support in the Mobile Access Software Blade gives remote terminal access from a browser, without a pre-installed RDP/VDI client.

This feature is supported in R77.10 and higher.

For WebSockets system requirements, see sk95311 (http://supportcontent.checkpoint.com/solutions?id=sk95311).

Check Point appliances can support hundreds of concurrent WebSocket users. The amount depends on the power of the appliance and their deployment (Load Sharing an appliance cluster can support more users). To get the best appliance that best suit your needs, contact your Check Point sales engineer.

Using WebSockets

To use WebSockets support:

Create a regular Web application to the WebSocket server.

- Make sure to include the port used for the WebSocket connection in the Authorized Locations of the Web application.

- The Web applications related to the WebSocket application must use Path Translation as their Link Translation method. It can be inherited from the gateway setting or configured in the Web application.

Monitoring WebSockets

To monitor WebSocket connections:

1. On the Security Gateway, enter expert mode.
2. Run: [expert@hostname:0]# PingerAdmin report type ws
   Or, to see all connections currently handled by the Pinger daemon (such as ActiveSync push), run: [expert@hostname:0]# PingerAdmin report all
Chapter 5

Single Sign On

In This Section:

Supported SSO Authentication Protocol .......................................................... 59
HTTP Based SSO .................................................................................................. 59
Web Form Based SSO ................................................................. 60
Application and Client Support for SSO ....................... 62
Basic SSO Configuration ............................................................................................ 63
SSO for Native Applications ................................................................................. 63
Advanced Configuration of SSO ........................................................................... 64
Advanced Configuration of Web Form SSO .......................................................... 66
Kerberos Authentication Support ................................................................. 67
Kerberos Constrained Delegation ........................................................................ 70
Certificate Attribute Forwarding ...................................................................... 72

Single Sign On (SSO) eliminates the need for users to re-authenticate to an application when they access it for a second time, during a Mobile Access session, or between sessions. The authentication credentials used to log in to the Mobile Access portal can be re-used automatically to authenticate to multiple applications accessed through Mobile Access. You can also record other credentials for the application, and store them for future use. SSO user credentials are securely stored on Mobile Access and therefore remain valid even if the user logs in from a different client machine.

Supported SSO Authentication Protocol

Mobile Access supports Single Sign On for authentication to internal Web and other application servers. The supported authentication protocols are:

- Basic Access - RFC enhancement. Not recommended because of security implications.
- Digest Access - RFC enhancement.
- Credential forwarding in HTTP headers - Ad hoc solution. Not recommended because of security implications.
- Web form (HTML) based.

HTTP Based SSO

For applications that perform authentication at the HTTP level, HTTP-based SSO is available, in which the credentials are forwarded in HTTP headers. This applies to the Basic, Digest, Integrated Windows Authentication, and Credential forwarding in HTTP headers authentication protocols.
When the user attempts to access these sites, a browser-specific form appears:

![Web Credentials - www.example.com](image)

The user must enter his/her user name and password for that application, and click OK.

**HTTP Based SSO Limitation**

If the Web server requests authentication for a POST request in either the digest or Integrated Windows Authentication methods, and the server does not support sending of "100 Continue" responses, Single Sign On is not supported.

**Web Form Based SSO**

Most Web applications have their own Web forms for authentication. For these applications, Mobile Access supports Web form (HTML) based SSO.

The advantage of Web form based SSO authentication over HTTP authentication is that users are presented with the login page of the application itself, rather than a more obtrusive browser-specific page.
A typical Web form is shown below, for Outlook Web Access, together with a Mobile Access SSO popup that assists the user.

It is recommended to use the Web form based SSO for every application that is configured to work with Web form authentication. Do not enable Web form SSO for other applications, in order to maintain performance and connectivity.

**Application Requirements for Easy Configuration**

Web form based SSO in its default configuration can be configured by selecting a single check box in SmartDashboard. In order for the default settings to work, the application must:

- Present the login form as the first form seen by the user.
- Redirect (status 301 or 302) on login success.

**Web Form Based SSO Limitations**

Web form based SSO does not support:

- Password remediation forms.
- Forms containing ‘old/new/confirm’ password fields. These fields are not recognized properly, and wrong credentials may be recorded or forwarded.

**Configuring SSO Name Format**

This feature prevents problems with SSO caused by different formats of credentials required by different applications. You configure the credential format for each application in GuiDBedit, and the Mobile Access gateway sends the credentials to the organizational server in the correct format. This applies to Web, Capsule Workspace Mail, and ActiveSync applications and works with Web Form based SSO.

**Note** - This feature is for LDAP users who connect to the Mobile Access portal. Internal users who connect to web applications though the portal with SSO authentication use a default of $$user.

For example, SSO can apply to both of these applications:

- Web application A that uses the format domain/username
- ActiveSync application B that uses the format username@domain
This feature is supported in R77.20 and higher. To learn how to activate this feature in R77.20, see sk101217 (http://supportcontent.checkpoint.com/solutions?id=sk101217).

To configure the format of credentials required for an application in R77.30 and higher:
1. Go to the Mobile Access tab > Applications.
2. Select an application type.
3. Click Edit to open an application.
4. Select Additional Settings > Single Sign-on.
5. In the Credentials Formats area, select the required format for the application.
6. Click OK.
7. Install policy.

To configure the format of credentials required for an application in R77.20:
1. Open GuiDBedit.
2. For a Capsule Workspace Mail or Web application, go to Other > network_applications > APPLICATION NAME > single_sign_on > username_and_domain_format.
3. For an ActiveSync application, go to Other > network_applications > APPLICATION NAME > username_and_domain_format.
4. Enter the internal server format credentials with these place holders:
   - $$user for user name
   - $$domain for domain
   For example, $$domain$$user or $$user@$$domain.
5. Save the changes.
6. Install policy.

Application and Client Support for SSO

The following table shows which SSO methods are available for each Mobile Access application:

<table>
<thead>
<tr>
<th>Mobile Access Application</th>
<th>Supports HTTP Based SSO</th>
<th>Supports Web Form Based SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File shares</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Citrix services</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Mail</td>
<td>Simplified</td>
<td>No</td>
</tr>
<tr>
<td>Native applications</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Most Mobile Access Web Applications and Citrix Services support Web Form SSO, with either no configuration, or minimal configuration required. Some applications have been tested and found to require manual configuration (of the HTTP Post details). Some applications do not support Web Form SSO at all.

For a list of common applications that are certified by Check Point to work with Web Form SSO, see SecureKnowledge solution sk35080 (http://supportcontent.checkpoint.com/solutions?id=sk35080).

**Mobile Access Client Support for SSO**

Single Sign On is available only via the Mobile Access portal. It is not available for authentication via the VPN clients: SSL Network Extender, SecureClient Mobile, and Endpoint Connect.
Basic SSO Configuration

To configure a basic SSO setup:

1. In the SmartDashboard Mobile Access tab, select the Additional Settings > Single Sign On page.
2. In the Single Sign On page, select an application and click Edit.
   The Single Sign On page of the application window opens.
3. Select Turn on single Sign On for this application.
4. Configure the sign on method for the application. The default option is:
   For Web applications, File Shares and Citrix Services:
   Prompt the users for their credentials and store them for future use
   For Web Mail applications this same option is called:
   Prompt user for credentials
   With this option, the application credentials are stored and reused. The portal credentials are not used to authenticate to applications.

Basic Configuration of Web Form SSO

Web form SSO is supported only for Mobile Access Web applications and Citrix services.
In the default settings, Web Form Single Sign On automatically analyses the sign-in Web page of the application. The default settings assume:
- HTTP redirect (301, 302) upon authentication success.
- No redirect upon authentication failure.

To configure Web Form SSO with default settings:

In the Single Sign On page of the Mobile Access application, select This application uses a Web form to accept credentials from other users

Note - Only enable Web form SSO for applications that use a Web form to accept user credentials, in order to maintain performance and connectivity.

SSO for Native Applications

Native applications that you access with SSL Network Extender can use Single Sign-On (SSO) functionality. With SSO support, users connect automatically to native applications that require login. The native application gets the Mobile Access portal login username and password parameters from the internal server.

This feature is supported in R77.20 and higher. It requires a SSL Network Extender client upgrade.

Configuring SSO for Native Applications

Use the dynamic parameters $$user and $$password to configure SSO for a native application. These parameters are resolved to the actual username and password of the logged-in user when the gateway sends the parameters to the native application.

These instructions show you how to configure the new $$password parameter in for a Simple native application. You can also use the $$password parameter in the application parameters in Advanced native applications.

To configure SSO:

1. Open SmartDashboard.
2. From the Mobile Access tab, select Applications > Native Applications.
3. Edit an existing or create a new native application object.
4. Select Endpoint Applications from the navigation tree of the object.
5. Select **Simple (Application is installed on the endpoint machine)** and enter information for these fields:
   - **Path and executable name** - Enter the path of the native application.
     For example for Remote Desktop Plus: `D:\rdp.exe`
   - **Parameters** - Enter this syntax for the username, password, and target remote host to connect to.
     For example: `/u:acme\$user /p:$password /v:192.0.2.2 /f`
     This setting defines how the gateway sends the username and password of a locally logged-in user to the native application.

6. Click **OK**.

7. Install policy.

**Advanced Configuration of SSO**

The following configuration instructions apply to both HTTP based SSO and to Web form based SSO. The advanced configuration options are supported for Web applications, file shares, and Citrix services.

For configuration options that are specific to Web form SSO, see **Advanced Configuration of Web Form SSO (on page 66).**

**Configuring Advanced Single Sign On**

There are a number of Single Sign On methods. The different options allow you to configure how to handle portal credentials, and how to handle other credentials used to authenticate to the application.

To configure the Single Sign On methods:
1. Go to the **Single Sign On** page of the Mobile Access application.
2. For the **Advanced** options, click **Edit**.
These are the available single sign on methods.

<table>
<thead>
<tr>
<th>SSO Method</th>
<th>Single Sign On is On/Off</th>
<th>Forward portal credentials</th>
<th>Learn other credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn on Single Sign On for this application - Unchecked</td>
<td>Off</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Users are always prompted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prompt users for their credentials, and store them for future use</td>
<td>On</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Default method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This application reuses the portal credentials. Users are not prompted.</td>
<td>On</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Advanced method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This application reuses the portal credentials. If authentication fails, Mobile Access prompts users and stores their credentials.</td>
<td>On</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Advanced method</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Login Settings**

Login settings allow you to configure the default Windows domain (if Windows authentication is being used), to notify users that their credentials will be stored, and to specify a hint to help users supply the correct credentials.

To configure the login settings for Single Sign On:

2. In the Login Settings section, click Edit.
   The Login Settings window opens.
3. Fill in the fields according to the explanations below.

**Windows Domain**

- The user of this application belongs to the following Windows domain:

  Specify the Windows domain or workgroup (for example "LOCALDOMAIN") if Windows authentication is used. Integrated Windows authentication requires the domain to be forwarded with the user name and password.

  If Accept the portal credentials from the gateway Single Sign On method is used, Mobile Access does not know the domain, because the user does not supply it with the portal credentials. The domain is fetched from the one specified here.

**User Notification**

- Notify the users that their credentials for this application are going to be stored

  When users access the application login page for the first time, they see a message that their credentials will be stored for future access.

- Allow the users to specify that their credentials for this application will not be stored

  When users access the application login page for the first time, they see a message from which they can select not to record their credentials.
Administrator Message

- **Show the following message together with the credentials prompt**
  Show a hint to the user about the credentials they must supply, for example, whether or not they should supply the domain name and user name (for example: AD/user) or just the user name (for example: user). After clicking the *Help me choose credentials* link, the user sees the hint. The message can include ASCII characters only.

Advanced Configuration of Web Form SSO

Use the advanced Single Sign On settings for Web form credentials to configure an application for Web form SSO if there is one of these:

- No HTTP redirect (301, 302) upon authentication success
- No redirect upon authentication failure.

You can specify different criteria for:

- Sign In Success or Failure Detection
- Credential Handling

**Sign In Success or Failure Detection**

Most Web applications respond to authentication success by redirecting to another page. If a redirect is not an indication of success, you can configure a different indicator of success or failure.

**To configure Sign In success or failure criteria:**

1. In the **Single Sign On** page of the Mobile Access application, in the **Web Form** section, click **Edit**.
2. Select **Specify a criterion for success or failure** and then select one of the following options:
   - **Mobile Access regards the authentication as successful, if after signing in, this application creates a cookie with the following name:**
     The application places a session cookie upon success. To obtain the exact name of the session cookie, install a sniffer or browser plug-in (such as the Fiddler HTTP debugging proxy).
   - **Mobile Access regards the authentication as a failure, if after signing in, this application redirects to the following URL:**
     The application redirects on failure. To find the target URL, install a sniffer or browser plug-in (such as the Fiddler HTTP debugging proxy). Use the following URL format:
     `<protocol>://<host>/[<path>]?< query>`

**Credential Handling**

By default, Mobile Access looks for the user name and password fields at the application URL. If the default settings do not work, you can either configure an automatic credential detection method, or you can manually hard-code the POST details.

**To configure automatic credential handling:**

1. In the **Single Sign On** page of the Mobile Access application, in the **Web Form** section, click **Edit**.
2. In the **Credentials Handling** section, click **Edit**.
   The **Credentials Handling** window opens.
3. Select **Automatically handle the credentials**.
4. Under **Sign in Web Form Detection Settings**, select:
   - **Mobile Access regards the following URL as the sign in Web form:**
     If the application presents a Web form that requires credentials, before the actual login form, so that Mobile Access is unable to automatically analyze the sign-in Web page, you can specify the URL of the actual login form.
     Syntax:
     `<protocol>://<host>/[<path>]?< query>`
5. Under **Password Validation Settings**, select

**Mobile Access sends the following password:**

Clients need to submit the sign on Web form with a user name and password. However, it is not secure to store the password on the client for future SSO use. Mobile Access therefore generates a dummy password that it sends to the client, and replaces it upon sign on with the real password. Some applications check the dummy password on the client side. If the Mobile Access dummy password is not compatible with the application, you can define a different one.

Note - This password cannot include special characters. Use ASCII characters only.

**Manually Defining HTTP Post Details**

If automatic Web form SSO does not work, you can define HTTP POST details.

To manually specify how to handle credentials:

1. From the **Credentials Handling** window, select **Manually specify how to handle the credentials**.
2. Fill in the fields for **When the following sign in URL is requested**:
   - **post to the following URL**
     In this and the previous field, the URL must be absolute. Use the URL format
     `<protocol>://<host>[/<path>][?< query>]`
   - **the following POST data**, which must include:
     - `$USERNAME` resolves to the user name stored on Mobile Access.
     - `$PASSWORD` resolves to the password stored on Mobile Access.

When manual credential handling is configured for Web form SSO, the HTTP authentication request window appears, when credentials are requested for the first time.

**Kerberos Authentication Support**

Kerberos is a network protocol that lets people and computers securely authenticate over a non-secure network. In Windows 2000 and higher, Kerberos is the default authentication protocol.

- Kerberos Authentication is supported for Web Applications (HTTP and HTTPS). Mobile Access can authorize against Kerberos servers on behalf of users.
- Microsoft IIS and other web servers employ Kerberos using the *Negotiate* method in HTTP authentication headers.
- Kerberos is sensitive to time differences between the Security Gateway and Domain Controller. Make sure clocks on the Mobile Access gateway and on the domain controller(s) are synchronized to within 1 minute. The best way to ensure this is to use an NTP time server.

**To use Kerberos with Mobile Access:**

- If Microsoft Active Directory is configured, the gateway automatically updates with the relevant settings from the AD Account Unit and Kerberos enabled. You can review the Kerberos settings in `$CVPNDIR/var/krb5.auto.conf`
  
  **Warning**: Do not manually edit `krb5.auto.conf`.

- If you must make a change to `krb5.auto.conf`, do it in the template file, `krb5.auto.conf.template`. The template is used to create the `krb5.auto.conf` file.

  To edit `krb5.auto.conf.template`:
  a) Open `$CVPNDIR/var/krb5.auto.conf.template` and add your changes.

  The file contains Kerberos conf file information and place holders for the Account Unit settings - the place holders are in the form of `<++PlaceHolderName+++>`.

  **Important**: Do not change the place holder names.
b) On the gateway, run: cvpnd_admin policy

Example of the template file, krb5.auto.conf.template:

```
[libdefaults]
<++libdefaults++>
rdns = false
[realms]
<++realms++>
[domain_realm]
<++domain_realm++>
```

Example of how it looks in krb5.auto.conf:

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
[realms]
EXAMPLE.COM = {
    kdc = 192.168.1.1
}
[domain_realm]
```

- If Microsoft Active Directory is not yet configured for Mobile Access, but you want to use it:
  a) Use the Mobile Access wizard to configure your AD.
  b) Edit the SmartDashboard Network Objects for the AD server and for the gateway ("Configuring Microsoft Active Directory for Mobile Access" on page 68).

- If you do not want to use Microsoft Active Directory, manually configure Kerberos for your environment ("Manual Configuration for Kerberos" on page 69).

**Configuring Microsoft Active Directory for Mobile Access**

If Microsoft AD is not configured in the Check Point environment, create or edit the required Network Objects. Use these steps if the LDAP Account Unit object was created without the Mobile Access wizard, or if there are connectivity issues with the AD Domain Control.

**Note:** In some environments, you will have to manually configure the AU object and the gateway object, even if you used the Wizard. Use these steps to make sure the settings are correct after you finish the wizard.

These steps assume you defined the Microsoft AD server as a Check Point LDAP Account Unit object. If that object does not exist, create one: Network Objects > Servers and OPSEC Applications > New > LDAP Account Unit.

**To make sure Microsoft Active Directory is configured for default settings:**

1. In the SmartDashboard, open the LDAP Account Unit object that represents the AD.
   In the General tab of the LDAP Account Unit Properties window, the value of Profile is Microsoft_AD.
2. Make sure the value of Domain is correct for the AD Domain.
3. Save changes and close the window.
To configure Microsoft Active Directory server priorities:

1. Open the object for the Security Gateway with Mobile Access enabled.
   If there is more than one, do these steps for each.
2. Open Other > User Directory.
   By default, the gateways use all Domain Controllers of the AD. If there is a connectivity issues (no or poor connectivity) from a gateway to a Domain Controller, adjust the priorities.
3. Make sure that Selected Account Units List is selected.
   When this is selected, the Selected AUs list is available. If the list is empty, click Add to add an LDAP Account Unit defined for Microsoft_AD.
4. Select the Microsoft AD server.
   The Servers priorities for selected AU is available.
5. Clear Use default priorities.
6. Select a host of the AD server.
   The Priority field is available.
7. Set the priority of the host with connectivity issues to be lower than a different host.
   For example: Priority 1 is highest. Priority 5 is lower.
8. Click Set.
9. Click OK.

Manual Configuration for Kerberos

If you are working with a directory that is not Microsoft AD, or experiencing problems with automatic configuration, manually configure Kerberos authentication.

To manually configure Kerberos:

2. Populate krb5.manual.conf with values that specify your domain addresses and domain controllers.
   Use this format:
   
   [libdefaults]
   default_realm = YOUR.AD.NAME

   [realms]
   YOUR.AD.NAME = {
   admin_server = your.domain.controller.name
   default_domain = your.dns.domain
   }

   [domain_realm]
   .your.dns.domain = YOUR.AD.NAME
   your.dns.domain = YOUR.AD.NAME

   In the file:

   - YOUR.AD.NAME is the Windows domain name.
   - To configure more than one Windows domain (also known as a “Realm”), add more domains to the [realms] section and to [domain_realm] section.
   - If each realm has more than one domain controller, instead of the admin_server statement use several statements of the type:

   [realms]
   <DOMAIN_NAME> = {
   kdc = <1st domain controller address>
   kdc = <2nd domain controller address>
   }

   Important: If you specify multiple domain addresses (realms) and domain controllers in krb5.manual.conf, you must also add them to the Mobile access configuration in $CVPNDIR/conf/cvpnd.C.
To add them, use these `cvpnd_settings` commands:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd kerberosRealms YOUR.AD.NAME
```

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd kerberosRealms YOUR.OTHER.AD.NAME
```

3. Test the manual configuration:
   a) Set `KRB5_CONFIG` as an environment variable in the shell to point to the relevant configuration file:
      - In the bash shell, run: `export KRB5_CONFIG=$CVPNDIR/var/krb5.manual.conf`
      - For tcsh or csh, run: `setenv KRB5_CONFIG $CVPNDIR/var/krb5.manual.conf`
   b) From the Mobile Access gateway command line, run: `kinit your-ad-username`.
      - If there are several realms, the `kinit` syntax applies to the default realm.
      - For other realms, use the syntax: `kinit your-ad-username@YOUR.OTHER.AD.NAME`

     You should get a prompt similar to: `Password for your-ad-username@YOUR.DOMAIN:`
   c) Enter the password.
   d) Run: `klist`

   The Ticket cache list shows one ticket.
   e) Delete the list by running: `kdestroy`.

4. Open `$CVPNDIR/conf/cvpnd.C` for editing.
5. Change the value of the `kerberosConfigMode` attribute from `auto` to `manual`.
   Alternatively, run: `cvpnd_settings $CVPNDIR/conf/cvpnd.C set kerberosConfigMode manual`
   **Note:** If you assign the value `none` to `kerberosConfigMode`, it disables Kerberos SSO.

**Important:** In a cluster environment, repeat steps 1 to 6 on each cluster member.

### Kerberos Constrained Delegation

Kerberos constrained delegation is a Single Sign-on method that uses Kerberos authentication for users to access internal resources without the need to enter a password. It is supported for the Mobile Access portal and Capsule Workspace.

**To enable Kerberos constrained delegation:**

2. Run `cvpnrestart` on the gateway.
3. In a cluster environment, repeat the steps on all cluster members.

### Configuring Kerberos Constrained Delegation

Before you begin, make sure:

- That your site supports Kerberos authentication.
- The Mobile Access-enabled gateway is configured to support Kerberos. To learn more about this, see the Mobile Access Administration Guide.
- The date and time on the gateway and Active Directory server are the same.
- You use FQDN and not an IP address with your internal server name. Make sure that the FQDN resolves both on the Security Gateway and on the Kerberos server.
The configuration includes:

- Configuring a Delegate User on the AD Server.
- Configuring Kerberos Constrained Delegation support on the Mobile Access gateway.

**Configuring a Delegate User on the AD Server**

A delegate user can have specified permissions without being part of a higher privileged group. For Kerberos Constrained Delegation, the delegate user can allow access to other users for specified services.

To configure a delegate user on the Active Directory (AD) server:

1. Add a new user to the AD server.
2. Open the command prompt on the AD server and run the command:
   ```
   setspn -A HTTP/<user name> <domain name>
   ```
   - `<user name>` - The user name for the user that was created.
   - `<domain name>` - The domain name that the created user belongs to.
3. From the **Users and Computers** tree, right-click the user to open the **User Properties** of the new user.
4. Click the **Delegation** tab.
5. In the **Services to which this account can present delegated credentials** table, click **Add** to add http on the server that the user is allowed to access.
6. Click **OK**.

**Configuring Support on the Mobile Access Gateway**

Kerberos Constrained Delegation is supported with Web Applications and Capsule Workspace Mail applications.

To configure Kerberos Constrained Delegation in SmartDashboard:

1. Make sure that an LDAP Account Unit is defined in SmartDashboard and that the credentials used in it have delegate privileges.
2. In the Mobile Access tab, open the application for which you want to configure Kerberos Constrained Delegation.
3. In **Additional Settings > Single Sign On:**
   - Select **Turn on Single Sign On for this application**.
   - Select **Advanced** and click **Edit**.
4. In the window that opens, select **This application reuses the portal credentials. Users are not prompted**.
5. Click **OK**.
6. Install policy.

**Troubleshooting**

If you have issues with Kerberos Constrained Delegation:

1. Make sure that the value of **EnableKCD** in `$CVPNDIR/conf/cvpnd_internal_settings.c` is **true**.
2. Run **cvpnrestart** on the gateway through SSH and see if there is a **Kerberos Constrained Delegation failure** entry in the Mobile Access logs in SmartView Tracker or SmartLog.
3. Make sure that the account unit credentials have delegate privileges.
4. Make sure that the date and time of the gateway and Active Directory server are synchronized.
5. Make sure that the DNS server is configured correctly and the gateway can resolve the web application host name and the Active Directory server.
Certificate Attribute Forwarding

Certificate attribute forwarding is a Single Sign-on method that transfers details from a user’s certificate to internal servers without the need for a username and password. It forwards the certificate attributes as HTTP headers to the internal servers when a user logs in with a certificate. Users can then log in to other applications automatically with Single Sign-on.

Configuring Certificate Attribute Forwarding

Configure Certificate attribute forwarding in the Mobile Access configuration file:
$CVPNDIR/conf/cvpnd.C

Important! After every change to cvpnd.C, you must restart the cvpn services: cvpnrestart

<table>
<thead>
<tr>
<th>To:</th>
<th>Parameter=value in $CVPNDIR/conf/cvpnd.C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable XX Product XX</td>
<td>:EnableCertHeadersForwarding (true)</td>
</tr>
<tr>
<td>Disable XX Product XX</td>
<td>:EnableCertHeadersForwarding (false)</td>
</tr>
</tbody>
</table>

To configure which attributes of the certificate are forwarded in the HTTP headers:

Add parameters to the CertHeaders section in $CVPNDIR/conf/cvpnd.C.

<table>
<thead>
<tr>
<th>To forward:</th>
<th>Parameter=value in $CVPNDIR/conf/cvpnd.C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete certificate, encoded in base 64</td>
<td>&quot;&lt;header_name&gt; : CERT.BASE64&quot;</td>
</tr>
<tr>
<td>Certificate Issuer DN</td>
<td>&quot;&lt;header_name&gt; : CERT.ISSUER.DN&quot;</td>
</tr>
<tr>
<td>Serial number of the certificate</td>
<td>&quot;&lt;header_name&gt; : CERT.SERIAL&quot;</td>
</tr>
<tr>
<td>Subject DN</td>
<td>&quot;&lt;header_name&gt; : CERT.SUBJECT.DN&quot;</td>
</tr>
<tr>
<td>Alternative subject DN</td>
<td>&quot;&lt;header_name&gt; : CERT.ALTERTIMATESUBJECT.DN&quot;</td>
</tr>
<tr>
<td>Valid start date, before which the certificate cannot be used</td>
<td>&quot;&lt;header_name&gt; : CERT.VALIDITY.NOTBEFORE&quot;</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>&quot;&lt;header_name&gt; : CERT.VALIDITY.NOTAFTER&quot;</td>
</tr>
</tbody>
</table>

Example:

To forward the certificate Issuer DN, edit cvpnd.C for this (where X-Cert-IssuerDN is the header name):

```python
:EnableCertHeadersForwarding (true)
:CertHeaders (  
    : ("X-Cert-IssuerDN : CERT.ISSUER.DN")
)
```
Chapter 6

Native Applications for Client-Based Access

In This Section:

Accessing Native Applications ................................................................. 73
Configuring VPN Clients ............................................................................. 76
Configuring SSL Network Extender Advanced Options ............................. 78
Endpoint Application Types ........................................................................ 79
Configuring a Simple Native Application .................................................... 81
Configuring an Advanced Native Application .............................................. 82
Protection Levels for Native Applications .................................................. 85
Adding Downloaded-from-Gateway Endpoint Applications ......................... 86
Configuring Downloaded-from-Gateway Endpoint Applications .................. 91

A **native application** is any IP-based application that is hosted on servers within the organization, and requires an installed client on the endpoint. The client is used to access the application and encrypt all traffic between the endpoint and Mobile Access.

SSL Network Extender automatically works with Mobile Access as a native application.

Microsoft Exchange, Telnet, and FTP, are all examples of native application servers. Authorized users can use their native clients (for example, telnet.exe, ftp.exe, or Outlook) to access these internal applications from outside the organization.

A native application is defined by the:

- Server hosting applications.
- Services used by applications.
- Connection direction (usually client to server, but can also be server to client, or client to client).
- Applications on the endpoint (client) machines. These applications are launched on demand on the user machine when the user clicks a link in the user portal. They can be:
  - Already installed on the endpoint machine, or
  - Run via a default browser, or
  - Downloaded from Mobile Access.

**Accessing Native Applications**

The SSL Network Extender client makes it possible to access native applications via Mobile Access. SSL Network Extender can operate in two modes: Network Mode and Applications Mode.

**SSL Network Extender**

The SSL Network Extender client lets users access native applications using Mobile Access.

- If the Mobile Access blade is enabled on the gateway, SSL Network Extender works through Mobile Access only. Configure its policy in the **Policy** page of the **Mobile Access** tab.
- If the Mobile Access blade is disabled and the IPsec VPN blade is enabled, SSL Network Extender works through the IPsec VPN blade. Configure its policy in the main security rule base.
**Native Applications for Client-Based Access**

**Note** - If SSL Network Extender was configured through IPsec VPN, and now you enabled the Mobile Access blade on the gateway, you must reconfigure the SSL Network Extender policy in the Mobile Access tab of SmartDashboard. SSL Network Extender rules in the main security rule base are not active if the Mobile Access tab is enabled.

SSL Network Extender is downloaded automatically from the Mobile Access portal to the endpoint machines, so that client software does not have to be pre-installed and configured on users’ PCs and laptops. SSL Network Extender tunnels application traffic using a secure, encrypted and authenticated SSL tunnel to the Mobile Access gateway.

SSL Network Extender requires ActiveX (for Windows with Internet Explorer), or Java. For details see First time Installation of ActiveX and Java Components (on page 15).

**SSL Network Extender Network Mode**

The SSL Network Extender Network Mode client provides secure remote access for all application types (both Native-IP-based and Web-based) in the internal network via SSL tunneling. To install the Network mode client, users must have administrator privileges on the client computer.

After installing the client, an authenticated user can access any authorized internal resource that is defined on Mobile Access as a native application. The user can access the resource by launching the client application, either directly from the desktop or from the Mobile Access portal.

**SSL Network Extender Application Mode**

The SSL Network Extender Application Mode client provides secure remote access for most application types (both Native (IP-based) and Web-based) in the internal network via SSL tunneling. Most TCP applications can be accessed in Application mode. The user does not require administrator privileges on the endpoint machine.

After the client is installed, the user can access any internal resource that is defined on Mobile Access as a native application. The application must be launched from the Mobile Access portal and not from the user’s desktop.

**Note** - UDP based applications are not supported with SSL Network Extender in Application mode.

**Supported Application Mode Applications**

Most TCP applications work with SSL Network Extender in the Application Mode. If an application is defined in the Mobile Access tab in SmartDashboard as one that can be used in Application Mode, a user that connects in Application Mode will be able to see it and launch it. If the application is not supported in Application Mode, a user who connects with Application Mode will not see it in the list of applications.

The following applications have been tested and are Check Point OPSEC-certified for use with Mobile Access SSL Network Extender in Application mode. Note that this mode is different from SSL Network Extender in Network mode which supports any IP-based application. While Application Mode is designed to work with most applications, only OPSEC-certified applications have been tested and verified to work with SSL Network Extender in Application mode. Only specified versions are guaranteed to work and are fully supported. However, in most cases other versions of the same client and most other applications that are TCP based will work.

**SSL Network Extender - Application Mode Support**

<table>
<thead>
<tr>
<th>Partner/ Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet / SSH</td>
<td>Microsoft Telnet (Command Line)</td>
<td>2000 XP</td>
</tr>
<tr>
<td>Microsoft</td>
<td>HyperTerminal</td>
<td>5.1</td>
</tr>
</tbody>
</table>

Mobile Access Administration Guide R77 Versions  | 74
## Native Applications for Client-Based Access

### Database Clients

<table>
<thead>
<tr>
<th>Partner/Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Putty</td>
<td>Putty</td>
<td>0.55</td>
</tr>
<tr>
<td>VanDyke</td>
<td>SecureCRT</td>
<td>4.1</td>
</tr>
</tbody>
</table>

### TN3270

<table>
<thead>
<tr>
<th>Partner/Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ericom</td>
<td>PowerTerm InterConnect for Windows</td>
<td>6.6.2</td>
</tr>
<tr>
<td>IBM</td>
<td>Personal Communications Workstation Program</td>
<td>5.8</td>
</tr>
</tbody>
</table>

### FTP

<table>
<thead>
<tr>
<th>Partner/Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>FTP (Command Line)</td>
<td>2000 XP</td>
</tr>
<tr>
<td>Ipswitch</td>
<td>WS_FTP Home/PRO</td>
<td>9.1.0.429</td>
</tr>
<tr>
<td>GlobalSCAPE</td>
<td>CuteFTP</td>
<td>4.2 7</td>
</tr>
</tbody>
</table>

### E-Mail (POP3, IMAP, SMTP)

<table>
<thead>
<tr>
<th>Partner/Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Outlook Express</td>
<td>6</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Outlook (See note below table)</td>
<td>2000 SP1 XP</td>
</tr>
<tr>
<td>QUALCOMM</td>
<td>Eudora</td>
<td>6.2</td>
</tr>
<tr>
<td>Mozilla</td>
<td>Thunderbird</td>
<td>1.0.2</td>
</tr>
<tr>
<td>IBM</td>
<td>Lotus Notes</td>
<td>6.0.3 6.5.3</td>
</tr>
</tbody>
</table>

### Web Browser (HTTP, HTTPS, Passive FTP)

<table>
<thead>
<tr>
<th>Partner/Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Internet Explorer</td>
<td>5.5 and up</td>
</tr>
<tr>
<td>Mozilla</td>
<td>Mozilla Firefox</td>
<td>1.0.3 1.0.4</td>
</tr>
</tbody>
</table>

### Terminal Services

<table>
<thead>
<tr>
<th>Partner/Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Remote Desktop Connection</td>
<td>XP 2000</td>
</tr>
</tbody>
</table>
### Native Applications for Client-Based Access

<table>
<thead>
<tr>
<th>Partner/ Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealVNC</td>
<td>VNC Viewer</td>
<td>4.1.1</td>
</tr>
<tr>
<td>Famatech</td>
<td>Remote Administrator</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td>Citrix</td>
<td>Program Neighborhood</td>
<td>6.20.985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9.0.0.32649</td>
</tr>
<tr>
<td>Citrix</td>
<td>Java Connection Center</td>
<td>8.0.1672</td>
</tr>
<tr>
<td>Citrix</td>
<td>JICA</td>
<td>8.2.1684</td>
</tr>
<tr>
<td>Citrix</td>
<td>ActiveX</td>
<td>8.0.24737.0</td>
</tr>
<tr>
<td>Productivity Suites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td>Lotus Notes</td>
<td>6.0.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.5.3</td>
</tr>
</tbody>
</table>

**Note** - Some Anti-Virus applications do not scan email when Microsoft Outlook is launched with SSL Network Extender Application mode, because the mail is encrypted in SSL before scanning begins.

### Configuring VPN Clients

**To configure SSL Network Extender on VPN clients:**

1. Open **Gateway Properties > Mobile Access > SSL Clients**.
   - SSL Network Extender is automatically enabled when the Mobile Access blade is turned on.
2. Select an option:
   - **Automatically decide on client type according to endpoint machine capabilities** downloads the SSL Network Extender Network Mode client if the user on the endpoint machine has administrator permissions, and downloads the Application Mode client if the user does not have administrator permissions.
   - **Application Mode only** specifies that the SSL Network Extender Application Mode client is downloaded to the endpoint machines — irrespective of the capabilities of the endpoint machine.
   - **Network Mode only** specifies that the SSL Network Extender Network Mode client is downloaded to the endpoint machines — irrespective of the capabilities of the endpoint machine. The user on the endpoint machine must have administrator permissions in order to access Native Applications.

If you had SSL Network Extender configured through IPsec VPN and now you enabled the Mobile Access blade on the gateway, you must reconfigure the SSL Network Extender policy in the Mobile Access tab of SmartDashboard. Rules regarding SSL Network Extender in the main security rule base are not active if the Mobile Access tab is enabled.

### Office Mode

When working with **Office Mode**, Remote Access clients receive an IP address allocated for them by the VPN administrator. These addresses are used by the clients in the source field of the IP packets they build. Since the IP packets are then encrypted and encapsulated, the packets appear to the Internet with their
original IP address. To the organization's internal network, after decapsulation and decryption, they appear with the allocated IP address. The clients seem to be on the internal network.

For more about Office Mode, see the R77 VPN Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=24849).

**Configuring Office Mode**

Configure Office Mode in **Gateway Properties > Mobile Access > Office Mode**. The settings configured here apply to Mobile Access clients and IPsec VPN clients.

**Office Mode Method**

Choose the methods used to allocate IP addresses for Office Mode. All of the methods selected below will be tried sequentially until the office mode IP addresses are allocated.

- **From ipassignment.conf in \FWDIR\conf** - You can over-ride the Office Mode settings created on Security Management server by editing a plain text file called *ipassignment.conf* in the \FWDIR\conf directory of the Check Point Security Gateway. The gateway uses these Office Mode settings and not those defined for the object in Security Management server.

  *ipassignment.conf* can specify:
  - An IP per user/group, so that a particular user or user group always receives the same Office Mode address. This allows the administrator to assign specific addresses to users, or particular IP ranges/networks to groups when they connect using Office Mode.
  - A different WINS server for a particular user or group
  - A different DNS server
  - Different DNS domain suffixes for each entry in the file.

- **From the RADIUS server used to authenticate the user** - A RADIUS server can be used for authenticating remote users. When a remote user connects to a gateway, the user name and password are passed on to the RADIUS server, which checks that the information is correct, and authenticates the user. The RADIUS server can also be configured to allocate IP addresses.

- **Using one of the following methods:**
  - **Manually (IP pool)** - Create a Network Object with the relevant addresses. The allocated addresses can be illegal but they have to be routable within the internal network.
  - **Automatically (Using DHCP)** - Specify the machine on which the DHCP server is installed. In addition, specify the virtual IP address to which the DHCP server replies. The DHCP server allocates addresses from the appropriate address range and relates to VPN as a DHCP relay agent. The virtual IP address must be routable to enable the DHCP send replies correctly. DHCP allocates IP addresses per MAC address. When VPN needs an Office Mode address, it creates a MAC address that represents the client and uses it in the address request. The MAC address can be unique per machine or per user. If it is unique per machine, then VPN ignores the user identity. If different users work from the same Remote Access client they are allocated the same IP address.

**Multiple Interfaces**

If the gateway has multiple external interfaces, there might be a routing problem for packets whose destination address is a client working in Office Mode. The destination IP address is replaced when the packet is encapsulated and thus previous routing information becomes irrelevant. Resolve this problem by setting the gateway to **Support connectivity enhancement for gateways with multiple external interfaces**. Do not select this option if your gateway has only one external interface, as this operation affects the performance.

**Anti-Spoofing**

If this option is selected, VPN verifies that packets whose encapsulated IP address is an Office Mode IP address are indeed coming from an address of a client working in Office Mode.

If the addresses are allocated by a DHCP server, VPN must know the range of allocated addresses from the DHCP scope for the Anti-Spoofing feature to work. Define a Network object that represents the DHCP scope and select it here.
**IP Pool Optional Parameters**

Configure additional optional parameters for how office mode addresses are assigned by clicking Optional Parameters. If the office mode addresses are allocated from an IP pool, this window allows you to specify the DNS and WINS addresses by selecting the appropriate Network Objects. In addition, specify the backup DNS and WINS servers and supply the Domain name.

If the office mode addresses are allocated by a DHCP server, DNS and WINS addresses are set on the DHCP server.

These details are transferred to the Remote Access client when a VPN is established.

**IP Lease Duration**

Specify the amount of time after which the Remote Access client stops using the allocated IP address and disconnects. By default, the duration is 15 minutes. The client tries to renew the IP address by requesting the same address after half of the set time has elapsed. When this request is granted, the client receives the same address until the lease expires. When the new lease expires, it must be renewed again.

**Configuring SSL Network Extender Advanced Options**

For advanced SSL Network Extender configuration options, in the SmartDashboard Mobile Access tab, select the Additional Settings > VPN Clients > Advanced Settings for SSL Network Extender page, and click Edit.

**Deployment Options**

- **Client upgrade upon connection** specifies how to deploy a new version of the SSL Network Extender Network Mode client on endpoint machines, when it becomes available.
  - **Note** - Upgrading requires Administrator privileges on the endpoint machine.

- **Client uninstall upon disconnection** specifies how to handle the installed SSL Network Extender Network Mode client on the endpoint machine when the client disconnects.
  - **Do not uninstall** allows the user to manually uninstall if they wish to.
  - **Ask User** allows the user to choose whether or not to uninstall.
  - **Always uninstall** does so automatically, when the user disconnects.

**Encryption**

- **Supported Encryption methods** defines the strength of the encryption used for communication between SSL Network Extender clients and all Mobile Access gateways and gateway clusters that are managed by the Security Management Server.
  - **3DES only**. This is the default. The 3DES encryption algorithm encrypts data three times, for an overall key length of 192 bits.
  - **3DES or RC4** to configure the SSL Network Extender client to support the RC4 encryption method, as well as 3DES. RC4 is a variable key-size stream cipher. The algorithm is based on the use of a random permutation. It requires a secure exchange of a shared key that is outside the specification. RC4 is a faster encryption method than 3DES.

**Launch SSL Network Extender Client**

These settings define the behavior of the SSL Network Extender clients when launched on the endpoint machines.

- **On demand, when user clicks 'Connect' on the portal** - SSL Network Extender only opens when the user clicks "Connect" from the Mobile Access portal.

- **Automatically, when user logs on** - When users log in to the Mobile Access portal, SSL Network Extender launches automatically.
• **Automatically minimize client window after client connects** - For either of the options above, choose to minimize the SSL Network Extender window to the system tray on the taskbar after connecting. This provides better usability for non-technical users.

## Endpoint Application Types

When defining a Native Application, you can define applications on endpoint machines. These applications launch on the endpoint machine when the user clicks a link in the Mobile Access portal. You do not have to configure endpoint applications for users using SSL Network Extender in Network Mode, as they will be able to access them using their native clients.

### Application Installed on Endpoint Machine

These endpoint applications are already installed on the endpoint machines.

### Application Runs Via a Default Browser

Run via default browser is used to define a link to any URL. The link appears in the Mobile Access portal, and launches the current Web browser (the same browser as the Mobile Access portal). The link can include $$user, which represents the user name of the currently logged-in user.

This option has a user experience similar to a Web Application with a URL: The application is opened in a Web browser. However, Mobile Access Web applications perform Link Translation on the URL and encrypt the connection over SSL, while the "Run via default browser" option with SSL Network Extender does not perform link translation, and encrypts using SSL Network Extender. You may prefer to define a Native Application rather than a Web Application for convenience, or because some websites have problems working with Link Translation.

### Applications Downloaded-from-Gateway

Downloaded-from-Gateway applications allow you to select a client application located on the Mobile Access gateway, that is downloaded from Mobile Access to the endpoint machine when the user clicks a link in the Mobile Access portal.

These applications allow end users to securely use client-server applications, without requiring a native client to be installed on their machines.

Two kinds of Downloaded-from-Gateway applications are available by default: **Certified Applications** and **Add-on Applications**. Certified applications are an integral part of Mobile Access, and are fully supported. Add-on Downloaded-from-Gateway applications are third-party applications, which are supplied as-is, and for which Check Point provides limited support.

Mobile Access provides eight built-in applications that the administrator can configure. Downloaded-from-Gateway applications are either Java-based applications or single-executable applications (including batch files). All the applications that are available by default, other than the Terminal (PuTTY) client, are Java based applications, and are therefore multi-platforms applications. The PuTTY client can only be used on Windows machines.

It is possible to add Downloaded-from-Gateway applications to Mobile Access, in addition to the built-in applications. See Adding Downloaded-from-Gateway Endpoint Applications (on page 86).

### Certified Applications

Certified applications are an integral part of Mobile Access, and are fully supported. The packages that are downloaded to the endpoint machine are signed by Check Point. The following table lists the available certified Downloaded-from-Gateway Native Applications:
Native Applications for Client-Based Access

**Downloaded-from-Gateway Certified Applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>Telnet terminal. Provides user oriented command line login sessions between hosts on the Internet.</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell (SSH) is designed for logging into and executing commands on a networked computer. It provides secure encrypted communications between two hosts over an insecure network. An SSH server, by default, listens on the standard TCP port 22.</td>
</tr>
<tr>
<td>TN3270</td>
<td>IBM 3270 terminal emulator tailored to writing screen-scraping applications. TN3270 is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminal.</td>
</tr>
<tr>
<td>TN5250</td>
<td>IBM 5250 terminal emulator that interprets and displays 5250 data streams.</td>
</tr>
</tbody>
</table>

For configuration details, see Configuring Downloaded-from-Gateway Endpoint Applications (on page 91).

**Add-on Applications**

Add-on Downloaded-from-Gateway applications are third-party applications, which are supplied as-is, for which Check Point provides limited support.

These packages are not signed by Check Point, and when they are downloaded by end-users a popup warning informs the user that the package is not signed. If the application does not function as expected, it can be deleted or replaced. The following table lists the available Downloaded-from-Gateway Native Applications:

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Desktop (RDP)</td>
<td>Downloaded-from-Gateway Client for Windows NT Terminal Server and Windows 2000/2003 Terminal Services. Communicates using Remote Desktop Protocol (RDP) in order to present the user’s NT desktop. Unlike Citrix ICA, no server extensions are required. Runs on Java 1.1 up (optimized for 1.4), and works on Linux, Windows and Mac.</td>
</tr>
<tr>
<td>Terminal (PuTTY)</td>
<td>An implementation of Telnet and SSH for Win32 platforms, including an Xterm terminal emulator.</td>
</tr>
<tr>
<td>Jabber</td>
<td>Downloaded-from-Gateway Jabber Client is an instant messenger based on the Jabber protocol. Runs on every computer with at least Java 1.4.</td>
</tr>
<tr>
<td>FTP</td>
<td>Graphical Java network and file transfer client. Supports FTP using its own FTP API and various other protocols like SMB, SFTP, NFS, HTTP, and file I/O using third party APIs, includes many advanced features such as recursive directory up/download, browsing FTP servers while transferring files, FTP resuming and queuing, browsing the LAN for Windows shares, and more.</td>
</tr>
</tbody>
</table>

For configuration details, see Configuring Downloaded-from-Gateway Endpoint Applications (on page 91).

**Configuring Authorized Locations per User Group**

The authorized locations (hosts or address ranges) of a Native application are defined in the *Authorized Locations* page of the Native Application. However, it is also possible to configure authorized locations per user group. Users who belong to two or more groups can access the union of the authorized locations of the groups.

For configuration details, see sk32111 (http://supportcontent.checkpoint.com/solutions?id=sk32111).
Ensuring the Link Appears in the End-User Browser

If an endpoint application is defined by the administrator, but is not available on the endpoint machine, the link to the application will not be shown in the Mobile Access portal.

For example, the link will not be shown if:

- An endpoint application that is pre-installed on the endpoint machine (of type "Already Installed") is configured, and the application is in fact not installed on the endpoint machine.
- A Downloaded-from-Gateway (Embedded) application requires Java, but Java is not installed on the endpoint machine.

Configuring a Simple Native Application

To configure a simple Native Application:

1. In the Mobile Access tab navigation tree, select Applications > Native Application.
2. Click New. The Native Application window opens. The following sections explain the fields in each page.

General Properties

In the General Properties page, define the name of the Native Application.

Authorized Locations

1. Go to the Authorized Locations page.
   An authorized location ensures users of the Native Application can only access the specified locations using the specified services.
2. Fill in the fields:
   - Host or Address Range is the machine or address range on which the application is hosted.
   - Service is the port on which the machine hosting the application listens for communication from application clients.

Applications on the Endpoint Computer

1. Go to the Endpoint Applications page.
2. Fill in the fields:
   - Add link in the Mobile Access portal must be selected if you want to make endpoint application(s) associated with the Native Applications available to users.
   - Link text can include $$user, a variable that represents the user name of the currently logged-in user.
   - Tooltip for additional information. Can include $$user, which represents the user name of the currently logged-in user.
   - Path and executable name must specify one of the following:

     Note - If the endpoint application is not available on the endpoint machine, the link to the application will not be shown in the end user's browser.

     - Full path of the application on the endpoint machines. For example, c:\WINDOWS\system32\ftp.exe
     - The location of the application by means of an environment variable. This allows the location of the application to be specified in a more generalized way. For example %windir%\system32\ftp.exe
     - If the application is listed in the Windows Start > Programs menu, only the application name need be entered, as it appears to the user in the Start menu. For example HyperTerminal.
Native Applications for Client-Based Access

- If the location of the application is in the path of the endpoint computer, only the application name need be entered. For example `ftp.exe`
- **Parameters** are used to pass additional information to applications on the endpoint computer, and to configure the way they are launched.

Using the $$user Variable in Native Applications

You can use the $$user variable to define customized login parameters for native applications. To do this, enter the $$user variable wherever you need to specify a user name.

For example, you can use the $$user variable to return the user name as a part of the login string for Remote Desktop. In this example, $$user.example.com (in the Parameters field) resolves to the login string `ethan.example.com` for Ethan or `richard.example.com` for Richard.

Completing the Native Application Configuration

If necessary, configure VPN clients. See Configuring VPN Clients (on page 76).

After doing so:
2. In the Policy page, associate:
   - **User groups**.
   - **Applications** that the users in those user groups are allowed to access.
   - **Install On** the Mobile Access gateways and gateway clusters that users in those user groups are allowed to connect to.
3. From the SmartDashboard main menu, choose Policy > Install and install the policy on the Mobile Access gateways.

Configuring an Advanced Native Application

To configure an advanced Native Application:
1. In the Mobile Access tab navigation tree, select Applications > Native Application.
2. Click New. The Native Application window opens. The following sections how to define advanced Native Application features.

Configuring Connection Direction

1. In the General Properties page of the Native Application object, click Connection direction. An Advanced window opens.
2. Select an option for the Direction of communication from the connection initiator:
   - **Client to server**: (For example, Telnet.) This is the default option. When you create a client to server application and assign it to a user group, you enable users of the group to initiate a connection to the specified server.
   - **Server to client**: (For example, X11.) When you create a server to client application, the specified server can initiate a connection to all SSL Network Extender or Secure Client Mobile users currently logged on to the Mobile Access gateway, regardless of their group association.
   - **Client to client**: (For example, running Remote Administration from one client to another.) When you create a client to client Native Application and assign it to a user group, you enable users of that group to initiate a connection to all of the SSL Network Extender or Secure Client Mobile users currently logged on to Mobile Access, regardless of their user group association.

   **Note** - A Client to Client Native Application does not require configuration of a destination address.
Multiple Hosts and Services

The native application can reside on a range of hosts, which can be accessed by the native application clients. You can also specify more than one service that clients may use to communicate with the application.

Users of the native application can only access the specified locations using the specified services.

To define a native application with multiple hosts and services:
1. Define a Native Application.
2. In the Authorized Locations page of the Native Application object, select Advanced: Edit.
   The Native Application - Advanced window opens.
3. Click Add or Edit.
   The Native Application Hosts window opens.

Configuring the Endpoint Application to Run Via a Default Browser

To configure the Endpoint Application to run via a default browser:
1. Define a Native Application.
2. In the Endpoint Applications page of the Native Application object, select Add link in the Mobile Access portal.
4. Click Add. The Edit Endpoint Application window opens.
5. Select Run via default browser. This is used to define a link to any URL. The link appears in the Mobile Access portal, and launches the current Web browser (the same browser as the Mobile Access portal). The link can include $$user, which represents the user name of the currently logged-in user.

This option has a similar user experience to a Web Application with a URL: The application is opened in a Web browser. However, Mobile Access Web applications perform Link Translation on the URL and encrypt the connection over SSL, while the “Run via default browser” option with SSL Network Extender does not perform link translation, and encrypts using SSL Network Extender. You may prefer to define a Native Application rather than a Web Application for convenience, or because some Web sites have problems working with Link Translation.

Automatically Starting the Application

To configure the Endpoint Application to start automatically:
1. Define a Native Application.
2. In the Endpoint Applications page of the Native Application object, select Add link in the Mobile Access portal.
4. Click Add or Edit. The Edit Endpoint Application window opens.
5. Click Advanced.
   The Advanced window opens.
   • Automatically Start this Application - Configure a Native Application to run a program or command automatically, after connecting to or disconnecting from SSL Network Extender (either Network mode or Application mode). When more than one Native Application is defined for automatic connection or disconnection, the applications run in the alphabetical order of the names of the Native Applications.
   • When SSL Network Extender is disconnected - Do not use this option to launch applications that require connectivity to the organization - SSL Network Extender Application Mode. In Network Mode, automatic start of applications when SSL Network Extender is disconnected, works correctly.
Native Applications for Client-Based Access

Making an Application Available in Application Mode

To make an application available in Application Mode:

1. Define a Native Application.
2. In the Endpoint Applications page of the Native Application object, select Add link in the Mobile Access portal.
4. Click Add or Edit. The Edit Endpoint Application window opens.
5. Click Advanced. The Advanced window opens.
6. Select Show link to this application in SSL Network Extender Application Mode. The option SSL Network Extender application mode compatibility lets you make an application available to Application Mode clients. Users that connect using the SSL Network Extender Application Mode client are able to see a link to the application and launch it. Use this option if the application works well in Application Mode.

Note - If this option is NOT selected:
- Users who connect with Application Mode, do not see it in their list of applications.
- Users with SecureClient Mobile on handheld devices, are unable to connect to the application.

Automatically Running Commands or Scripts

It is possible to configure a Native Application to run a program or command automatically, after connecting to or disconnecting from SSL Network Extender (either Network mode or Application mode).

Note - The user must have the appropriate privileges on the endpoint machine to run the commands.

One example of how automatically running a command can be useful is to mount or unmount a network drive. Giving users access to network drives is a convenient way of providing access to internal resources. A drive can be mapped by configuring an application that invokes the Windows net use command.

Note - When more than one Native Application is defined for automatic connection or disconnection, the applications run in the alphabetical order of the names of the Native Applications.

For configuration details, see How to Automatically Map and Unmap a Network Drive (on page 84).

It is possible to extend this ability by defining a dynamic add-on Downloaded-from-Gateway application that runs a script (batch file) containing a sequence of commands to execute on the endpoint machine. This script can be launched manually when the user clicks a link, or it can launch automatically after connecting to or disconnecting from SSL Network Extender.

For configuration details, see How to Automatically Run a Script (Batch File) (on page 85).

How to Automatically Map and Unmap a Network Drive

A drive can be mapped by configuring an application that invokes the Windows net use command.

Note - The net use command is available for SSL Network Mode only.

To automatically map (mount) and unmap (unmount) a network drive, create a Native Application that automatically maps the network drive when SSL Network Extender is launched:

1. Define a Native Application.
2. In the Endpoint Applications page of the Native Application object, select Add link in the Mobile Access portal.
4. Click Add or Edit. The Edit Endpoint Application window opens.
5. Configure the **Edit Endpoint Application** page as follows:
   - **Already installed.**
   - **Path and executable name:** net.exe
   - **Parameters:** use drive_letter: \server name\share name

6. Click **Advanced**. In the **Advanced** page, check **When SSL Network Extender is launched**.

7. Create another Native Application that automatically unmaps the network drive when SSL Network Extender is disconnected. Configure the **Edit Endpoint Application** page as follows:
   - **Already installed.**
   - **Path and executable name:** net.exe
   - **Parameters:** use /DELETE drive_letter:

8. Click **Advanced**. In the **Advanced** page, check **When SSL Network Extender is disconnected**.

### How to Automatically Run a Script (Batch File)

It is possible to define a new Downloaded-from-Gateway Endpoint Application (embedded application) that runs a script (batch file) automatically after connecting to or disconnecting from SSL Network Extender.

Proceed as follows:

1. Create a batch (script) file containing a sequence of commands.
2. Define the batch file as a new Downloaded-from-Gateway Endpoint Application (Embedded Application) (see "Adding Downloaded-from-Gateway Endpoint Applications" on page 86).
3. Define a Native Application.
4. In the **Endpoint Applications** page of the Native Application object, select **Add link in the Mobile Access portal**.
5. Select **Advanced > Edit**. The **Endpoint Applications - Advanced** window opens.
6. Click **Add** or **Edit**. The **Edit Endpoint Application** window opens.
7. Click **Advanced**.
8. In the **Automatically start this application** section of the **Advanced** page, select **When SSL Network Extender is launched**.

### Protection Levels for Native Applications

On Mobile Access gateways of version R71 and higher, protection levels can be set individually for each native application.

Protection Levels are predefined sets of security settings that offer a balance between connectivity and security. Protection Levels allow Mobile Access administrators to define application protections for groups of applications with similar requirements.

Mobile Access comes with three default Protection Levels — Normal, Restrictive, and Permissive. You can create additional Protection Levels and change the protections for existing Protection Levels.

**Protection Levels in Older Gateways:**

For Mobile Access gateways of versions before R71, one Protection Level can be set for all native applications, or all native applications can rely on the security requirements of the Mobile Access gateway. These settings are configured on the main **Native Applications** page.

**Protection Levels in R71 and Higher Gateways:**

For Mobile Access gateways of versions R71 and higher, Protection Level settings are configured in the Properties window of each native application by selecting **Additional Settings > Protection Level**.

**Note** - The Protection Level settings in Mobile Access gateways of versions R71 and higher cannot be set globally on the main **Native Applications** page.
When defining an application, in the Protection Level page of the application object, you can choose:

- **This application relies on the security requirements of the gateway**
  Rely on the gateway security requirement. Users authorized to use the portal are also authorized to use this application. This is the default option.

- **This application has additional security requirements specific to the following protection level**
  Associate the Protection Level with the application. Users are required to be compliant with the security requirement for this application in addition to the requirements of the portal.

### Defining Protection Levels

**To access the Protection Level page from the Mobile Access tab:**

1. From the Mobile Access tab in SmartDashboard, select the Additional Settings > Protection Levels page from the navigation tree.
2. Click **New** to create a new Protection Level or double-click an existing Protection Level to modify it. The Protection Levels window opens, displaying the General Properties page.

**To access the Protection Level page from a Mobile Access application:**

1. From the Properties window of a Mobile Access application, select Additional Setting > Protection Level.
2. To create a new Protection Level, select Manage > New.
3. To edit the settings of a Protection Level, select the Protection Level from the drop down list and then select Manage > Details.
   The Protection Levels window opens, displaying the General Properties page.

**To define a Protection Level:**

1. In the General Properties page, enter a unique name for the Protection Level (for a new Protection Level only), select a display color and optionally add a comment in the appropriate fields.
2. Click on Authentication in the navigation tree and select one or more authentication methods from the available choices. Users accessing an application with this Protection Level must use one of the selected authentication schemes.
3. If required, select User must successfully authenticate via SMS.
4. Click Endpoint Security in the navigation tree and select one or both of the following options:
   - Applications using this Protection Level can only be accessed if the endpoint machine complies with the following Endpoint compliance policy. Also, select a policy. This option allows access to the associated application only if the scanned client computer complies with the selected policy.
   - Applications using this Protection Level can only be accesses from within Secure Workspace. This option requires Secure Workspace to be running on the client computer.
5. Click OK to close the Protection Level window
6. Install the Security Policy.

### Adding Downloaded-from-Gateway Endpoint Applications

You can add Downloaded-from-Gateway applications to Mobile Access, in addition to the eight built-in applications. This section explains how, and gives two detailed examples.

**Downloaded-from-Gateway Application Requirements**

Downloaded-from-Gateway applications are either Java-based applications or single-executable applications (including batch files).

Java applications have the following requirements:

- Application must be packaged into a JAR file
- The JVM of a version required by the application must be installed on the endpoint machine.
- The application must have a Main class.

Single-executable applications have the following requirements:
- Must not require installation.
- Must be platform-specific for Windows, Linux or MAC OS.

**Adding a New Application**

To add a new Downloaded-from-Gateway application, first put the application in the relevant directory on the gateway. Then use the Database Tool (GuiDBedit) to set its properties.

**To add a new downloaded-from-gateway endpoint application:**

1. Compress your downloaded-from-gateway application file into CAB file with the same name as the original file but with a .cab extension.
   
   To compress a file into a CAB file, you can use the Microsoft Cabinet Tool `cabarc.exe` (which can be downloaded from the Microsoft Web site). For example:
   ```
   cabarc.exe -m LZX:20 -s 6144 N ssh2.cab ssh2.jar
   ```

2. Copy both your downloaded-from-gateway application file and the .cab file you created to the gateway machine at: `$CPVNDIR/htdocs/SNX/CSHELL`

3. Change the application file permissions to read, write and execute.

4. Run the Check Point Database Tool GuiDBedit.exe from the directory where SmartConsole is installed (in the same installation directory as SmartDashboard).


6. Select **Table > Other > embedded_applications**. The `embedded_applications` table shows.

7. In the right side pane, right-click and select **New**.

8. In the **Object** field, enter a name for the new downloaded-from-gateway application.

9. Specify the characteristics of the new downloaded-from-gateway application.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>display_name</td>
<td>The application name, which will appear in the drop-down list of downloaded-from-gateway applications in SmartDashboard, in the <strong>Edit Endpoint Application</strong> window.</td>
</tr>
<tr>
<td>embedded_application_type</td>
<td>The type of downloaded-from-gateway application. Choose one of the options in the <strong>Valid Values</strong> list (java_applet, linux_executable, mac_executable, windows_executable).</td>
</tr>
<tr>
<td>file_name</td>
<td>The name of the file you placed in <code>$CPVNDIR/htdocs/SNX/CSHELL</code> (not the .cab version).</td>
</tr>
<tr>
<td>server_name_required_params</td>
<td>Indicate if the new downloaded-from-gateway application requires the server name to be configured in the Parameters field of the new downloaded-from-gateway application, in the SmartDashboard <strong>Edit Endpoint Application</strong> window.</td>
</tr>
<tr>
<td>pre_custom_params</td>
<td>Parameters concatenated before the <code>server_name_required_params</code> field. Usually used when configuring a new downloaded-from-gateway Java application. In that case, specify the Main Class name of the application.</td>
</tr>
<tr>
<td>post_custom_params</td>
<td>Parameters concatenated after the <code>server_name_required_params</code> field. Can be left blank.</td>
</tr>
<tr>
<td>type</td>
<td>Leave as <code>embedded_application</code>.</td>
</tr>
</tbody>
</table>
You will now be able to see and configure the new downloaded-from-gateway application in SmartDashboard, just as you do with the built-in downloaded-from-gateway applications. The downloaded-from-gateway applications appear in the Edit Network Application page of the Native Application object (Getting there: Native Application object > Endpoint applications page > Advanced: Edit > Add/Edit).

**Example: Adding a New SSH Application**

This example adds two applications to Mobile Access as new downloaded-from-Mobile Access applications:

1. **SSH2 Java application:**
   - Jar file name: ssh2.jar
   - Main class name: ssh2.Main
   - The application gets its server name as a parameter.
   - Name in SmartDashboard: Jssh2 Client.

2. **SSH2 Windows executable:**
   - Executable file name: WinSsh2.exe
   - The application gets its server name as parameter.
   - Name in SmartDashboard: Essh2 Client.

**To add these applications:**

1. Compress the ssh2.jar and WinSsh2.exe application files into ssh2.cab and WinSsh2.cab:
   ```
   # cabarc.exe -m LZX:20 -s 6144 N ssh2.cab ssh2.jar
   # cabarc.exe -m LZX:20 -s 6144 N WinSsh2.cab WinSsh2.exe
   ```

2. Assuming the IP address of the SSH2 server is 1.1.1.1, save the files ssh2.jar and WinSsh2.exe to $CVPNDIR/htdocs/SNX/CSHELL with the proper permissions.
3. Put the application files in $CVPNDIR/htdocs/SNX/CSHELL with the proper permissions.
4. Use GuiDBedit to configure the two new downloaded-from-Mobile Access applications.

**SSH2 Java Application**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>display_name</td>
<td>Jssh2 Client</td>
</tr>
<tr>
<td>embedded_application_type</td>
<td>java_applet</td>
</tr>
<tr>
<td>file_name</td>
<td>ssh2.jar</td>
</tr>
<tr>
<td>post_custom_params</td>
<td>Empty</td>
</tr>
<tr>
<td>pre_custom_params</td>
<td>ssh2.Main</td>
</tr>
<tr>
<td>server_name_required_params</td>
<td>true</td>
</tr>
<tr>
<td>type</td>
<td>embedded_application</td>
</tr>
</tbody>
</table>

**SSH2 Windows Executable**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>display_name</td>
<td>Essh2 Client</td>
</tr>
<tr>
<td>embedded_application_type</td>
<td>windows_executable</td>
</tr>
</tbody>
</table>
Native Applications for Client-Based Access

Field Name | Value
---|---
file_name | WinSsh2.exe
post_custom_params | Empty
pre_custom_params | Empty
server_name_required_params | true
type | embedded_application

When you configure one of these new downloaded-from-Mobile Access applications *(Jssh2 Client and Essh2 Client)* in SmartDashboard, the Parameters field will be: 1.1.1.1 (the SSH2 server IP in this example).

**Example: Adding a New Microsoft Remote Desktop Profile**

This example demonstrates how to configure Mobile Access to work with Microsoft Remote Desktop, with a predefined profile. It also shows how to configure the profile per user group.

1. Create the Remote Desktop Profile (on page 89)
2. Create a CAB Package from the Profile (on page 90)
3. Configure the Package Downloaded-from-Gateway Application (on page 90)
4. Configure the Link to the Remote Desktop Application (on page 90)
5. Configure the Remote Desktop Profile to Start Automatically (on page 91)
6. Assign the Native Application to the User Group (on page 91)

Repeat for every new Microsoft Remote Desktop Connection.

**Create the Remote Desktop Profile**

Create the RDP profile file (with an .rdp extension) using Microsoft Remote Desktop Connection, found at %SystemRoot%\system32\mstsc.exe.

When creating the profile, you can define the address, the settings, applications that should run at log in, and more.

In this example, the profile file has the name of the relevant user group. For a user group called mygr1, save a profile file called mygr1.rdp.
Create a CAB Package from the Profile

1. Compress the profile file into CAB file with the same name as the original file. The Microsoft Cabinet Tool Cabarc.exe can be used. It is available at http://msdn2.microsoft.com/en-us/library/aa751974.aspx.

For this example, run the command:
cabarc.exe -m LZX:20 -s 6144 N mygr1.cab mygr1.rdp
This produces the output file mygr1.cab.

2. Copy both mygr1.rdp and mygr1.cab to the Mobile Access machine at $CVPNDIR/htdocs/SNX/CSHELL.

3. Change their permissions to read, write and execute.

Configure the Package Downloaded-from-Gateway Application

1. Run the Database Tool GuiDBedit.exe from the directory where SmartConsole is installed. The default location is:
C:\Program Files\CheckPoint\SmartConsole\R71\PROGRAM.

2. Enter the administrator user name and password.

3. Select Table > Other > embedded_applications.
   The embedded_applications table opens.

4. In the right side pane, right-click and select New.

5. In the Object field, enter a name for the new downloaded-from-gateway application. Give it the name of the relevant user group. In this example: mygr1

6. Specify the characteristics of the new downloaded-from-gateway application as follows:
   - display_name: mygr1_RDP_Policy
   - embedded_application_type: windows_executable
   - file_name: mygr1.rdp

You can now see and configure the new downloaded-from-gateway application in SmartDashboard, just as for the built-in downloaded-from-gateway applications.

Configure the Link to the Remote Desktop Application

Configure the link to Microsoft Remote Desktop that will appear in the SSL Network Extender window. Define it as an Already Installed endpoint application.
Define a Native Application.

2. In the Endpoint Application page of the Native Application, select Add a Link to the application in the Mobile Access portal.

3. Select Advanced, and click Edit.

   The Endpoint Applications - Advanced window opens.

4. Click Add. The Edit Endpoint Application window opens.

5. In the Edit Endpoint Application window, use the following settings, as shown in the screen capture:
   - Link text (Multi-language): MS-RDP (or any other name).
   - Path and executable name: %SystemRoot%\system32\mstsc.exe
   - Parameters: %temp%\mygr1.rdp

6. Click OK.

Configure the Remote Desktop Profile to Start Automatically

In the same Native Application, add another endpoint application for the Remote Desktop Profile. Define it as a Downloaded from Mobile Access endpoint application, which is downloaded to the user desktop as soon as SSL Network Extender is launched.

1. In the Endpoint Applications - Advanced window, click Add.

   The Edit Endpoint Application window opens.

2. Configure the Remote Desktop profile package with the following settings.
   - Add link to the application in the Mobile Access portal must be unchecked.
   - Name: mygr1_RDP_Policy (as configured in GuiDBedit.exe).

3. Click Advanced.

   The Advanced window opens.

4. Select Automatically Start this Application: When SSL Network Extender is launched.

5. Click OK three times to save and close the Native Application.

Assign the Native Application to the User Group

Assign the Native Application to the relevant user group.

Configuring Downloaded-from-Gateway Endpoint Applications

In the Endpoint Applications page of the Native Application object:

1. Select Add link in the Mobile Access portal.

2. Select Advanced > Edit. The Endpoint Applications - Advanced window opens.

3. Click Add. The Edit Endpoint Application window opens.

4. Select Downloaded-from-Gateway.

5. From the Name drop-down list, select the desired downloaded-from-gateway application.

6. Specify the Parameters for the downloaded-from-gateway application. The parameters field is used to pass additional information to the downloaded-from-gateway applications on the endpoint machine, and to configure the way they are launched.

   The $$user variable can be used here to dynamically change according to the login name of the currently logged in user.

   See the configuration sections below for details of the required parameters:

   Note - In the configuration sections for certified and add-on applications, below:
   parameter is a compulsory parameter,
   [parameter] is an optional parameter,
   | indicates a required choice of one from many.

   - Configuring the Telnet Client (Certified Application) (on page 92)
   - Configuring the SSH Client (Certified Application) (on page 92)
- Configuring the TN3270 Client (Certified Application) (on page 92)
- Configuring the TN5250 Client (Certified Application) (on page 92)
- Configuring the Remote Desktop Client (Add-On Application) (on page 93)
- Configuring the PuTTY Client (Add-On Application) (on page 94)
- Configuring the Jabber Client (Add-On Application) (on page 94)
- Configuring the FTP Client (Add-On Application) (on page 94)

7. Continue with Completing the Native Application Configuration (on page 82).

**Configuring the Telnet Client (Certified Application)**

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters field</td>
<td>Server name or IP address. Default port is 23.</td>
</tr>
<tr>
<td>Parameters usage</td>
<td>server [port]</td>
</tr>
<tr>
<td>Description</td>
<td>Telnet terminal. Provides user oriented command line login sessions between hosts on the Internet.</td>
</tr>
<tr>
<td>Home page</td>
<td><a href="http://javassh.org">http://javassh.org</a></td>
</tr>
</tbody>
</table>

**Configuring the SSH Client (Certified Application)**

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters field</td>
<td>Server name or IP address.</td>
</tr>
<tr>
<td>Parameters usage</td>
<td>server</td>
</tr>
<tr>
<td>Description</td>
<td>Secure Shell (SSH) is designed for logging into and executing commands on a networked computer. It provides secure encrypted communications between two hosts over an insecure network. An SSH server, by default, listens on the standard TCP port 22.</td>
</tr>
<tr>
<td>Home page</td>
<td><a href="http://javassh.org">http://javassh.org</a></td>
</tr>
</tbody>
</table>

**Configuring the TN3270 Client (Certified Application)**

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>All. Requires Java 1.3.1 or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters field</td>
<td>Ignored</td>
</tr>
<tr>
<td>Description</td>
<td>IBM 3270 terminal emulator tailored to writing screen-scraping applications. TN3270 is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminal.</td>
</tr>
<tr>
<td>Home page</td>
<td><a href="http://jagacy.com">http://jagacy.com</a></td>
</tr>
</tbody>
</table>

**Configuring the TN5250 Client (Certified Application)**

| Supported Platforms | All endpoint machines must have Java 1.4 or higher. |
Native Applications for Client-Based Access

Parameters field
Optional. Can use the Configure button on the application instead. For the full list of options that can be used in the parameters field, see the Quick Start Guide http://tn5250j.sourceforge.net/quick.html.

Parameters usage
[Server [options]]

Description
IBM 5250 terminal emulator that interprets and displays 5250 data streams. You will be presented with a Connections screen for defining sessions. Select the configure button to define sessions when the session selection window opens. On first invocation of the emulator there are some console warning messages. These inform you that defaults files are being set up for the first run.

Home page
http://tn5250j.sourceforge.net/index.html

Quick Start Guide
http://tn5250j.sourceforge.net/quick.html

Configuring the Remote Desktop Client (Add-On Application)

Supported Platforms
All platforms. Endpoint machines must have Java 1.4 or higher.

Parameters field
Must contain the server name or its IP address.

Parameters usage
[options] server[:port]
For example: -g 800x600 -l WARN RDP_Server. Options:
- -b - Bandwidth saving (good for 56k modem, but higher latency). This option clears the TCP 'no delay' flag.
- -d - Windows domain you are connecting to.
- -f - Show the window full-screen (requires Java 1.4 for proper operation).
- -g WIDTHxHEIGHT. - The size of the desktop in pixels.
- -m - Keyboard layout on terminal server for languages (for example, en-us).
- -l {DEBUG, INFO, WARN, ERROR, FATAL} - Amount of debug output (otherwise known as the logging level).
- -lc - Path to a log4j configuration file.
- -n - Override the name of the endpoint machine.
- -u - Name of the user to connect as.
- -p - Password for the above user.
- -s - Shell to launch when the session is started.
- -t - Port to connect to (useful if you are using an SSH tunnel, for example).
- -T - Override the window title.

Description
Downloaded-from-Mobile Access Client for Windows NT Terminal Server and Windows 2000/2003 Terminal Services. Communicates using Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required. Runs on Java 1.1 up (optimized for 1.4), and works on Linux, Windows and Mac.

Home page
http://properjavardp.sourceforge.net

Mobile Access Administration Guide R77 Versions | 93
### Configuring the PuTTY Client (Add-On Application)

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>Windows only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters field</td>
<td>Optional. Leaving the Parameters field empty leads PuTTY Client to open in full graphical mode.</td>
</tr>
<tr>
<td>Parameters usage</td>
<td><code>[-ssh -telnet -rlogin -raw] [user@]server [port]</code></td>
</tr>
<tr>
<td>Description</td>
<td>An implementation of Telnet and SSH for Win32 platforms, including an Xterm terminal emulator.</td>
</tr>
<tr>
<td>Home page</td>
<td><a href="http://www.eos.ncsu.edu/remoteaccess/putty.html">http://www.eos.ncsu.edu/remoteaccess/putty.html</a></td>
</tr>
</tbody>
</table>

### Configuring the Jabber Client (Add-On Application)

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>All platforms. Endpoint machines must have Java 1.4 or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters field</td>
<td>Ignored</td>
</tr>
<tr>
<td>Description</td>
<td>Downloaded-from-Gateway Jabber Client is an instant messenger based on the Jabber protocol. Runs on every computer with at least Java 1.4.</td>
</tr>
<tr>
<td>Home page</td>
<td><a href="http://jeti.jabberstudio.org">http://jeti.jabberstudio.org</a></td>
</tr>
</tbody>
</table>

### Configuring the FTP Client (Add-On Application)

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>All. endpoint machines must have Java 1.4 or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters field</td>
<td>Ignored</td>
</tr>
<tr>
<td>Description</td>
<td>Graphical Java network and file transfer client. Supports FTP using its own FTP API and various other protocols like SMB, SFTP, NFS, HTTP, and file I/O using third party APIs, includes many advanced features such as recursive directory up/download, browsing FTP servers while transferring files, FTP resuming and queuing, browsing the LAN for Windows shares, and more.</td>
</tr>
</tbody>
</table>
Chapter 7

Exchange Mail Applications for Smartphones and Tablets

In This Section:

- Capsule Workspace Mail Applications ................................................................. 95
- ActiveSync Applications .......................................................................................... 96
- Policy Requirements for ActiveSync Applications .................................................. 97
- Configuring a TLS/SSL Version for an Application .................................................. 97

Capsule Workspace Mail and Active Sync Applications are applications for smartphone and tablet users to connect to email through an Exchange server. Web applications and File shares can also be available on smartphones and tablets.

Capsule Workspace Mail Applications

Capsule Workspace Mail Applications work with Exchange servers to make business email available on mobile devices with a Capsule Workspace App. The application is in a secure area on the Mobile Device that is usually protected with a passcode. All data in Capsule Workspace is encrypted.

During the Mobile Access Wizard, if you select Mobile Devices > Capsule Workspace, and enter an Exchange server, a Capsule Workspace Mail Application is automatically created. Make sure that users have access to the Capsule Workspace Mail Application in your Mobile Access policy.

To configure a Capsule Workspace Mail application:

1. If it is a new application, in the Mobile Access tab > Applications > Capsule Workspace Mail, click New.
   - If it is an existing application, in the Mobile Access tab > Applications > Capsule Workspace Mail, double-click the application.
   - A Capsule Workspace Mail window opens.

2. In the General Properties page:
   - Enter a Name for the application in SmartDashboard
   - Optional: Enter a comment
   - Enter the name of the Exchange Server that will communicate with the gateway and the Port. For example, ad.example.com.

3. In the Exchange Access page, in the Define access settings area:
   - Use encryption (https) - By default, traffic to the Exchange server works with HTTPS.
   - Use non-default path - If the Exchange Web Services path on the Exchange server to the application is not the default, enter the path here.
     - The default path is EWS/Exchange.asmx and the URL is https://<IP address of the Exchange Server>/EWS/Exchange.asmx.
   - Use specific domain - If you want users to authenticate to a specified domain on the Exchange server, enter it here.

4. In the Exchange Access page, in the Proxy Settings area, if there is a proxy server between the Exchange Server and the gateway, configure the settings here.
   - Use gateway proxy settings - By default the proxy settings configured for the gateway are used.
   - Do not use proxy server - Select if no proxy server is required.
• **Use specific proxy server** - Configure a proxy server that the gateway communicates with to reach the Exchange Server.
  
  (i) Select the **Host** and **Service**.
  
  (ii) If credentials are required to access the proxy server, select **Use credentials for accessing the proxy server** and enter the **Username** and **Password**.

5. In the **Display Link** page:
   
   • **Title** - The name of the application that users will see on their mobile devices.
   
   • **Description** - The description of the application that users will see on their mobile devices.

6. In the **Single Sign On** page, select the source of the credentials used for Single Sign-On for this application:
   
   • **Login to Exchange with the application credentials** - By default, use the same credentials that users use to log in to the Business Secure Container. This only applies if the authentication method configured for them on the gateway is Username/Password (**Gateway Properties > Mobile Access > Authentication**).
   
   • **Prompt for user credentials and store them locally for reuse** - Use different credentials for the Business Secure Container.
     
     - **Show the user the following message on the credentials prompt** - Select this and enter a message that users see when prompted to enter the credentials required for the Business Secure Container.

7. In the **Periodic Test** page, select which tests are run regularly on the gateways to make sure they can connect to the Exchange server. If there is a connectivity problem, a System Alert log generated.
   
   • **Run periodic test from gateways that have access to this application** - A test makes sure there is connectivity between the gateway and Exchange server. The test runs at the interval that you enter.
   
   • **Perform extensive test using the following account** - Periodically run a test to make sure that a user can authenticate to the Exchange server. To run this test you must enter a valid **Username** and **Password**.

   - **Note** - If the account password changes, you must enter the new password here.

### ActiveSync Applications

An ActiveSync application is an email application that works with ActiveSync, which is native in most Mobile devices. Mobile devices that can use the ActiveSync protocol and connect to an Exchange server can access ActiveSync applications.

As opposed to Capsule Workspace Mail applications, ActiveSync applications are not located in the Business Secure Container and are not protected. If you use the ActiveSync application, make sure that your mobile device is protected in other ways so that your sensitive business data and Exchange user credentials stay safe.

Make sure to give users access to the ActiveSync application in your Mobile Access policy.

**To configure an ActiveSync application:**

1. If it is a new application, in the **Mobile Access tab > Applications > ActiveSync Applications**, click **New**.
   
   If it is an existing application, in the **Mobile Access tab > Applications > ActiveSync Applications**, double-click the application.
   
   An **ActiveSync Application** window opens.

2. In the **General Properties** page:
   
   • Enter a **Name** for the application in SmartDashboard
   
   • Optional: Enter a comment
   
   • Enter the name of the **Exchange Server** that will communicate with the gateway and the **Port**. For example, ad. example.com.
3. In the Exchange Access page, in the Define access settings area:
   - **Use encryption (https)** - By default, traffic to the Exchange server works with HTTPS.
   - **Use non-default path** - If the ActiveSync path on the Exchange server to the application is not the default, enter the path here.
   - **Use specific domain** - If you want users to authenticate to a specified domain on the Exchange server, enter it here.

4. In the Exchange Access page, in the Proxy Settings area, if there is a proxy server between the Exchange Server and the gateway, configure the settings here:
   - **Use gateway proxy settings** - By default the proxy settings configured for the gateway are used.
   - **Do not use proxy server** - Select if no proxy server is required.
   - **Use specific proxy server** - Configure a proxy server that the gateway communicates with to reach the Exchange Server.
     (i) Select the Host and Service.
     (ii) If credentials are required to access the proxy server, select Use credentials for accessing the proxy server and enter the Username and Password.

5. In the Display Link page:
   - **Title** - The name of the application that users will see on their mobile devices.
   - **Description** - The description of the application that users will see on their mobile devices.

6. In the Periodic Test page, select which tests are run regularly on the gateways to make sure they can connect to the Exchange server. If there is a connectivity problem, a System Alert log generated.
   - **Run periodic test from gateways that have access to this application** - A test makes sure there is connectivity between the gateway and Exchange server. The test runs at the interval that you enter.
   - **Perform extensive test using the following account** - Periodically run a test to make sure that a user can authenticate to the Exchange server. To run this test you must enter a valid Username and Password.

   **Note** - If the account password changes, you must enter the new password here.

### 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 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.

### Configuring a TLS/SSL Version for an Application

You can configure which SSL protocol to use on the internal server for Web applications and Exchange Mail applications. For example, you can configure that a Capsule Workspace Mail application always uses TLS 1.0. If you do not configure this, Mobile Access uses the default version that the organizational server recommends.

Configure the feature for each application in GuiDBedit.

This feature is supported in R77.20 and higher. To learn how to activate this feature, see sk101217 (http://supportcontent.checkpoint.com/solutions?id=sk101217).
To configure an SSL version for an application:

1. Open GuiDBedit.
2. Go to Other > network_applications > APPLICATION NAME > internal_resource_ssl_version.
3. Select a version. The options are:
   - auto (default) - Uses the version that the organizational server recommends
   - SSLv3 (SSL 3.0)
   - TLSv1 (TLS 1.0)
4. Save the changes.
5. Install policy.
Chapter 8

Mobile Access for Smartphones and Tablets

In This Section:

- Overview of Mobile Access for Smartphones and Tablets ............................................. 99
- Certificate Authentication for Handheld Devices .......................................................... 99
- Managing Client Certificates ......................................................................................... 99
- Remote Wipe .................................................................................................................. 100
- Managing Capsule Workspace Settings ....................................................................... 100
- Push Notifications ......................................................................................................... 102
- ESOD Bypass for Mobile Apps ..................................................................................... 106
- MDM Cooperative Enforcement ................................................................................... 103
- System Specific Configuration ....................................................................................... 109
- Instructions for End Users ............................................................................................ 116
- Advanced Gateway Configuration for Handheld Devices .......................................... 118

Overview of Mobile Access for Smartphones and Tablets

To manage your users and their access to resources, make sure to:

- For email, calendar, and contact access, configure Capsule Workspace Mail or ActiveSync applications ("Exchange Mail Applications for Smartphones and Tablets" on page 95). This can be done automatically in the Mobile Access Wizard.
- Configure Web applications on page 37, if necessary.
- Make sure users have the information required to authenticate to the gateway. For client certificates, use the Certificate Creation and Distribution Wizard ("Creating Client Certificates" on page 100).
- Make sure users' Mobile Settings ("Managing Capsule Workspace Settings" on page 103) meet your organization's needs.
- Tell users which App to install.
- Make sure smartphone and tablet users are included in your Mobile Access Policy.

Certificate Authentication for Handheld Devices

For handheld devices to connect to the gateway, these certificates must be properly configured:

- If the configured authentication methods is Personal Certificate, generate client certificates for users ("Managing Client Certificates" on page 100).
- A server certificate (see "Server Certificates" on page 176) signed by a trusted third-party Certification Authority (for example, Entrust) is strongly recommended. If you have a third-party certificate, make sure the CA is trusted by the device. If you do not have a third-party certificate, a self-signed (ICA) certificate, is already configured on the server.
Managing Client 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.

Manage client certificates on the Client Certificate page of the Mobile Access tab.

The page has two panes.

- In the Client Certificates pane:
  - Create, edit, and revoke client certificates.
  - See all certificates, their status, expiration date and enrollment key. By default, only the first 50 results show in the certificate list. Click Show more to see more results.
  - Search for specified certificates.
  - Send certificate information to users.

- In the Email Templates for Certificate Distribution pane:
  - Create and edit email templates for client certificate distribution.
  - Preview email templates.

Creating Client Certificates

A Wizard helps you create and distribute client certificates to multiple users or a single user.

Note - If you use LDAP or AD, creating 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.

To create and distribute certificates with the client certificate wizard:

1. In the Mobile Access tab, open the Client Certificates page.
2. In the Client Certificates pane, select New.
   The Certificate Creation and Distribution wizard opens.
3. In the Certificate Distribution page, select how to distribute the enrollment keys to users. You can select one or both options.
   a. Send an email containing the enrollment keys using the selected email template - Each user gets an email, based on the template you choose, that contains an enrollment key.
      - Template - Select the email template that will be used. You can click View to preview the selected template.
      - Site - Select the gateway that users will connect to.
      - Mail Server - Select the mail server that will send the emails. You can click Edit to view and change its details. In the From Address field, set the email address that the email will come from.
   b. Generate a file that contains all of the enrollment keys - Generate a file for your records that contains a list of all users and their enrollment keys. Click Browse to select the path where a file will be saved.
4. Optional: To change the expiration date of the enrollment key, edit the number of days in Users must enroll within x days.
5. Optional: Add a comment that will show next to the certificate in the certificate list on the Client Certificates page.
6. Click Next.
   The Users page opens.
7. Click Add to add the users or groups that require certificates.
   - Type text in the search field to search for a user or group.
   - Select a type of group to narrow your search.
8. When all included users or groups show in the list, click Generate to create the certificates and send the emails.
9. If more than 10 certificates are being generated, click **Yes** to confirm that you want to continue. A progress window shows. If errors occur, an error report opens.
10. Click **Finish**.

**Revoking Certificates**

If the status of a certificate is Pending Enrollment, after you revoke it, the certificate does not show in the **Client Certificate** list.

**To revoke one or more certificates:**
1. Select the certificate or certificates from the **Client Certificate** list.
2. Click **Revoke**.
3. Click **OK**.

After you revoke a certificate, it does not show in the **Client Certificate** list.

**Creating Templates for Certificate Distribution**

You can create multiple email templates to use to distribute certificate enrollment keys to users. When you create new certificates, the wizard prompts you to select which email template to use to distribute the enrollment keys.

In the template, you can insert:
- **Predefined fields** - Such as Username, Registration Key, Expiration Date
- **Links** - A link or QR code that users can go to or scan from their mobile devices. You can insert multiple links into an email template.

**To create or edit an email template:**
1. In the **Mobile Access** tab, open the **Client Certificates** page.
2. To create a new template: In the **Email Templates for Certificate Distribution** pane, select **New**.
   To edit a template: In the **Email Templates for Certificate Distribution** pane, double-click a template.
   The **Email Template** 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.

   - **Certificate and Site 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 to give users access to internal websites, file shares, and Exchange servers.
     - **Capsule Connect/VPN** - A full L3 tunnel app that gives users network access to all mobile applications.
     - **Used in a Per-App VPN site** - In R77.30 and higher, you can use Per-App VPN for more granular control of which applications can access the VPN tunnel. You must configure the
b. **Download Application** - Direct users to 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 to give users access to internal websites, file shares, and Exchange servers.
  - **Capsule Connect/VPN** - 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 complete 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**.

### Cloning a Template

Clone an email template to create a template that is similar to one that already exists.

**To create a clone of an email template:**

1. Select a template from the template list in the **Client Certificates** page.
2. Click **Clone**.
3. A new copy of the selected template opens for you to edit.

### Remote Wipe

Remote Wipe removes the offline data cached on the user's mobile device.

This feature is supported in R77.10 and higher.

When the administrator revokes the internal CA certificate, a Remote Wipe push notification is sent, if the Remote Wipe configuration for the client enables **Remote Wipe by Push Notification**. Remote Wipe is triggered when the device gets the push notification.

**Note:** Remote Wipe by Push Notification works by best effort. There is no guarantee that the gateway will send the notification, or that the client will get it successfully.

If the device does not get the Remote Wipe push notification, Remote Wipe is triggered when the client does an activity that requires connection to the gateway while using a revoked internal CA certificate.

Remote Wipe send logs:

- If a Remote Wipe Push Notification is sent.
- When a Remote Wipe process ends successfully.

This feature is supported in R77.10 and higher.

**To configure Remote Wipe:**

1. Run the command on the gateway.

**Syntax:** `cvpnd_settings <conf_file_path> {set|listAdd|listRemove} <name> <value>`

- To enable or disable Remote Wipe:
  
  ```sh
  [expert@hostname:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C set RemoteWipeEnabled {true|false}
  ```

  Remote Wipe is enabled by default.
To enable or disable Remote Wipe by Push Notification (wipe is done if client gets notification):

```
[expert@hostname:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C set RemoteWipePushEnabled {true|false}
```

The Remote Wipe Push Notifications feature is enabled by default. For supported clients, see sk95587.

To set supported devices for Remote Wipe Push Notifications, based on operating system:

```
[expert@hostname:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd RemoteWipePushSupportedClientOS {iOS | Android}
```

2. Run: `[expert@hostname:0]# cvpnrestart`
   You must restart the cvpn service to apply the changes.

To see that your changes are applied, open the `$CVPNDIR/conf/cvpnd.C` file in Read-Only mode.

### To trigger Remote Wipe on a device:

1. Make sure that `cvpnd.C` is configured for Remote Wipe and, if you want, for Push Notifications. If you change the file, run: `[expert@hostname:0]# cvpnrestart`

2. Revoke the client certificate:
   a) Open **Mobile Access** tab > **Client Certificates**.
   b) Select certificates.
   c) Click **Revoke**.
   d) Click **OK**.

### To see Remote Wipe logs:

1. Open SmartLog.

2. Query for: "Remote Wipe" AND blade:"Mobile Access" action:"Failed Log In"
   You can filter these results for user DN, device ID, or certificate serial number.

---

### Managing Capsule Workspace Settings

For Capsule Workspace, many settings that affect the user experience on mobile devices come from the **Mobile Profile**. Each Mobile Access user group has an assigned Mobile Profile. By default, all users get the Default Profile.

The settings in the Mobile Profile include:

- Passcode and access Settings
- Mail, Calendar, and Contacts availability
- Settings for offline content
- Settings for push notifications
- Settings for Calendar and Contacts

To enable some features, you must install the R77.30 Add-on. See the **Release Notes** for more information.

Manage the Mobile Profiles in **Mobile Access** tab > **Capsule Workspace Settings**.

- **In the Mobile Profiles** pane:
  - See all Mobile Profiles.
  - Create, edit, delete, clone, and rename Mobile Profiles.

- **In the Mobile Profile Policy** pane:
  - Create rules to assign Mobile Profiles to user groups.
  - Search for a user or group within the policy rules.
Creating and Editing Mobile Profiles

Create and edit Mobile Profiles to meet the security requirements of your organization and the needs of different users. Assign Mobile Profiles to user groups in the Mobile Profile Policy. The Mobile Profile Policy applies to Capsule Workspace App users.

To create or edit a Mobile Profile

In the Mobile Access tab > Capsule Workspace Settings > Mobile Profiles pane:

- To create a new Mobile Profile, click New.
- To edit a Mobile Profile, select the profile and click Edit.

The Mobile Profile opens.

Configure these settings in the Mobile Profile:

To enable some features, you must install the R77.30 Add-on. See the Release Notes for more information.

- **Access Settings** - Configure settings related to user access and security:
  - **Session timeout** - After users authenticate with the authentication method configured in Gateway Properties > Mobile Access > Authentication, configure how long they stay authenticated to the gateway.
  - **Activate Passcode lock** - Select to protect the Business Secure Container area of the mobile device with a passcode.
    - **Passcode profile** - Select a passcode profile ("Passcode Profiles" on page 105) to use. The profile includes the passcode complexity, length, expiration, and number of failed attempts allowed.
    - **Allow storing user credentials on the device for single-sign on** - If username and password authentication is used, store the authentication credentials on the device. Then users are only prompted for their passcode not also for their username and password.
  - **Report jail-broken devices** - Create a log if a jail-broken device connects to the gateway.
    - **Block access from jail-broken devices** - Block devices that are jail-broken from connecting to the gateway.
  - **Track user's GPS location** (upon user’s approval) - Tracks devices connecting to the gateway.

- **Allowed Items** - Select which Exchange features are available on devices:
  - **Mail**
  - **Calendar**
  - **Contacts**
  - **Notes**

- **Offline Content** - Configure what data is saved and for how long when the Check Point App cannot reach the gateway.
  - **Mail from the last x days** - Select the length of time from which emails are saved.
    - **Cache Mail** - Select which parts of the email are saved in the offline cache.
  - **Calendar from the last x months and the following x months** - Select which parts of the calendar are saved: the length of time in the past and length of time in the future.
    - **Cache Calendar** - Select which parts of the calendar entry are saved in the offline cache.
  - **Synchronize contacts** - Synchronize contacts so they are available offline.

- **Push Notifications** - Configure what information shows in the push notifications for emails and meetings. For example, you can select that only the sender's address shows and not the subject.
  - **Allow push notifications** - When selected, users get push notifications. This only takes effect if push notifications are enabled for Capsule Workspace on the gateway that users connect to.
    - **Mail** - See a list of the configured notification for emails.
    - **Meeting** - See a list of the configured notification for meetings.
  - **Manage** - Click to see all configured push notifications, preview them, and change them.
• **Mail** -
  • **Allow copy paste of mail content** - Select if email content can be copied and pasted into other applications on the device.

• **Calendar** -
  • **Allow calendar sync to the device** - Select if the business calendar gets information from the native device calendar

• **Contacts** - Select which contacts to show in Capsule Workspace in addition to business contacts:
  • Global Address List
  • Local Phone

• **Check Point Capsule Docs** -
  • **Allow caching Check Point Capsule Docs credentials** - Select if credentials are required to open Capsule Docs protected documents are cached on the device. If they are not cached, users must enter their credentials each time they open a document for the first time.
  • **Allow caching Check Point Capsule Docs keys** - Select if a Capsule Docs keys are cached on the device. If they are cached users can open a previously opened document with no need to enter credentials.

**Passcode Profiles**

A passcode lock protects Capsule Workspace in mobile devices. In each Mobile Profile, configure which Passcode Profile it uses. The profile includes the passcode requirements, expiration, and number of failed attempts allowed. The default passcode profiles are Normal, Permissive, and Restrictive. You can edit the default profiles and create new profiles.

**To edit a Passcode Profile:**

• In the **Mobile Access tab > Additional Settings > Passcode Profile**, select a Passcode Profile and click **Edit**.

**To create a new Passcode Profile:**

• In the **Mobile Access tab > Additional Settings > Passcode Profile**, click **New**.

A Passcode Profile includes these settings:

• **Passcode Requirements** - The complexity requirements. When you configure this, remember that users usually have a small on-screen keyboard.
  • Simple Passcode (4 digits) - Users create a simple password of 4 numbers.
  • **Custom password** - Select from the requirements below.
    ▪ Minimum passcode length - Enter the minimum number of characters.
    ▪ Require alphanumeric characters - Show an alphanumeric keyboard and require at least one character to be a letter.
    ▪ Minimum complex characters - Enter the number of characters that must be a special character.

• **Force passcode expiration** - Enter the number of days after which user's passcodes expires and must be replaced.

• **Allow grace period for entering passcode** - Select to let users access the Business Secure Container for a specified period of time without re-entering their passcode. Enter the quantity of time in minutes.

• **Exit after a few failures in passcode verification** - Select to lock users out after a specified number of failed attempts. After the failed attempts, users must re-authenticate. If the authentication method includes username and password, users must enter them. If the authentication is certificate-only, users need a new certificate.

• **Enforce passcode history** - When selected, users cannot use a passcode that is the same as earlier passcodes. Select the number of earlier passcodes that users cannot use.
Push Notifications

This feature sends push notifications for incoming emails and meeting requests on handheld devices, while the Capsule Workspace Mail app is in the background. The app icon shows the number of new, unhandled notifications. One user can get notifications for multiple devices.

This feature is supported from R77.10. The configuration in R77.20 and higher is easier.

Push notifications are disabled by default in this version.

To use push notifications, the gateway must have connectivity to these URLs on ports 443 and 80:

- https://push.checkpoint.com (209.87.211.173 and 217.68.8.71)
- http://crl.verisign.com/pca3-g5.crl

Notes -

- Users must enable notifications for the Capsule Workspace Mail app on iOS devices
- Push notifications can increase Exchange server CPU usage if many users are connected
- The Exchange server must have access to the Mobile Access Portal.
- If you change the URL or IP address of the Mobile Access Portal after you enable push notifications, you must update the Push Portal attributes with GuiDBedit:
  a) In GuiDBedit, go to the portals section of your gateway > portal_name > ExchangeRegistration.
  b) Change main_url and ip_address to match the URL of the Mobile Access Portal.
  c) Save.
  d) Install policy on the gateway.

Configuring Push Notifications

To enable push notifications in R77.30 and higher:

To enable this feature, you must install the R77.30 Add-on. See the Release Notes for more information.

Enable push notifications from the Mobile Access Wizard or from the Gateway Properties of each gateway.

- From the Mobile Access Wizard:
  - If you enable Capsule Workspace Mail in the Mobile Access Wizard, push notifications are automatically enabled for the gateway.
  - If you enable Capsule Workspace Mail from the Mobile Access tab, push notifications are NOT enabled.

- From the Gateway Properties:
  a) Open a gateway object that has Mobile Access enabled.
  b) Select Mobile Access > Capsule Workspace from the tree.
  c) Select Enable Push Notifications.
  d) Click OK.

To enable push notifications in R77.20:

To learn how to activate this feature in R77.20, see sk101217 (http://supportcontent.checkpoint.com/solutions?id=sk101217).

Enable push notifications from the Mobile Access Wizard or from GuiDBedit.

- From the Mobile Access Wizard:
  - If you enable Capsule Workspace Mail in the Mobile Access Wizard, push notifications are automatically enabled for the gateway.
If you enable Capsule Workspace Mail from the Mobile Access tab, push notifications are NOT enabled.

In GuiDBedit:
   a) Open GuiDBedit.
   b) Search for `enable_push_notification`.
   c) Change the value of `enable_push_notification` to true on each Mobile Access Gateway object that will send push notifications.
   d) Save.
   e) Open SmartDashboard.
   f) Open each Mobile Access Gateway object and click **OK**.
   g) Install policy.

**To enable push notifications in R77.10:**

1. Before you make changes to `$CVPNDIR/conf/cvpnd.C`, create a backup copy
2. In `$CVPNDIR/conf/cvpnd.C`, change the value of `PNEnable` to **true**.
3. Run: `[expert@hostname:0]# cvpnrestart`
4. If the certificate on the Security Gateway is not trusted by the Exchange server, see *To import a certificate to the Exchange server* in Exchange Server and Gateway Communication (on page 108).

**Customizing Push Notifications**

In R77.30 and higher, you can customize push notifications from the mobile profile in the Mobile Access tab > Capsule Workspace Settings.

For R77.20 and lower gateways, use these instructions:

You can configure some custom options in the `$CVPNDIR/conf/cvpnd.C` file.

**Before you make changes to `$CVPNDIR/conf/cvpnd.C`, create a backup copy.**

**To send push notifications to a list of specified users:**

1. In `$CVPNDIR/conf/cvpnd.C`, change the value of `PNAllowUserNamesInListOnly` to **true**.
2. Configure the list of users to whom you want to send push notifications:

   ```
   PNAllowedUserNames {
       : (user1)
       : (user2)
   }
   ```
3. Run: `[expert@hostname:0]# cvpnrestart`

**To define the format of push notifications for email messages:**

1. Set the `PNDefaultMailMessage` parameter:
   ```
   PNDefaultMailMessage ("$push_notification_emoji$ $push_notification_importance$$push_notification_sender$: $push_notification_subject$"
   ```
2. Run: `[expert@hostname:0]# cvpnrestart`

**To define the format of push notifications for meeting requests:**

1. Set the `PNDefaultMeetingMessage` parameter:
   ```
   PNDefaultMeetingMessage ("$push_notification_emoji$ $push_notification_importance$$push_notification_sender$: Meeting Request - $push_notification_subject$")
   ```
2. Run: `[expert@hostname:0]# cvpnrestart`
**Exchange Server and Gateway Communication**

Make sure that the Exchange server can access the Mobile Access Portal.

On R77.20 and higher gateways, all confidential information between the Exchange server and the gateway uses encrypted SSL tunnels. All non-confidential information uses unencrypted HTTP connections.

You can configure all push notification communication to use SSL tunnels.

**To force all push notification communication to go through SSL tunnels:**

2. Open GuidBedit.
3. Search for the field main_url (Ctrl +F).
4. Press F3 to see next main_url until you find main_url that contains the value ExchangeRegistration.
5. Double-click the ExchangeRegistration main_url field and edit the value to be https:// and not http://.
6. Save.
7. Open SmartDashboard.
8. Open the Mobile Access gateway object.
9. Click OK.
10. Install policy.

On R77.10 gateways, if the certificate on the Security Gateway is not trusted, import the certificate to the Exchange Server. This is not necessary on R77.20 and higher gateways. For details about how to get the gateway certificate, see sk98203 (http://supportcontent.checkpoint.com/solutions?id=sk98203).

**To import a certificate to the Exchange server:**

1. Download the certificate to the Exchange server.
2. Run the Windows certificate installation wizard: double-click the certificate file, and follow the wizard steps.
3. Run Microsoft Management Console.
4. In the window that opens, click **File > Add/Remove Snap-in.**
   - **Add or Remove Snap-ins** window opens.
5. Select **Certificates** from the Available snap-ins, and click **Add**.
6. Select **My user account** and click **Finish**.
7. Select **Certificates** and click **Add** again.
8. Select **Computer account** and click **Next**.
9. Click **Finish**.
10. Click **OK**.

The certificate is stored in **Local computer** and in **Current user** stores.

**Monitoring Push Notification Usage**

Use the fwpush (on page 192) commands to monitor, debug, and troubleshoot push notification activity.

**Note** - Users must first install the latest version of the Capsule Workspace app from the app store and connect to the site created on the gateway.

To see failed batches, expired push notifications, and delayed push notifications, see:

$FWDIR/log/pushd_failed_posts

**Legal disclaimer on product functionality**

Check Point uses Apple and Google services to deliver push notifications to iOS and Android devices. This is consistent with industry practice and similar to other applications vendors. Accordingly, Check Point assumes no liability in the event a notification is not sent or is not successfully pushed.
Information which is sent as a push notification passes through Check Point’s push service and the Apple or Google push service (according to the user’s device). Check Point does not keep, filter, or read any information that passes through. Check Point may review basic information to determine if a push notification reached its destination.

Check Point provides configuration options for the information sent as a push notification. The administrator can choose whether to set the subject, the sender, or the importance of any email, and can send the meeting location for meeting invitations.

Check Point will not be held liable for any loss of information that may result during the push notification process.

**ESOD Bypass for Mobile Apps**

Hand-held devices cannot run Endpoint Security on Demand (ESOD) components. By default, ESOD is disabled for smartphones and tablets.

If your organization has ESOD enabled, mobile apps cannot access ESOD enforced applications.

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

**To change the ESOD setting on the Security Gateway:**

1. On the Security Gateway run:
   
   
   cvpnd_settings $CVPNDIR/conf/cvpnd.C set MobileAppBypassESODforApps "true" or "false"
   
   - true - Bypasses ESOD for mobile apps (default).
   - false - Does not bypass ESOD.

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.

**MDM Cooperative Enforcement**

Support for Mobile Device Management (MDM) through third-party vendors enforces a unified security policy for devices that access internal resources. Only managed devices that comply with the organizational security policy can successfully connect and access your business resources.

This feature is supported in R77.10 and higher.

Check Point Apps establish a secure VPN connection to the corporate network through a Check Point Security Gateway. The Security Gateway queries the policy of the MDM server. The MDM server verifies the compliance level of employees’ mobile devices when the VPN connection is established. The Security Gateway uses the MDM results to allow or block access, according to the device security and the user’s permissions.

This feature is supported by Check Point Capsule Connect and Capsule Workspace clients.

For the most updated vendor information see sk98201 (http://supportcontent.checkpoint.com/solutions?id=sk98201).

To configure MDM Cooperative Enforcement with iOS 7, see sk98447 (http://supportcontent.checkpoint.com/solutions?id=sk98447).

**Overview of the MDM Enforcement workflow:**

1. Before you start you must have:
   
   - An MDM account set up with required vendor license, if necessary
   - Necessary licenses for Capsule Connect or Capsule Workspace
   - Users with supported iOS or Android devices

3. For iOS 7 only: Configure settings and policy for your MDM vendor. See sk98447 (http://supportcontent.checkpoint.com/solutions?id=sk98447).
4. Make sure that the MDM functionality works - from a mobile device or Security Gateway console.

**Configuring MDM on the Security Gateway**

Enable MDM Enforcement in a configuration file on the gateway. Then define global options and vendor-specific options.

**To configure Mobile Device Management on a Security Gateway:**

1. Open the Gaia shell on the Security Gateway.
2. Log in to expert mode.
3. Open this file to edit: /FWDIR/conf/mdm.conf
4. Edit the global options.
   MDM is disabled by default. You must change enabled to 1.
5. Edit the vendor options.
6. Save the file.
7. Test the configuration.
8. Install policy.

**Global Options**

<table>
<thead>
<tr>
<th>mdm.conf Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| enabled          | 0 - MDM disabled  
|                  | 1 - MDM enabled   |
| monitor_only     | 0 - Full enforcement: non-compliant mobile devices cannot log in.  
|                  | 1 - Monitor only: non-compliant devices can log in and attempts are logged. |
| fail_open        | Defines behavior for cases of uncertainty, when an error occurs while checking MDM status.  
|                  | 0 - Drop VPN connections when an error occurs while checking MDM compliance status.  
|                  | 1 - Allow VPN connections when an error occurs while checking MDM compliance status. |
| session_timeout_in_sec | Maximum seconds allowed to determine device compliance status between the gateway and the MDM cloud service. Starts at device login. If passed, the action of fail_open starts. Recommended: keep default. |
| active_vendor    | Name of active third-party vendor, to test MDM compliance. You can configure multiple MDM vendors ("Advanced Vendor Support" on page 111), but only one can be active. |
| password_is_obscured | 0 - password parameters in mdm.conf show in clear text.  
### mdm.conf Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>verify_ssl_cert</td>
<td>0 - SSL certificates not verified when gateway accesses MDM cloud services. 1 - SSL certificates verified. Prevents some DNS poisoning, spoofing, man-in-the-middle attacks against gateway. Recommended: keep default (1). If the MDM server is in a cloud, this parameter must be 1. If you change it, the devices will be vulnerable to MITM attacks. (This risk is lower if the MDM server is local.)</td>
</tr>
<tr>
<td>ssl_ca_bundle_path</td>
<td>Local path on gateway of known CA certificate files. You can add more certificates to those that come with installation. Recommended: keep default.</td>
</tr>
<tr>
<td>ssl_cipher_list</td>
<td>Allowed ciphers for HTTPS between gateway and MDM cloud services. Recommended: keep default.</td>
</tr>
<tr>
<td>ssl_use_tls_v1</td>
<td>To use TLSv1 or SSL for HTTPS between gateway and MDM cloud services. Recommended: keep default.</td>
</tr>
</tbody>
</table>

### Vendor Options

In mdm.conf, there is a block of options for each vendor. You can add more, if you have an understanding of the vendor's API and expertise with PHP programming. See Advanced Vendor Support (on page 111).

For the most updated vendor information see sk98201 (http://supportcontent.checkpoint.com/solutions?id=sk98201).

### Obscuring Passwords in mdm.conf

If the global property password_is_obscured is enabled, obscure all parameters named password in the Vendor Configuration blocks.

**To get an obscured password string from your password:**

1. Run: `[expert@hostname:0]# obfuscate_password <password>`
   
   The output is a string. For example: `33542b323a3528343640`

2. Copy the string to the mdm.conf file, as the password value.

3. Save the file.

4. Install policy.

### Advanced Vendor Support

You can add more vendors. This requires PHP programming skills and an understanding of the third-party MDM vendor's cloud API.

In these steps, we use "BestMDM" as the name of a fictional MDM vendor. BestMDM's API requires an XML request to be sent to their URL that includes credentials and the ID of the device. It returns an XML response with the device status and reason.

**Example Request:**

```xml
<request>
  <username>api_username</username>
  <password>api_password</password>
  <device>device_id</device>
</request>
```
To add support for a new third-party vendor:

1. Open to edit: $CVPNDIR/phpincs/MDMVendors.php
2. Search for the text: to add another vendor
3. Remove the comment for a case branch.
4. Enter your MDM vendor name.
   For example:
   ```php
case "BestMDM":
    BestMDM($mdm_data);
    break;
```
5. At the end of the file, add a new PHP function. It must access the vendor's cloud API, and return a
   status and reason array.
   For example:
   ```php
function BestMDM($mdm_data) {
   // Build the request XML
   $request_xml = new SimpleXMLElement("<request><username/><password/><device/></request>");
   // Fill its fields with data from $mdm_data.
   // Note that "username", "password" and "device_id" always in $mdm_data.
   $request_xml->username = $mdm_data["username"];  
   $request_xml->password = $mdm_data["password"];  
   $request_xml->device = $mdm_data["device_id"];  
   // Make POST request using the supplied class URLRequest
   // (The class URLRequest is defined in the same .php file).
   $url = "https://bestmdm.com/api";
   $conn = new URLRequest(); // open HTTP/HTTPS request session
   $resp_data = $conn->Request( $url, $post_body = $xml->asXML() );
   // Handle possible network error.
   If ($resp_data === FALSE)
    return array("status"=>MDM_ERROR, "reason"=> $conn->get_error_message());
   // Now $resp_data is raw string returned by the cloud API. Parse it as XML:
   $resp_xml = new SimpleXMLElement($resp_data);
   // Check the status codes returned by the vendor’s API.
   $status = MDM_ERROR;
   switch ($resp_xml->status) {
   case "not_managed":
    return array("status"=>MDM_NOT_MANAGED, "reason"=>"");
   case "compliant":
    return array("status"=>MDM_COMPLIANT, "reason"=>"");
   case "not_compliant":
    return array("status"=>MDM_NOT_COMPLIANT, "reason"=>");
   }
```
>reason);
    default:
        return array("status"=>MDM_ERROR, "reason"=>"unknown status");
    } // end switch
} // end BestMDM compliance protocol handler

### Status Codes:
- **MDM_ERROR** - Error occurred while accessing the MDM vendor’s Cloud API.
- **MDM_NOT_MANAGED** - The device is not registered in the vendor’s database.
- **MDM_NOT_COMPLIANT** - The device is known to the vendor as “not compliant with its policy”.
- **MDM_COMPLIANT** - The device is known to the vendor as “compliant with its policy”.

6. **Define $mdm_data as an array of data from mdm.conf and the device ID.**

```
Array(
    "device_id"=><MAC address of device, or other ID known by the vendor>,
    "username"=><username to access the API of the MDM vendor>,
    "password"=><password to access the API of the MDM vendor>
)
```

**Important Notes:**
- Global parameters and vendor parameters are merged in one list.
- If a vendor parameter is the same name as a global parameter, the vendor parameter overrides the global parameter.
- If $mdm_data includes a password parameter, and password_is_obscured=1, the password is decrypted automatically. The function gets the clear text password.

**Example of $mdm_data:**

<table>
<thead>
<tr>
<th>With mdm.conf:</th>
<th>$mdm_data value:</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td>Array(</td>
</tr>
<tr>
<td>:enabled (1)</td>
<td>&quot;enabled&quot;=&gt;1,</td>
</tr>
<tr>
<td>:monitor_only (0)</td>
<td>&quot;monitor_only&quot;=&gt;0,</td>
</tr>
<tr>
<td>:fail_open (0)</td>
<td>&quot;fail_open&quot;=&gt;0,</td>
</tr>
<tr>
<td>:active_vendor (BestVendor)</td>
<td>&quot;active_vendor&quot;=&gt;&quot;BestVendor&quot;,</td>
</tr>
<tr>
<td>:BestVendor (</td>
<td>&quot;username&quot;=&gt;&quot;MyUser&quot;,</td>
</tr>
<tr>
<td>:username (MyUser)</td>
<td>&quot;auth_key&quot;=&gt;&quot;12345&quot;,</td>
</tr>
<tr>
<td>:auth_key (12345)</td>
<td>&quot;device_id&quot;=&gt;&quot;12:34:56:78:9A:BC:DE:F0&quot;</td>
</tr>
<tr>
<td>)</td>
<td>)</td>
</tr>
</tbody>
</table>

7. **Save MDMVendors.php.**
8. **Open $FWDIR/conf/mdm.conf.**
9. **Add a section after the last block for the new vendor.**
   For example:
   ```
   :BestMDM ( 
     :username (MyUserName) 
     :password (123456) 
   )
   ```
10. **Change the value of active_vendor to be the name of the new vendor.**
    For example: :active_vendor (BestMDM)
11. **Save the file.**
12. **Install policy.**
Testing MDM

To make sure that MDM functionality is configured correctly:
1. On a mobile device, launch the Check Point Mobile app.
2. Connect to the Security Gateway.
3. On SmartDashboard, open SmartView Tracker.
4. Search for **Network Security Blades > Mobile Access Blade > Login Activity**.
   - The **Compliance Check, Information, and Reason** values in the details of the device login, show data about MDM compliance status and requirements.

Advanced Testing

You can make sure the MDM configuration works without a device in hand, but it requires expert knowledge.
You log in to a test web page and enter the WiFi MAC address of a real device. For security, the MDM test page is disabled by default.

**To enable the test page:**
1. Log in to the Security Gateway console in **expert** mode.
2. Save a backup of `$CVPNDIR/conf/includes/Login.location.conf`.
3. Open `Login.location.conf` to edit.
4. Search for **test your integration**, and carefully follow the instructions there.
5. After you make required changes, save the file and run: `[expert@hostname:0]# cvpnrestart`
6. Open the Mobile Access Portal with the `/Login/MDMProxy` path.
   - For example: `https://<gateway_hostname>/sslvpn/Login/MDMProxy`
7. Enter the device MAC address.
8. Click **Submit**.
   - If there are issues for that device to access the third-party MDM vendor, the page shows diagnostics.
9. Revert `Login.location.conf` to the backup file.
10. Run: `[expert@hostname:0]# cvpnrestart`

To prevent security risks, always revert and close the test page.

**Example Diagnostics:**
- Parameters for the MDM vendor's cloud service (such as **Username** or **Password**) are not configured correctly in `$FWDIR/conf/mdm.conf`.
- There is a network problem accessing MDM vendor's cloud service.
- There is a problem with SSL certificates, which prevents the gateway from accessing the MDM vendor's cloud service.

System Specific Configuration

This section describes system specific configuration required for iPhones, iPads, and Android devices. In some instances, end-user configuration is also required.

**iPhone and iPad Configuration**

**Connecting iPhone/iPad Clients to ActiveSync Applications**

When you allow access to an ActiveSync application, users see the **Mail Setup** item and 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.
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.

**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.

**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.

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.

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.

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.

Instructions for End Users
Give these instructions to end users to configure their mobile devices to work with Mobile Access.

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.

Advanced Gateway Configuration for Handheld Devices
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 <conf_file_path> set <attribute_name> "<value>"
```

**To get the current value of an attribute:**

```
cvpnd_settings <conf_file_path> get <attribute_name>
```

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ActiveSyncAllowed</code> (true)</td>
<td>If access to ActiveSync applications is allowed.</td>
</tr>
</tbody>
</table>
| `ActiveSyncExchangeServerAuthenticationMethod` (basic)        | Method of forwarding authentication from the Mobile Access gateway to the internal Exchange server.  
|                                                              | Valid values: basic, digest, ntlm                                           |
| `ActiveSyncClientCertificateNeeded` (true)                    | If ActiveSync access for all mobile devices requires a client certificate. Changing this value affects all mobile devices using the gateway. |
| `MobileAppAllowActiveSyncProfileConfig` (true)                | 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.                                       |
| `MobileAppMinRequiredClientOSVersion` (3.1)                   | Minimum operating system version for iPhones and iPads. If a client fails this requirement, user sees Your OS version must be upgraded |
| `MobileAppAndroidMinRequiredClientOSVersion` (2.1)            | Minimum operating system version for Android. If a client fails this requirement, user sees Your OS version must be upgraded |
| `MobileAppMinRecommendedClientOSVersion` (3.1)                | 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. |
| `MobileAppAndroidMinRecommendedClientOSVersion` (2.1)        | Recommended operating system version for Android. If a client fails this recommendation, user sees a message but usage continues.  
<p>|                                                              | Note: value must be equal to or greater than Required value, or Mobile Access will not start. |
| <code>MobileAppMinRequiredClientAppVersion</code> (1.3)                  | Minimum App version required for iPhones and iPads. If a client fails this requirement, user sees Application Update Required |</p>
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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.</td>
</tr>
</tbody>
</table>
Chapter 9

User Authentication in Mobile Access

In This Section:

- User Authentication to the Mobile Access Portal .......................................................... 121
- Two-Factor Authentication with DynamicID ................................................................. 123
- Multiple Realms .............................................................................................................. 131
- Session Settings ............................................................................................................. 135

User Authentication to the Mobile Access Portal

To enter the Mobile Access portal and get access to its applications, users defined in SmartDashboard must authenticate to the Security Gateway. Authentication ensures that a user is who he or she claims to be. Users authenticate using one of these Authentication schemes:

- **Check Point Password** - Users are challenged to enter a password and user name that are stored in the internal Security Gateway database.
- **Personal Certificates** - Digital Certificates are issued by the Internal Certificate Authority or by a third party OPSEC certified Certificate Authority.
- **RADIUS Server** - Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme. The Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users. The RADIUS protocol uses UDP for communications with the gateway. RADIUS Servers and RADIUS Server Group objects are defined in SmartDashboard. For more about configuring a Security Gateway to use a RADIUS server, see the R77 Security Gateway Technical Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=24836).
- **SecurID** - SecurID is a proprietary authentication method of RSA Security. An external SecurID server manages access by changing passwords every few seconds. Each user carries a SecurID token, a piece of hardware that is synchronized with the central server and displays the current password. The Security Gateway forwards authentication requests by remote users to the ACE/Server. For more about configuring a Security Gateway to use SecurID, see the R77 Security Gateway Technical Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=24836).

A user who tries to authenticate with an authentication scheme that is not configured for the Mobile Access gateway will not be allowed to access resources through the gateway.

Optionally, two-factor authentication with DynamicID One Time Password can also be required as a secondary authentication method. When this is configured, users who successfully complete the first-phase authentication are challenged to enter an additional credential: a DynamicID One Time Password (OTP). The OTP is sent to their mobile communications device (such as a mobile phone) through SMS or directly to their email account.

Configuring Authentication

Permitted authentication schemes must be configured for each Security Gateway.

On the Security Gateway, you can configure authentication in one of two places:

- In the **Gateway Properties** window of a gateway in Mobile Access > Authentication. If you select an authentication method on this page, that is the method that all users must use to authenticate to Mobile
Access. You can configure other authentication methods that users must use for different blades on different pages.

On this page you can also configure per gateway settings for Two-Factor Authentication with a DynamicID One Time Password. The default authentication scheme is **Username and Password**.

- In the **Gateway Properties** window of a gateway in **Legacy Authentication**, In the **Legacy Authentication** page, you can allow access to users authenticating with different authentication methods. Authentication using Client Certificates from the Internal Certificate Authority is enabled by default in addition to the selected method.

In the **Mobile Access** tab, select **Authentication** to show an overview of the Mobile Access Security Gateways and their authentication schemes.

On this page you can also configure global settings for Two-Factor Authentication with a DynamicID One Time Password that will be used for all gateways that do not have their own DynamicID settings.

---

### Requiring Certificates for Mobile Devices

You can configure a protection level for Mobile Access applications that only lets mobile devices use the application if they authenticate with a client certificate. It is necessary to define the Mobile Access Authentication settings on each Mobile Access Security Gateway. This feature has an effect on these applications:

- ActiveSync applications
- Capsule Workspace Mail

**To require client certificates for mobile devices:**

2. From the navigation menu, select **Mobile Access > Authentication**.
3. Make sure that the Authentication Method is one of these options:
   - Username and password
   - RADIUS
   - SecurID
4. Select **Require client certificate when using ActiveSync applications or Capsule Workspace Mail**.
5. Install the policy.

---

### How the Gateway Searches for Users

If you configure authentication for a blade from the main Security Gateway **Legacy Authentication** page, the Security Gateway searches for users in a standard way when they try to authenticate. The gateway searches:

1. The internal users database.
2. If the specified user is not defined in this database, the gateway queries the User Directory (LDAP) servers defined in the Account Unit one at a time, and according to their priority.
3. If the information still cannot be found, the gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

If you configure an authentication method for a specific blade, the gateway searches for users according to the user groups that are used for authorization in that blade.

For example, in Mobile Access, the gateway looks at the Mobile Access policy to see which user groups are part of the policy. When the gateway tries to authenticate a user, it starts to search for users in the databases related to those user groups.

In IPsec VPN, the gateway looks at the Remote Access VPN Community to see which user groups are included. It starts to search for users in the databases related to those user groups.

A search based on the authentication scheme is faster, with better results. You can have users with the same user name in unrelated groups. The gateway will know which user is relevant for the blade based on the user groups.
Two-Factor Authentication with DynamicID

Two-factor authentication is a system where two different methods are used to authenticate users. Using two-factors as opposed to one delivers a higher level of authentication assurance.

In the first phase of the authentication, users must authenticate to the Mobile Access portal using either:

- The authentication method configured in Gateway Properties > Mobile Access > Authentication. If an authentication method is configured on this page, users must use that method and not other methods configured on a different Authentication page of the Security Gateway.
- One of the authentication methods that is enabled in the Gateway Properties > Other > Legacy Authentication page of the Security Gateway.

Users who successfully complete the first-phase authentication can be challenged to provide an additional credential: a DynamicID One Time Password (OTP). The OTP is sent to their mobile communications device (such as a mobile phone) via SMS or directly to their email account.

How DynamicID Works

When logging in to the Mobile Access portal, users see an additional authentication challenge such as:

Please type the verification code sent to your phone.

Users enter the one time password that is sent to the configured phone number or email address and they are then admitted to the Mobile Access portal.

On the User Portal sign in screen, the I didn’t get the verification code link shows. If the user does not receive an SMS or email with the verification code within a short period of time, the user can click that button to receive options for resending the verification code.

Administrators can allow users to select a phone number or email address from a list. Only some of the phone number digits are revealed. Users can then select the correct phone number or email address from the list and click Send to resend the verification code. By default, users can request to resend the message three times before they are locked out of the Portal.

Match Word

The Match Word feature ensures that users can identify the correct DynamicID verification code in situations when they may receive multiple messages. Users are provided with a match word on the Login page that will also appear in the correct message. If users receive multiple SMS messages, they can identify the correct one, as it will contain the same match word.

The SMS Service Provider

The DynamicID messages are sent by the SMS service provider that Mobile Access is configured to work with. DynamicID can be configured to work with any SMS provider that is able to accept an HTTP request and translate it into an SMS and that can receive email messages.

If DynamicID is configured to work with email only, an SMS Service Provider is not necessary.

To access the SMS service provider, the proxy settings that are configured in the SmartDashboard Mobile Access tab, Additional Settings > Network Elements > HTTP Proxy page are used. If none is defined, no proxy is used.

Whichever provider you work with, in order for the SMS messages to be sent to users, valid account details must be obtained from the provider and be configured in Mobile Access.

SMS Authentication Granularity

Two-factor authentication with DynamicID can be made a requirement for logging in to the gateway. Alternatively, DynamicID authentication can be made a requirement for accessing particular applications. This flexibility allows for varying security clearance levels.
Making two-factor authentication with DynamicID a requirement for accessing specific applications is done by configuring a Protection Level to require two-factor authentication, and associating the Protection Level with Mobile Access applications (see "Two-Factor Authentication per Application" on page 129).

In an environment with multiple Mobile Access gateways, making two-factor authentication a requirement for logging into a particular gateway is done by configuring two-factor authentication for that gateway ("Two-Factor Authentication per Gateway" on page 129).

**Basic DynamicID Configuration for SMS or Email**

The workflow for basic configuration of two-factor authentication via DynamicID is:

1. Obtaining the SMS provider credentials and/or email settings.
2. Configuring the Phone Directory
3. Basic SmartDashboard Configuration of DynamicID
4. Testing DynamicID Two-Factor Authentication

**Obtaining the SMS Provider Credentials**

Get these required SMS service provider settings from your SMS provider.

- A URL in the format specified by the SMS provider or a valid email address.
- Account credentials:
  - User name
  - Password
  - API ID (optional and may be left empty)

**Configuring the Phone Directory**

The default phone number and email search method is that the gateway searches for phone numbers or email addresses in user records on the LDAP account unit, and then in the phone directory on the local gateway. If the phone number configured is actually an email address, an email will be sent instead of an SMS message. The phone number and email search method can be changed in the Phone Number or Email Retrieval section of the Two-Factor Authentication with DynamicID - Advanced window.

**Configuring Phone Numbers or Email Addresses in LDAP**

If users authenticate via LDAP, configure the list of phone numbers on LDAP by defining a phone number or email address for each user. By default, Mobile Access uses the Mobile field in the Telephones tab. If the phone number configured is actually an email address, an email will be sent instead of an SMS message.

**Configuring Phone Numbers or Email Addresses on Each Security Gateway**

Configure the list of phone numbers or email addresses on each Mobile Access gateway. For a Mobile Access cluster, configure the directory on each cluster member.

**To configure a list of phone numbers on a gateway:**

1. Log in to the Mobile Access gateway using a secure console connection.
2. Change to Expert mode: Type `expert` and then the expert mode password.
3. Backup `$CVPNDIR/conf/SmsPhones.lst`
4. Edit `$CVPNDIR/conf/SmsPhones.lst`, and add to it a list of user names and phone numbers, and/or email addresses. The list must be followed by a blank line. Use this syntax:

```plaintext
<user name | Full DN> <phone number | email address>
```
### Parameter | Meaning
--- | ---
user name or Full DN | Either a user name or, for users that log in using a certificate, the full DN of the certificate.

phone number | All printable characters can be used in the phone number, excluding the space character, which is not allowed. Only the digits are relevant.

email address | A valid email address in the format user@domain.com

#### Example of acceptable ways to enter users and their phone numbers or email addresses in $CVPNDIR/conf/SmsPhones.lst
- bob +044-888-8888
- jane tom@domain.com
- CN=tom,OU=users,O=example.com +044-7777777
- CN=mary,OU=users,O=example.com +mary@domain.com

### Configuring Multiple Phone Numbers
You can let users choose from multiple phone numbers when resending the verification code.

**To configure choice of numbers:**
- Enter one number in the LDAP directory in the Mobile field and one or more in the gateway configuration file:
  - $CVPNDIR/conf/SmsPhones.lst
  
  Enter multiple phone numbers separated by white space in the gateway configuration file:
  - $CVPNDIR/conf/SmsPhones.lst
  
  For example, user_a 917-555-5555 603-444-4444

### Basic SmartDashboard Configuration of DynamicID
Configure the Authentication settings to make two-factor authentication necessary for all mobile devices.

**To configure DynamicID settings in SmartDashboard:**

1. From the Mobile Access tab, select Authentication. The Authentication page opens.
2. Select Challenge users to provide the DynamicID one time password.
3. Fill in the SMS Provider and Email Settings field using one of the following formats:
   a) To let the DynamicID code to be delivered by SMS only, use the following syntax:
   ```plaintext
   https://api.example.com/http/sendmsg?api_id=$APIID&user=$USERNAME&password=$PASSWORD&to=$PHONE&text=$MESSAGE
   ```
   b) To let the DynamicID code to be delivered by email only, without an SMS service provider, use the following syntax:
   ```plaintext
   mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslvpn@example.com;BODY=$RAWMESSAGE
   ```
   c) To let the DynamicID code to be delivered by SMS or email, use the following syntax:
   ```plaintext
   mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslvpn@example.com;BODY=$RAWMESSAGE
   ```

The following table explains parameters used in the SMS Provider and Email Settings field. The value of these parameters is automatically used when sending the SMS or email.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$APIID</td>
<td>The value of this parameter is the API ID.</td>
</tr>
<tr>
<td>$USERNAME</td>
<td>The value of this parameter is the username for the SMS provider.</td>
</tr>
<tr>
<td>$PASSWORD</td>
<td>The value of this parameter is the password for the SMS provider.</td>
</tr>
<tr>
<td>$PHONE</td>
<td>User phone number, as found in Active Directory or in the local file on the gateway, including digits only and without a + sign.</td>
</tr>
<tr>
<td>$EMAIL</td>
<td>The email address of the user as found in Active Directory or in the local SmsPhones.lst file on the gateway. If the email address should be different than the listed one, it can be written explicitly.</td>
</tr>
<tr>
<td>$MESSAGE</td>
<td>The value of this parameter is the message configured in the Advanced Two-Factor Authentication Configuration Options in SmartDashboard.</td>
</tr>
<tr>
<td>$RAWMESSAGE</td>
<td>The text from $Message but without HTTP encoding.</td>
</tr>
</tbody>
</table>

4. In the **SMS Provider Account Credentials** section, enter the credentials received from the SMS provider:
   - Username
   - Password
   - API ID (optional)

5. For additional configuration options, click **Advanced**.

6. Configure the Mobile Access Security Gateway to let computers and devices use DynamicID.
   a) Double-click the Mobile Access Security Gateway.
   b) From the navigation tree, select **Mobile Access > Authentication**.
   c) In the **Two-Factor Authentication** section, configure these settings:
      - For a Security Gateway that uses the global authentication settings, select **Global settings**.
      - For a Security Gateway that uses different authentication settings, select **Custom settings**.
      - For mobile devices, select **Allow DynamicID for mobile devices**.
   d) Click **OK**.

7. Install the policy.

**Testing Two-Factor Authentication**

To test the two-factor authentication via DynamicID, after completing the configuration:

1. Browse to the URL of the Mobile Access portal.
2. Log in as a user. Supply the gateway authentication credentials.
3. Wait to receive the DynamicID code on your mobile communication device or check your email.
4. Enter the DynamicID code in the portal.

You should now be logged in to the Mobile Access portal.

**Advanced Two-Factor Authentication Configuration**

Advanced options for two-factor authentication with DynamicID are available on the SmartDashboard **Users and Authentication > Authentication > Authentication to gateway > Two-Factor Authentication with DynamicID -Advanced** page.

You can also configure advanced options for two-factor authentication per gateway on the **Mobile Access Gateway Properties** window, in the **Additional Settings Authentication > Advanced** page.

The following sections explain the fields.
**DynamicID Authentication Enforcement**

- **Optional**
  Allow users to log in but deny access to applications that require DynamicID authentication:
  When users log in, they are given the option to “Skip” the two-factor authentication. Users who choose **skip** are allowed to log in, but are denied access to applications that require two-factor authentication.

- **Mandatory**
  Users must successfully authenticate using DynamicID in order to log in.

**DynamicID Message**

- **Message text to be sent to the user**
  By default, the text of the message is "**Mobile Access DynamicID one time password:**". The message can contain the template fields shown in the following table to include the user’s name and prompt users to use enter a One Time Password.
  For example, the message could say: **$NAME, use the verification code $CODE to enter the portal.**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$NAME</td>
<td>User name used in the first phase of authentication to the portal.</td>
</tr>
<tr>
<td>$CODE</td>
<td>Replaced with the One Time Password. By default, $CODE is added to the end of the message.</td>
</tr>
</tbody>
</table>

**DynamicID Settings**

- **Length of one time password** is 6 digits by default
- **One time password expiration (in minutes)** is 5 minutes by default. Ensure there is a reasonably sufficient time for the message to arrive at the mobile communication device or email account, for the user to retrieve the password, and to type it in.
- **Number of times users can attempt to enter the one time password before the entire authentication process restarts.** By default the user has 3 tries.

**Display User Details**

- In the portal, display the phone number or email address that received the DynamicID. By default, the phone number to which the SMS message was sent is not shown.

**Country Code**

- **Default country code for phone numbers that do not include country code.** The default country code is added if the phone number stored on the LDAP server or on the local file on the gateway starts with 0.

**Phone Number or Email Retrieval**

- **Active Directory and Local File**
  Try to retrieve the user details from the Active Directory user record. If unsuccessful, retrieve from the local file on the gateway. The LDAP account unit is defined in the **Users and Authentication > Authentication > LDAP Account Units** page of the SmartDashboard Mobile Access tab. The phone directory on the local gateway is stored at **$CVPNDIR/conf/SmsPhones.lst.**
• Active Directory Only
  Retrieve phone numbers from Active Directory user record without using the local file on the gateway. The LDAP account unit is defined in the Users and Authentication > Authentication > LDAP Account Units page of the SmartDashboard Mobile Access tab.

• Local File Only
  Retrieve the user details from the local file on the gateway. The phone directory on the local gateway is stored at $CVPNDIR/conf/SmsPhones.lst.

Configuring Resend Verification and Match Word

The DynamicID troubleshooting and match word features are configured in GuiDBedit, Check Point’s database tool that is a standard component of the SmartConsole. To run GuiDBedit, access:

C:\%ProgramFiles%\CheckPoint\SmartConsole\R77\PROGRAM\GuiDBedit.exe

The GuiDBedit table to edit depends on the Two Factor Authentication with SMS One Time Password (OTP) setting that you configured in SmartDashboard in the Mobile Access Gateway Properties page > Authentication.

• If your DynamicID One Time Password settings are global across all of your gateways (use the global settings configured in the Mobile Access tab is selected), in GuiDBedit select Other > Mobile Access Global Properties.

• If your DynamicID One Time Password settings are configured for a specific gateway (This gateway has its own two-factor authentication settings is selected), in GuiDBedit select network_objects and then select the specific gateway you want to edit.

The following table shows the DynamicID features that can be configured, and where in GuiDBedit to configure them.

### Configuring DynamicID Settings in GuiDBedit

<table>
<thead>
<tr>
<th>Feature</th>
<th>Field Name/s to Edit</th>
<th>Value Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Word</td>
<td>use_message_matching_helper</td>
<td>true: match word provided&lt;br/&gt;false: match word not provided (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resend message</td>
<td>Enable_end_user_re_transmit_message</td>
<td>true: enable resend SMS feature (default)&lt;br/&gt;false: disable resend SMS feature</td>
</tr>
<tr>
<td>Display multiple phone</td>
<td>enable_end_user_select_phone_num</td>
<td>true: enable option to choose from multiple phone numbers or email addresses when&lt;br/&gt;resending the verification code (default)&lt;br/&gt;false: one phone number or email address&lt;br/&gt;from the LDAP server or local file is used automatically without choice</td>
</tr>
<tr>
<td>numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conceal displayed phone</td>
<td>Edit both:&lt;br/&gt;reveal_partial_phone_num</td>
<td>true: conceal part of the phone number or email address (default)&lt;br/&gt;false: display the full phone number or email address&lt;br/&gt;1-20: Choose the amount of digits to reveal (default is 4)</td>
</tr>
<tr>
<td>numbers</td>
<td>number_of_digits_revealed</td>
<td></td>
</tr>
</tbody>
</table>

After editing the values in GuiDBedit, save the changes, connect to SmartDashboard, and install the policy.

Configuring the Number of Times Messages are Resent

By default, users can request to resend the verification code message three times by clicking the **I didn’t get the verification code** link before they are locked out of the Mobile Access Portal. The number of times
the message can be resent is configured using the `cvpnd_settings` command from the Mobile Access CLI in expert mode.

The instructions below relate to actually resending the verification code message. The number of times users can try to input the verification code is configured in SmartDashboard in the **Two Factor Authentication Advanced** window.

To change the number of times the verification code message can be resent to 5, run:

```bash
cvpnd_settings $CVPNDIR/conf/cvpnd.C set smsMaxResendRetries 5
```

You can replace "5" with any other number to configure a different amount of retries.

After making the changes, run `cvpnrestart` to activate the settings.

If the Mobile Access gateway is part of a cluster, be sure to make the same changes on each cluster member.

**Two-Factor Authentication per Gateway**

Successful two-factor authentication can be made a requirement for logging on to some but not all Mobile Access gateways.

There are two possible approaches:

- **Globally on, with custom settings per gateway**: Turn on two-factor authentication globally, and then for each Mobile Access gateway, configure custom settings: either turn off the feature, or configure gateway-specific settings.

- **Globally off, with custom settings per gateway**: Turn off two-factor authentication globally, and then for selected Mobile Access gateways, turn it on, while configuring custom settings for those gateways.

You can also let mobile devices use two-factor authentication with DynamicID to connect to this Mobile Access Security Gateway.

**To configure two-factor authentication** Globally on, with custom settings per gateway:

1. Set up basic two-factor authentication.
2. For each Security Gateway, go to **Gateway Properties > Mobile Access > Authentication**.
3. Do one of these options:
   - **To use the global settings** - Select **Global settings** and the global settings are used from the **Authentication to Gateway** page of the Mobile Access tab. This is the default.
   - **To turn off two-factor authentication for the gateway** - Select **Custom Settings for this Gateway** and click **Configure**. In the window that opens, do not select the check box. This turns off two-factor authentication for this gateway.
   - **To activate two-factor authentication for the gateway with custom settings** - Select **Custom Settings for this Gateway** and click **Configure**. In the window that opens, select the check box. You must then configure custom SMS Provider Credentials for this gateway. Optionally, configure **Advanced** options.
4. Repeat step 3 to step 4 for all other gateways.
5. Install the policy. Select **Policy > Install**.

**Two-Factor Authentication per Application**

Two-factor authentication can be made a requirement for accessing particular applications. This is done by configuring a Protection Level to require two-factor authentication, and associating the Protection Level with Mobile Access applications.

**To configure two-factor authentication per application:**

1. Configure basic two-factor authentication ("Basic DynamicID Configuration for SMS or Email" on page 124).
   a) Configure the phone directory.
   b) Configure the application settings in **Mobile Access tab > Authentication**.
   c) Configure the Mobile Access Security Gateways to let the mobile devices use DynamicID.
2. Configure the Protection Level ("Defining Protection Levels" on page 37).
   - In the Mobile Access tab > Authentication, select User must successfully authenticate via SMS.
3. Assign the protection level to Mobile Access applications that require two-factor authentication (see "Using Protection Levels" on page 36).
4. Install the policy.

Changing the SMS Provider Certificates and Protocol

By default, it is recommended to use a secure (https) protocol for communication with the SMS provider. Mobile Access also validates the provider server certificate using a predefined bundle of trusted CAs.

If your SMS provider uses a non-trusted server certificate you can do one of the following:

- Add the server certificate issuer to the trusted CA bundle under $CVPNDIR/var/ssl/ca-bundle/ and run:
  $CVPNDIR/bin/rehash_ca_bundle

- Ignore the server certificate validation by editing $CVPNDIR/conf/cvpnd.C and replacing the SmsWebClientProcArgs value with ("-k").

If your SMS provider is working with the non-secure http protocol, edit the file $CVPNDIR/conf/cvpnd.C and replace the SmsWebClientProcArgs value with (""").

Two-Factor Authentication for Certain Authentication Methods

You can configure DynamicID to be enforced only if the primary authentication method was of a certain type. For example, you can configure DynamicID to be required if someone authenticates using a user name and password, but not if they use RADIUS authentication.

By default, DynamicID is enforced for all authentication types when it is configured in SmartDashboard. The default enforceSMSforAuthTypes parameter in the cvpnd.C configuration file is:

```plaintext
:enforceSMSforAuthTypes ( 
  : (USER_PASS) 
  : (CERT) 
  : (RADIUS) 
  : (SECURID) 
)
```

To enforce DynamicID only for specified authentication types, remove the authentication types for which DynamicID enforcement is not required. For example, to require DynamicID when a user authenticates with a certificate or user name and password, but not with SECURID or RADIUS authentication, edit the lines:

```plaintext
:enforceSMSforAuthTypes ( 
  : (USER_PASS) 
  : (CERT) 
)
```

DynamicID Authentication for Specific Methods and by Protection Level

If in SmartDashboard you configured a Protection Level to require two-factor authentication with DynamicID, the cvpnd.C configuration file settings override the Protection Level Authentication settings in SmartDashboard.

For example: You configured the Restrictive Protection Level to require DynamicID for Certificate authentication, but you removed CERT from the enforceSMSforAuthTypes parameter. DynamicID authentication will not be required for anyone using Certificate authentication, even when accessing an application assigned to the Restrictive Protection Level.
Multiple Realms

This feature gives support for multiple authentication realms in the Mobile Access Portal.

After installation, if you log in to the gateway portal, the login page appears as if there are no multiple realms. After you configure new realms, the login page will have a new drop-down list. Users will select the authentication realm they want to use.

Best Practice - We recommend that you:

- Open SmartDashboard and configure authentication on this realm before you continue.
- Review the built-in realms in GuiDBedit before you create a new realm.

Use GuiDBedit to add authentication realms. Open GuiDBedit on the Security Management Server, and configure each Mobile Access Security Gateway in the environment with the next procedures.

This feature is supported in R77.10 and higher.

Workflow

To use multiple authentication realms:

2. Apply configuration to Mobile Access gateways ("Applying New Realms" on page 133).
4. Optional: Configure the SMS enforcement for each authentication realm ("Two-Factor Authentication for Certain Authentication Methods" on page 130).

Creating New Realms

These instructions are for GuiDBedit. Remember to do them for all Mobile Access Security Gateways.

To add multiple realms:

1. Open Tables > Network Objects > network_objects, and select a Mobile Access Security Gateway.
2. Find the realms_for_blades field.
   - It is easiest to find by searching for ssl_vpn realm.
3. Right-click realms_for_blades and select Add.
4. Enter a name for the new realm.
   - The realm name must not include spaces.
   - When you create a new realm, you cannot use a name that is used by a built-in realm. Reserved names for authentication realms are:
     - ssl_vpn
     - vpn
     - mobile_realm
     - active_sync_realm
     - active_sync_secure_realm
5. Click OK.
   - The new authentication realm is in the realms_for_blades container.

Configuring Authentication Schemes

When you add an authentication realm, the most important property to customize is the authentication scheme. The fields of this property set the types of authentication, their order, and other basic values. For example, you can configure a realm to accept certificate authentication and username authentication, with certificates being first.
This procedure is done in GuiDBedit, after you add a new realm. Do it again for each authentication scheme that will be in the realm.

**To configure an authentication scheme:**

1. Expand `realms_for_blades` > the realm you added > `authentication`.
2. Right-click `auth_schemes` and select `Add`.
3. In the window that opens, set the basic properties of the authentication scheme.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>When you have multiple authentication schemes in one realm, this value sets the priorities. Zero (0) is first.</td>
</tr>
<tr>
<td></td>
<td>• If <code>certificate</code> authentication is included in the authentication schemes, it must be first (Index = 0).</td>
</tr>
<tr>
<td></td>
<td>• <code>SMS</code> cannot be included in the authentication schemes. Configure it in SmartDashboard. It will always be last.</td>
</tr>
<tr>
<td>Object</td>
<td>Must stay <code>realm_auth_scheme</code></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the scheme. It must not be the same name as a realm that exists and it must not include spaces.</td>
</tr>
</tbody>
</table>

4. Click `OK`. The scheme comes into view as a new object, with its default fields.
5. Right-click the `auth_scheme` field and select `Edit`.
6. Enter a display name.
7. Choose an authentication scheme.

<table>
<thead>
<tr>
<th>Field</th>
<th>If selected, follow up with:</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate</td>
<td>Make sure <code>Index</code> is 0.</td>
</tr>
<tr>
<td>defined_on_user</td>
<td></td>
</tr>
<tr>
<td>radius</td>
<td>Edit <code>radius_server</code> and select the server.</td>
</tr>
<tr>
<td>securid</td>
<td></td>
</tr>
<tr>
<td>user_pass</td>
<td></td>
</tr>
<tr>
<td>os_password, tacacs</td>
<td>Do not select these schemes. They do not work with Mobile Access.</td>
</tr>
</tbody>
</table>

8. Enter a display name.
9. If the authentication scheme is certificate, right-click `certificate_parsing_rules` and set it to `realm_certificate`.

**Defining Fetch Directories**

If you use only the built-in realms, do not define fetch directories. These are automatically generated by the configuration of each Mobile Access Software Blade. If you make changes to the `realms_for_blades` > `directory` properties, your changes will be overwritten by the built-in automatic calculations.

If you create new realms, you can define fetch directory options. When you create a new realm, the `fetch_type` attribute is set to `all` by default. During authentication, the system will try to find the user in defined directories: internal, ldap, and generic. This is recommended for most environments, but you can change it.
To change the fetch directories:

1. Open the directory field.
2. Change the value of fetch_type to fetch_options. Properties of the fetch_options attribute come into view. Each is a boolean for the user directory type.
3. Make sure the fetch_options value is realm_fetch_options.
4. Under fetch_options, set the associated fetch directory properties to true:

<table>
<thead>
<tr>
<th>Valid Value</th>
<th>Description</th>
<th>If true, do:</th>
</tr>
</thead>
<tbody>
<tr>
<td>do_ldap_fetch</td>
<td>Use LDAP user directories to lookup authentication credentials.</td>
<td>Edit ldap.au and choose the ldap account unit reference. (You can use SmartDashboard to configure a new AU.)</td>
</tr>
<tr>
<td>do_internal_fetch</td>
<td>Use user accounts defined on SmartDashboard.</td>
<td></td>
</tr>
<tr>
<td>do_generic_fetch</td>
<td>User RADIUS servers named &quot;generic&quot; for external user directories.</td>
<td>Edit radius and choose the RADIUS server.</td>
</tr>
</tbody>
</table>

5. Edit the display_string. This is the name of the authentication method that users will see. This attribute is mandatory.

**Applying New Realms**

After you create the realms and define the options for each Mobile Access Security Gateway, do this to apply the realms.

To apply new realms:

1. Save the changes.
2. Close Guibedit.
3. Open SmartDashboard.
   When the policy is installed, the gateways get the new realms and their configurations.
5. Add the new realms to the static configuration of each Mobile Access Security Gateway.

**Adding Realms to Static Configuration of Gateways**

You must configure the Mobile Access Security Gateways to complete the procedure of applying new realms. When you configure realms for the gateways, use the name of the realm that you created when you chose Add (“Creating New Realms” on page 131). Do not use the display name.

To add realms to gateway configuration:

1. In each gateway, in expert mode, run:
   ```
   [expert@hostname:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd portalRealmNames <realm_name>
   
   For example, to add a realm named my_new_realm:
   ```
   ```
   [expert@hostname:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd portalRealmNames my_new_realm
   ```
   2. Run: [expert@hostname:0]# cvpnrestart
Troubleshooting

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Cause and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <code>ssl_vpn</code> default realm is not displayed to the user.</td>
<td>If you add new realms, the default realm is not displayed as an authentication type. To use the <code>ssl_vpn</code> realm with the new realms, add it to the static configuration of the Security Gateways.</td>
</tr>
<tr>
<td>Added realms are not displayed to users.</td>
<td>Make sure the change is applied:</td>
</tr>
<tr>
<td>Users are not able to log in.</td>
<td>There may be a mismatch between realm lists on the gateways and the server.</td>
</tr>
</tbody>
</table>

Two-Factor Authentication for Certain Authentication Methods

You can configure DynamicID to be enforced only if the primary authentication method was of a certain type. For example, you can configure DynamicID to be required if someone authenticates using a user name and password, but not if they use RADIUS authentication.

By default, DynamicID is enforced for all authentication types when it is configured in SmartDashboard. The `default enforceSMSforAuthTypes` parameter in the `cvpnd.C` configuration file is:

```
:enforceSMSforAuthTypes ( : (USER_PASS) : (CERT) : (RADIUS) : (SECURID) )
```

To enforce DynamicID only for specified authentication types, remove the authentication types for which DynamicID enforcement is not required. For example, to require DynamicID when a user authenticates with a certificate or user name and password, but not with SECURID or RADIUS authentication, edit the lines:

```
:enforceSMSforAuthTypes ( : (USER_PASS) : (CERT) )
```

DynamicID Authentication for Specific Methods and by Protection Level

If in SmartDashboard you configured a Protection Level to require two-factor authentication with DynamicID, the `cvpnd.C` configuration file settings override the Protection Level Authentication settings in SmartDashboard.
Session Settings

Once authenticated, remote users are assigned a Mobile Access session. The session provides the context in which Mobile Access processes all subsequent requests until the user logs out or the session ends due to a time-out.

This section discusses Mobile Access settings and best practices for Mobile Access sessions. These settings are configured in SmartDashboard from the Mobile Access tab by selecting Additional Settings > Session.

Session Timeouts

Once authenticated, remote users work in a Mobile Access session until they log out or the session terminates. Security best practices provide for limiting the length of active and inactive Mobile Access sessions to prevent abuse of secure remote resources.

Note - Mobile Access uses the system time to keep track of session timeouts. Changing the system time may disrupt existing session timeouts. Therefore, it is recommended to change the system time during low activity hours.

Mobile Access provides two types of session timeouts, both of which are configured in SmartDashboard from the Mobile Access tab by selecting Additional Settings > Session.

- Re-authenticate users every is the maximum session time. When this period is reached, the user must log in again. The default value is 60 minutes. Changing this timeout affects only future sessions, not current sessions.

- Disconnect idle sessions after is the disconnection time-out if the connection remains idle. The default value is 15 minutes. When users connect via SSL Network Extender, this timeout does not apply.

Roaming

The Roaming option allows users to change their IP addresses during an active session.

Note - SSL Network Extender users can always change IP address while connected, regardless of the Roaming setting.

Tracking

Configure Mobile Access to log session activity, including login attempts, logouts, timeouts, activity states and license expiration warnings.

Securing Authentication Credentials

Having multiple users on the same machine accessing the Mobile Access portal can be a security hazard. A user logged in to the Mobile Access portal can open a new browser window and get the access of the earlier session. Then the user can browse directly to the Mobile Access portal without entering the login credentials again.

To make sure authentication credentials are not stolen by others, recommend to users that they log off or close all browser windows when done using a browser.
**Simultaneous Logins to the Portal**

Having a single user logged in to Mobile Access more than once, from two different locations for example, is a potential security issue.

Simultaneous login prevention enables a gateway to automatically disconnect a remote user who is logged more than once.

When simultaneous login prevention is enabled, and a user's authentication information used to log in from two different computers, only the later login is considered legitimate, and the earlier session is logged out.

**Configuring Simultaneous Login Prevention**

Simultaneous login prevention is configured in SmartDashboard from the Mobile Access tab by selecting Additional Settings > Session.

The options are:

- **User is allowed several simultaneous logins to the Portal**
  - Simultaneous login detection is disabled. This is the default option.

- **User is allowed only a single login to the portal**
  - Inform user before disconnecting his previous session not selected
  - The earlier user is disconnected and the later user is allowed. The earlier user is logged out. For Mobile Access portal users, the following message appears: "Your Mobile Access session has timed out. would you like to sign in again now?". The later user is not informed that an earlier user is logged in.

- **User is allowed only a single login to the portal**
  - Inform user before disconnecting his previous session selected
  - The later user is informed that an earlier user is logged in, and is given the choice of canceling the login and retaining the existing session, or logging in and terminating the existing session. If the existing session is terminated, the user is logged out with the message: "Your Mobile Access session has timed out. would you like to sign in again now?".

**Tracking of Simultaneous Logins**

To track simultaneous login events, select All Events in the Tracking section of the Additional Settings > Session page.

When the gateway disconnects a user, the gateway records a log of the disconnection, containing the connection information of both logins.

All disconnect and connect events create a corresponding entry in the traffic log. The following values of the authentication status field relate to simultaneous logins:

- **Success** - User successfully logged in. Existing active sessions were terminated.
- **Inactive** - User successfully authenticated, but existing sessions need to be terminated prior to logging on.
- **Disconnected** - An existing user session has been terminated because the same user has logged on to another session.

**Simultaneous Login Issues**

The following issues may arise in connection with simultaneous login:

**Endpoint Connect- Simultaneous Login Issues**

For Endpoint Connect users, Mobile Access does not prevent simultaneous login. This is equivalent to the **User can have several simultaneous logins to the portal** option. An Endpoint Connect user cannot log out another user with the same user name, and cannot be logged out by another user with the same user name.
SecureClient Mobile - Simultaneous Login Issues

With User can have only a single simultaneous login to the portal selected and Inform user before disconnecting previous sessions not selected SecureClient Mobile users can be logged off by another user, and can log off other users.

However, the Inform user before disconnecting his previous session option does not work, because no message can be sent to those users. User can be logged off, but cannot log off other users.

Other Simultaneous Login Issues

1. When a session is disconnected by another user and SSL Network Extender application mode client is being used, the SSL Network Extender window remains open, while the session is disconnected.
   Similarly, when a session is disconnected by another user and Secure Workspace is being used, Secure Workspace remains open, while the session is disconnected.

2. When a session is disconnected by another user and Citrix is being used, the Citrix window remains open, while the session is disconnected.

3. All current sessions are deleted when changing the section from User can have only a single login to the Portal to User is allowed several simultaneous logins to the Portal.
Chapter 10

Endpoint Security On Demand

In This Section:

- Endpoint Compliance Enforcement ................................................................. 138
- Configuring Endpoint Compliance ................................................................. 141
- Endpoint Compliance Scanner End-User Workflow ........................................ 149
- Completing the Endpoint Compliance Configuration ...................................... 150
- Secure Workspace ............................................................................................ 151
- Endpoint Compliance Updates .......................................................................... 164

Endpoint Compliance Enforcement

The Check Point Endpoint Security On Demand scanner enforces endpoint compliance by scanning the endpoint to see if it complies with a pre-defined endpoint compliance policy. For example, an endpoint compliance policy would make sure that the endpoint client has updated Anti-Virus and an active firewall. If the endpoint is compliant with the endpoint compliance policy, the user is allowed to access the portal.

By ensuring that endpoints comply with a security policy, Endpoint Security On Demand protects enterprises from threats emanating from unsecured endpoint computers that can result in data loss and excessive bandwidth consumption.

The endpoint compliance policy is made up of rules. A policy can specify, for example, that the endpoint machine must have an approved Anti-Virus application, and that it must be free of spyware. A policy could also specify that a machine must be managed by the organization in order to gain full access to internal data and applications.

On gateways of version R71 and higher, a combination of Endpoint Compliance Policy and Secure Workspace Policy can require the following Policy: Any client connecting to the gateway from a machine that is not managed by the organization or that does not meet a specific enforcement policy, must use Check Point Secure Workspace. This ensures that no unauthorized information is accessed.

**Endpoint Compliance Policy Granularity**

The administrators can make compliance with a policy a requirement for accessing either the portal or specific applications. This makes it possible to assign varying levels of security clearance to the portal and to Mobile Access applications.

Endpoint Compliance policies can be assigned to Mobile Access gateways. They can also be assigned to Protection Levels, which are in turn associated with Mobile Access applications.

- If an Endpoint Compliance policy is assigned to a gateway, endpoint machines must comply with the policy before they are allowed to log in to the portal.
- If an endpoint machine does not comply with the Endpoint Compliance policy on a gateway, users can be required to use Check Point Secure Workspace. This is possible on gateways of version R71 and higher.
- To provide additional protection to an application, it is possible to "harden" the Endpoint Compliance protection that is enforced by the gateway by assigning an Endpoint Compliance policy to a Protection Level, and then assigning that Protection Level to an application.

In order to access that application, the endpoint machine must comply with the policy associated with the Protection Level, in addition to the policy associated with the gateway.

In either case, the scan takes place before logging in to the portal. Only one scan is performed. Compliance to policies is determined according to the results of the scan.
**Endpoint Compliance Policy Rule Types**

There are different types of Endpoint Compliance policy rules, for different types of security applications. It is possible to have multiple rules of the same type, each with different settings.

**Windows Security Rule**

Windows security rules perform Windows-specific checks. For example:

- Check for the latest Windows Service Pack on endpoint.
- Check the enabled/disabled state of the built-in Microsoft Windows Automatic Updates system.
- Check for Microsoft Windows Hotfixes and patches on the endpoint.
- Enforce Windows patches by their ID.

Endpoint computers running Windows must pass these checks in order to gain access to the network.

At least one of the Hotfixes in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

**Anti-Spyware Application Rule**

Choose which Anti-Spyware applications endpoint computers (on the Windows platform) must have to gain access to the network.

Ensure that appropriate Anti-Spyware software is running on endpoint computers, and that the software version and virus signature files are up-to-date.

At least one of the Anti-Spyware applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Anti-Spyware enforcement rules are pre-configured with supported anti-spyware providers. To require a non-supported Anti-Spyware provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

**Anti-Virus Application Rule**

Choose which Anti-Virus applications the endpoint computer must have in order to gain access to the network.

Ensure that appropriate Anti-Virus software is running on endpoint computers, and that the software version and virus signature files are up-to-date.

At least one of the Anti-Virus applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Anti-Virus enforcement rules are pre-configured with supported Anti-Virus providers. To require a non-supported anti-virus provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

**Firewall Application Rule**

Choose which personal firewall applications endpoint computers (on Windows, Linux or Macintosh platforms) must have to gain access to your network.

Ensure that appropriate firewall software is installed, enabled and running on endpoint computers.

At least one of the firewall applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.
For convenience, firewall enforcement rules are pre-configured with supported firewall providers. To require a non-supported firewall provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

**Custom Check Rule**

Perform custom checks on endpoint computers (on the Windows, Linux or Macintosh platforms) that are not covered by any of the other rule types. For example:

- Custom applications. These applications may include proprietary spyware scanners that supplement the predefined types and/or other special security solutions.
- Specific files.
- Registry keys or processes running on the endpoint computer.
- Non-English or localized names of processes and files.

Custom check rules can be configured to check for specific versions and modification dates.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule, and the error message that is presented to users in the event of non-compliance, such as remediation information.

**OR Group of Rules**

An "OR Group of Rules" rule includes a list of previously defined rules. An endpoint satisfies a rule of type "OR Group of Rules" if it satisfies one or more of the rules included in the "OR Group of Rules" rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

**Spyware Scan Rule**

Select the action that should take place for each type of spyware present on endpoint computers. You can change the protections for types of spyware threats.

<table>
<thead>
<tr>
<th>Spyware Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialer</td>
<td>Software that change the user’s dial-up connection settings so that instead of connecting to a local Internet Service Provider, the user connects to a different network, usually a toll number or international phone number.</td>
</tr>
<tr>
<td>Worm</td>
<td>Programs that replicate over a network for the purpose of disrupting communications or damaging software or data.</td>
</tr>
<tr>
<td>Keystroke Logger</td>
<td>Programs that record user input activity (keystrokes or mouse activity). Some keystroke loggers transmit the recorded information to third parties.</td>
</tr>
<tr>
<td>Hacker Tool</td>
<td>Tools that facilitate unauthorized access to a computer and/or extraction of data from a computer.</td>
</tr>
<tr>
<td>Remote Administration Tool</td>
<td>Commercially developed software that allows remote system access and control.</td>
</tr>
<tr>
<td>Trojan</td>
<td>Malicious programs that masquerade as harmless applications.</td>
</tr>
<tr>
<td>Adware</td>
<td>Programs that display advertisements or record information about Web use habits and forward it to marketers or advertisers without the user’s authorization or knowledge.</td>
</tr>
<tr>
<td>Other</td>
<td>Any unsolicited software that secretly performs undesirable actions on a user’s computer and does not fit any of the above descriptions.</td>
</tr>
</tbody>
</table>
Spyware Type | Description
---|---
Screen Logger | Software that record what a user's monitor displays.
Tracking Cookie | Cookies that are used to deliver information about the user's Internet activity to marketers.
Browser Plug-in | Software that modifies or adds browser functionality. Browser plug-ins change the default search page to a pay-per-search site, change the user's home page, or transmit the browser history to a third party.

You define an exception list of spyware software (see "Excluding a Spyware Signature from a Scan" on page 148). For example, you can allow that a signature that is recognized as spyware by Mobile Access, but which you see as legitimate.

In the rule, set the action to take if an endpoint computer fails to comply. Set the error message that users see in the event of non-compliance, such as remediation information.

**Endpoint Compliance Logs**

If the end user machine is not compliant with one or more of the Endpoint Compliance policy rules, Mobile Access generates Endpoint Compliance-specific logs with the category “Endpoint Security on Demand” (Endpoint Security On Demand). The log entries appear in SmartView Tracker, and include the:

1. Rule ID and name that causes the authorization failure.
2. Policies that this rules belongs to.

   ![Note] - Mobile Access logs non-compliant rules from all policies, not only the Endpoint Compliance policy that is assigned to the gateway or to an application. This means that there may be entries in SmartView Tracker for rules that do not appear in the report presented to the end user.

3. A description in the “info” field of the log. Two logging levels are available to the administrator: (For configuration details, see Configuring Endpoint Compliance Logs (on page 147).)
   - **Summary**: only one log entry per scan is written to SmartView Tracker. The log entry shows endpoints that do not comply with the Endpoint Compliance policy. The date and time of the scan, the source IP, and the Endpoint Compliance scan ID are logged.
   - **Details**: In addition to the Summary mode information, this adds a log entry for each non-compliant rule. For example, in the case of a Spyware Scan rule that screens for tracking cookies, a log entry is generated that contains the following fields:
     - Malware name: unwantedexample.
     - Malware type: 3rd party cookie.
     - Description: symptom type: URL. Symptom value: cookie: bob@unwantedexample.net.

**Configuring Endpoint Compliance**

The workflow for configuring Endpoint Compliance enforcement is below. Each step is described in detail in the sections that follow:

1. **Plan the Endpoint Compliance Policy**
   Decide on security clearance levels for Mobile Access portals and applications. For example, is it OK for users to gain access to all Mobile Access applications as long as they comply with a single policy? If some resources are more sensitive than others, you may wish to draw up a more stringent policy for some applications than for others.

2. **Use the ICSInfo Tool**
   Set up a stand-alone test computer with all the endpoint security applications you want to create enforcement rules for, and the run the ICSInfo tool to obtain the information needed to correctly define Endpoint Compliance policy rules.
3. **Create Endpoint Compliance Policies**
   Policies are made up of rules. In order to comply with the policy, endpoints must comply with all rules in the policy. Rules can be used in more than one policy. Rules that are not in a policy are not used.
   There are different types of rules for different security applications. The Endpoint Compliance policy configuration tool comes with a number of predefined rules which can be edited to match the needs of the organization.

4. **Configure Endpoint Compliance Settings for Applications and Gateways**
   Configure which Endpoint Compliance Policies should be assigned to which applications and gateways.
   - To make access to the portal conditional on passing an Endpoint Compliance scan, assign a policy to a gateway.
   - To make access to applications conditional on passing an Endpoint Compliance scan:
     - Assign a policy to a Protection Level.
     - Assign Protection Levels to Mobile Access applications.

5. **Complete the Endpoint Compliance Configuration**
   Configure tracking options for the endpoint scan results, then save and install the security policy

---

**Planning the Endpoint Compliance Policy**

Defining the Endpoint Compliance policy for Mobile Access clients involves some planning, prior to performing the SmartDashboard configuration.

You need to define security clearance levels for the both the Mobile Access portal (that is, the gateway) and for portal applications. There are various approaches, and the best one to use depends on how granular you need to make the policy.

**Basic Approach:**

The simplest approach is to define a single Endpoint Compliance policy for the gateway and all applications accessed via the gateway. In this approach, all applications accessed via the gateway are protected by the Endpoint Compliance policy of the gateway. Users whose client machines comply with the policy have access to the portal and all applications.

For example:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Endpoint Compliance Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway A</td>
<td>Low Security</td>
</tr>
<tr>
<td>Web App P</td>
<td>Rely on gateway requirements</td>
</tr>
<tr>
<td>Web App Q</td>
<td>Rely on gateway requirements</td>
</tr>
<tr>
<td>File Share R</td>
<td>Rely on gateway requirements</td>
</tr>
</tbody>
</table>

**Advanced Approach:**

A more advanced approach is appropriate if there is one application (or a small number of applications) that has stricter security requirements than other applications. These additional requirements are specified in a separate Endpoint Compliance policy, which is enforced in addition to the gateway policy. To access the Mobile Access portal, all users must fulfill the threshold security requirements of the gateway policy. Users clicking a link in the portal to an application with additional security requirements are only allowed access to the application if they fulfill those additional requirements.
For example:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Endpoint Compliance Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway A</td>
<td>Low Security</td>
</tr>
<tr>
<td>Web App P</td>
<td>Rely on gateway requirements</td>
</tr>
<tr>
<td>Web App Q</td>
<td>High Security</td>
</tr>
<tr>
<td>File Share R</td>
<td>Rely on gateway requirements</td>
</tr>
</tbody>
</table>

**Very Advanced Approach:**

Where most or every application has its own endpoint security requirements, it is possible to define an individual Endpoint Compliance policy for each application. In this scenario, there are no gateway security requirements: All users are able to access the portal. However, when clicking a link to an application, users are only allowed access if they fulfill the requirements for that application. If no requirements are configured for the application, users are allowed to access it.

For example:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Endpoint Compliance policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway A</td>
<td>None</td>
</tr>
<tr>
<td>Web App P</td>
<td>Low Security</td>
</tr>
<tr>
<td>Web App Q</td>
<td>High Security</td>
</tr>
<tr>
<td>File Share R</td>
<td>Medium Security</td>
</tr>
</tbody>
</table>

**Example Rules for Endpoint Compliance Policies**

The following table illustrates Endpoint Compliance policies with different rules, for different security requirements.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default Windows Security rule</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Anti-Virus applications check</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Firewall applications check</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Spyware Scan rule</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Using the ICSInfo Tool**

When defining Endpoint Compliance policy rules, you must use the correct format. This format varies from vendor to vendor. The ICSinfo.exe utility scans your computer, and generates an xml file that gives you the information in the correct format for all supported security programs it finds.

Run ICSinfo before configuring the Endpoint Compliance policy rules.
To use the ICSinfo.exe utility:

1. Set up a stand-alone test computer with all the endpoint security applications you want to create enforcement rules for. Be sure to apply the latest updates to your security software.
2. Copy the ICSinfo tool from the Mobile Access gateway to the test computer. The tool is located at $CVPNDIR/htdocs/ICS/components/ICSinfo.exe.
3. Run ICSinfo.exe. This utility lists all detected security software, along with the required information in the correct format. The xml format output file ICSinfo.xml can be viewed in a browser. The sections of the file can be collapsed or expanded by clicking the - or +.
4. Record the information for each security program and use this information to create your Endpoint Compliance policy rules.

Creating Endpoint Compliance Policies

To create Endpoint Compliance policies, you define rules, and then assign the rules to a policy. There are different types of rules for different security applications. The Endpoint Compliance policy configuration tool comes with a number of predefined rules which can be edited to match the needs of the organization.

To configure Endpoint Compliance policies:

1. From the SmartDashboard Mobile Access tab navigation tree, select Endpoint Security On Demand > Endpoint Compliance. The Endpoint Compliance page appears.
2. Click Edit policies. The Endpoint Compliance policy configuration tool opens at the Policies page.
3. Either create a new Endpoint Compliance policy or edit an existing policy.
   b. To edit an existing policy, select the policy and click Edit. The Policies > Edit Policy page opens.
4. Give the policy a Name, and a Description. The description can be long and detailed.
5. This step applies only to Endpoint Compliance policies that include Spyware Scan rules (Note that a Spyware Scan rule is different from an Anti-Spyware rule):
   If an endpoint machine has a valid Anti-Spyware of Anti-Virus application, you may consider they do not need to undergo an Endpoint Security On Demand Spyware Scan. If that is the case, select Bypass malware scan if endpoint meets Anti-Virus or Anti-Spyware requirements.
      Note - This option is disabled if there is no Spyware Scan rule in the policy.
6. Within a Policy, either add previously defined Endpoint Compliance rules, or create new rules or edit previously defined rules. There are different types of rules for different security applications. It is possible to have multiple rules of the same type, each with different settings.
   a. To add a previously defined rule, click Add. The Add Enforcement Rules page opens. Select a rule and click OK.
   b. To create a rule, click New Rule, and select the rule type
   c. To edit a previously defined rule, select the rule and click Edit.
7. Define the rules.
      Note - For explanations of fields in the Endpoint Compliance rules, see the online help.
8. Click OK. This takes you back to the Edit Policy or the New Policy page.
9. Click OK. This takes you back to the Policies page.
10. Click OK. This completes the configuration of the Endpoint Compliance Policies, and takes you back to the Endpoint Security On Demand > Endpoint Compliance page.

After the Endpoint Compliance policies are configured, Endpoint Compliance settings can be configured to make use of the policies.
**Configuring Endpoint Compliance Settings for Applications and Gateways**

The Endpoint Compliance scanner performs a scan on the endpoint computer when the user connects to a Mobile Access portal. Mobile Access enforces the Endpoint Compliance policy, and allows access to the Mobile Access portal applications according to the Endpoint Compliance policy.

**To configure Endpoint Compliance:**

2. In the Endpoint Security Settings on Mobile Access Gateways section, select a gateway and click Edit.
   The Endpoint Compliance page of the Mobile Access Properties window opens.
3. Enable Scan endpoint machine when user connects.
4. Choose one of the following approaches:
   - Basic Approach: Configuring a Common Policy for the Portal and all Applications (on page 145)
   - Advanced Approach: Configuring a Threshold Policy for the Portal, Hardened for Specific Applications (on page 145)
   - Very Advanced Approach: Configuring Individual Policies for Each Application (on page 146)

**Basic Approach: Configuring a Common Policy for the Portal and all Applications**

To make access to the portal and all applications conditional on passing an Endpoint Compliance scan, assign a policy to the gateway:

1. Enable the Threshold policy to access any application via this gateway, the endpoint must comply with the following policy option.
2. From the drop-down list, select the Endpoint Compliance policy to be used for all applications accessed via this gateway.
3. Click OK.
   This takes you back to the Endpoint compliance page.
4. Maintain all applications with their default Endpoint compliance settings. In the Additional Settings > Protection Level page of the application, ensure This application relies on the security requirements of the gateway is selected.
5. Continue with Configuring Endpoint Compliance Logs (on page 147).

**Advanced Approach: Configuring a Threshold Policy for the Portal, Hardened for Specific Applications**

To configure the threshold Endpoint Compliance policy for the portal, hardened for specific Mobile Access applications, define a policy for the gateway. Then, for applications that require hardened endpoint security, assign a Protection Level to the application.

1. In the Endpoint Compliance page of the gateway, enable the Threshold policy: to access any application via this gateway, the endpoint must comply with the following policy option.
2. From the drop-down list, select the default Endpoint Compliance policy to be used for applications accessed via this gateway.
3. Click OK.
4. In the Mobile Access tab Endpoint Compliance page, select the application that requires hardened endpoint security and click Edit.
   The Mobile Access application opens at the Additional Settings > Protection Level page. (Mobile Access applications are defined in the Applications section of the Mobile Access tab.)
5. Select the second option (This application has additional...).
6. From the drop-down list, select a Protection Level for this application.
   To define a new Protection Level, click Manage and define the protection level ("Defining Protection Levels" on page 37).
7. Click OK.
8. Continue with Configuring Endpoint Compliance Logs (on page 147).

Very Advanced Approach: Configuring Individual Policies for Each Application

It is possible to configure an individual policy for each application. In this scenario, there are no gateway security requirements: All users are able to access the portal. However, when clicking a link to an application, users are only allowed access if they fulfill the requirements for that application. If no requirements are configured for the application, users are allowed to access it.

To configure an individual policy for each application:
1. In the Endpoint Compliance page of the gateway, enable the No threshold option.
2. Click OK.
3. In the Mobile Access tab Endpoint Compliance page, select the application that requires hardened endpoint security.
4. Click Edit.
   The Mobile Access application opens at the Additional Settings > Protection Level page. (Mobile Access applications are defined in the Applications section of the Mobile Access tab.)
5. Select the second option (This application has additional...), and from the drop-down list, select a Protection Level with the required Endpoint compliance policy for this application.
6. To define a new Protection Level, click Manage and define the protection level ("Defining Protection Levels" on page 37).
   Note - If This application relies on the security requirements of the gateway is selected for the Mobile Access application, users are allowed to access the application without any Endpoint Compliance requirements.
7. Repeat steps step 3 to step 5 for all Mobile Access applications that require hardened endpoint security.
8. Click OK.

Configuring Advanced Endpoint Compliance Settings

You can edit the Advanced Endpoint Compliance Settings to configure whether or not to allow access to the gateway and applications if the Endpoint Compliance scanner is not supported on the endpoint operating system.

- In the Endpoint Security On Demand > Endpoint Compliance page, click Edit.
  The Advanced Endpoint Compliance Settings window opens.
  In this window you can decide whether or not to allow access to the gateway and applications if the Endpoint Compliance scanner is not supported on the endpoint operating system.

The Endpoint Compliance scanner supports the following operating systems: Windows, Mac, and Linux.

Configuring Platform-Based Bypass Per OS

If you want to allow some endpoint operating systems to bypass Endpoint Compliance requirements, you must select the Allow access option in the Advanced Endpoint Compliance Settings window.

For details, see the operating system compatibility table in the Mobile Access Release Notes.

To configure different rules on endpoints with different operating systems, see SecureKnowledge solution sk34989 (http://supportcontent.checkpoint.com/solutions?id=sk34989).

Platform-Based Bypass Per Protection Level

Configuring Endpoint Compliance Settings per Protection Level lets you set Platform-Based Bypass per application.
By default all Advanced Endpoint Compliance Settings are taken from the SmartDashboard configuration, in the Advanced Endpoint Compliance Settings page.

**Enabling Platform Based Bypass per Protection Level**

To configure different access permissions for various Protection Levels for Endpoint Compliance scanning, run:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C set useICSRelaxedModeInProtectionLevel true
```

To return to the default setting, change `true` to `false` in the above command.

**Configuring the Protection Levels that are Bypassed**

In the Mobile Access tab of SmartDashboard, under **Additional Settings > Protection Levels**, is a list of Protection Levels. From this page you can edit the Authentication and Endpoint Security settings that are required for applications assigned to each Protection Level. You can also create new Protection Levels.

In the Mobile Access application properties, assign a Protection Level to an application. For example, if you want to allow access to an application only if the user is compliant with Endpoint Compliance policy1, but you also need to accommodate the user connecting from an endpoint that does not support Endpoint Compliance scanning (such as an iPhone), then:

1. Create or use a Protection Level named ESOD_Relaxed_PL which enforces Endpoint Compliance Policy policy1.
2. Assign the Protection Level to the application.
3. Configure the Protection Level as "Bypassed".

To configure different access permissions for various Protection Levels for Endpoint Compliance, from the Mobile Access CLI, in expert mode, run:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd ICSRelaxedModeProtectionLevelNames ESOD_Relaxed_PL
```

You can add other Protection Levels as well.

**To restore a Protection Level from being "Bypassed", for Endpoint Compliance:**

1. Run:

   ```
cvpnd_settings $CVPNDIR/conf/cvpnd.C listRemove ICSRelaxedModeProtectionLevelNames
```

2. Follow the on-screen instructions.

**To finalize the configuration of granular platform-based bypass for Endpoint Security On Demand:**

1. Restart the Mobile Access services by running `cvpnrrestart`.
   - If the Mobile Access gateway is part of a cluster, be sure to make the same change on each cluster member.
2. In SmartDashboard, assign the Protection Levels to the applications.
3. Install the policy.

**Configuring Endpoint Compliance Logs**

Mobile Access generates Endpoint Compliance-specific logs. The logs can be viewed using SmartView Tracker, and have the category "Endpoint Security On Demand" (abbreviated in the log entry as "Endpoint Security on Demand"). The Endpoint Security On Demand information can be found on the "info" field of the logs.

For more information, see Endpoint Compliance Logs (on page 141).

**To configure tracking options for the Endpoint Compliance scanner:**

1. In the Mobile Access tab of SmartDashboard, select **Endpoint Security On Demand > Endpoint Compliance** from the navigation tree.
In the Endpoint Compliance page, in the Tracking section, enable Log the endpoint scan results to record the results of Endpoint Compliance scans to the log. Select Details or Summary to determine the level of detail to record in the log file.

The Tracking options are:

- **Summary**: only one log entry per scan is written to SmartView Tracker. The log entry shows endpoints that do not comply with the Endpoint Compliance policy. The date and time of the scan, the source IP, and the Endpoint Compliance scan ID are logged.

- **Details**: in addition to the Summary mode information, this adds a log entry for each non-compliant rule.
  For example, in the case of a Spyware Scan rule that screens for tracking cookies, a log entry is generated that contains the following fields:
  a) Malware name: unwantedexample.
  b) Malware type: 3rd party cookie.
  c) Description: symptom type: URL. Symptom value: cookie: bob@unwantedexample.net.

### Assign Policies to Gateways and Applications

**To assign policies to gateways:**

2. Edit any gateway whose access will be conditional on passing an Endpoint Compliance scan. Choose the Threshold policy and select Scan the endpoint machine when a user connects.

**To assign policies to applications:**

1. To make access to applications conditional on passing an Endpoint Compliance scan, assign a policy to a Protection Level.
2. Assign Protection Levels to Mobile Access applications.

### Excluding a Spyware Signature from a Scan

It is possible to exclude a specific spyware from a scan so that its presence on an endpoint computer does not cause the computer to fail the scan. Obtain the name of the spyware signature from a scan report and then modify the Endpoint Compliance policy to exclude that signature.

**To exclude a spyware signature from a scan:**

1. Configure Mobile Access so that endpoint computers must undergo an Endpoint compliance scan before they connect. The Endpoint Compliance policy must include a Spyware Scan rule.
2. Set up a stand-alone test computer that has the spyware to be excluded from the scan.
3. Run an Endpoint compliance scan on the test computer by connecting from it to Mobile Access.
   When Endpoint Security On Demand detects the spyware (irrespective of the action configured in the Spyware Scan rule), the name of the spyware (something like Win32.megaspy.passwordthief) is included in the report.
4. Make a note of the name of the spyware.
5. Open SmartDashboard.
7. Click Edit Policies.
8. Select the policy that is applicable to the clients, and click Edit.
9. Select the Spyware Scan rule from the list and click Edit.
10. In the Software exception list section, click Add.
11. Type the Name of the spyware obtained in step 3, and a Description.
12. Click OK three times to close the Endpoint Compliance policy editor.
13. Install the policy (Policy > Install).
Preventing an Endpoint Compliance Scan Upon Every Login

By default, the end user computer is scanned by the Endpoint Compliance scanner every time the user logs in. This is the default, and most secure configuration.

It is possible to configure Mobile Access so that after logging in, the user is not scanned, even after logging in again, until the end of a timeout period.

For configuration details, see sk34844 (http://supportcontent.checkpoint.com/solutions?id=sk34844).

Endpoint Compliance Scanner End-User Workflow

The Endpoint Compliance scanner on endpoint computers is supported on browsers that run ActiveX (for Windows with Internet Explorer), or Java.

When using the Endpoint Compliance scanner with Internet Explorer, the browser must be configured to download and run ActiveX controls and to allow Active Scripting. This section explains how to configure Internet Explorer to ensure that the Endpoint Compliance scanner will install and run properly on the endpoint computer.

To configure Internet Explorer for the Endpoint Compliance scanner:

1. Select Tools > Internet Options from the Internet Explorer menu.
2. Select the Security tab.
3. Select the Web content zone used by the endpoint computer for remote connections from the Security Settings window.
4. Click Custom Level.
5. Enable the following options in the Security Settings window and then click OK:
   - Download signed ActiveX controls
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked as safe for scripting
   - Active scripting
6. Select the Privacy tab. Select the Medium setting and then click Advanced.
7. Enable Override automatic cookie handling and then enable Accept in the 1st party cookies section.
8. Click OK.

Endpoint Compliance Scanner End-User Experience

When a user connects to a portal where the Endpoint Compliance is enabled, the end user computer is scanned before the user sees the login screen.

Note - The Endpoint Compliance scan starts if Endpoint compliance is configured for a Mobile Access application in a portal, even if portal access does not require compliance with a policy.

The Endpoint Compliance Scanner is installed on the endpoint machine, by using ActiveX (for Windows with Internet Explorer), or Java (see “First time Installation of ActiveX and Java Components” on page 15).

To login to the Mobile Access Portal with the Endpoint Compliance scanner enabled:

1. Enter the Mobile Access Portal URL in your browser.
2. If using the Endpoint Compliance scanner for the first time on a particular endpoint computer, you are prompted to download and install the Check Point Deployment Agent ActiveX or Java control. Some warnings may appear, regarding the Mobile Access site server certificate, and the downloaded applet.
3. During the scan, a progress bar is displayed.
4. If the endpoint computer successfully passes the Endpoint compliance scan, the Mobile Access Portal login screen appears.
   - If the endpoint computer fails to pass the scan, Endpoint Security On Demand displays a result screen showing the potentially harmful software and security rule violations detected during the scan.
• Click on a potentially harmful software item to display a short description of the detected malware, what it does and recommended removal method(s).
• If the Continue Anyway button appears, you can continue and log on to the Mobile Access Portal without removing the malware or correcting the security rule violation.
• If there is no Continue Anyway button, you must remove the detected malware or correct the security rule violation before you can log on to the Mobile Access Portal. When you have corrected the problem, click Scan again to repeat the scan.

5. When the Mobile Access Portal login page appears, you can log on normally.

Note - The user and administrator see the scan results as log entries in the Traffic Log. Each entry shows the user name, user group, source computer, malware name, malware type, and malware description.

Using Endpoint Security On Demand with Unsupported Browsers

Endpoint Security On Demand for Mobile Access requires browsers that support ActiveX or Java.

The following sections describe Endpoint Security On Demand behavior when users attempt to access the Mobile Access Portal using an unsupported browser.

• If the Block access to all applications option on the Endpoint compliance scan Policy page is enabled and either of the following conditions exist, the endpoint computer cannot connect to the Mobile Access Portal.
  • The Prevent Connectivity option is enabled for at least one malware protection rule.
  • The Restrict action is selected for at least one enforcement rule (anti-virus or custom).

In this case, Endpoint Security On Demand presents an error message and generates a log entry in the administrator's traffic log.

• In all other cases, users can log on to the Mobile Access Portal without passing an Endpoint compliance scan. In some cases, an incompatibility message appears with a Continue button that allows users to proceed with Mobile Access login. Endpoint Security On Demand generates a log entry in the administrator’s traffic log.

• When an application's Protection Level is configured to require an Endpoint Compliance scan, users can still gain access to the Mobile Access Portal, but cannot run that application.

Preventing Portal Access with Unsupported Browsers

The following steps can prevent users using unsupported browsers from gaining access to the Mobile Access Portal and applications without passing an Endpoint Compliance scan:

• Enable the Scan endpoint machine when user connects option, and set a threshold policy. This setting is found on the Endpoint Security On Demand > Endpoint compliance page.

• Assign Protection Levels that require passing an Endpoint Compliance scan to all applications.

• Prevent users from using an unsupported browser to access the Mobile Access portal by forcing Endpoint Security On Demand to reject all connections from unsupported browsers. Do this by manually editing a Mobile Access configuration file as follows:
  On the Mobile Access gateway, in the SCVPNDIR/conf/cvnd.C file, set the useMagicBrowser parameter to 'false'.

Completing the Endpoint Compliance Configuration

After completing the Endpoint Compliance configuration, take an overall view of the configuration by looking at the Endpoint Security On Demand > Endpoint Compliance page of the Mobile Access tab.

The Endpoint Compliance page shows:

• Number of Mobile Access gateways configured to scan endpoint machines.
• Security policy required on the gateway.
- Number of Mobile Access applications, with Level of Enforcement (full, partial, or none).
If this is correct for your organization, save and install the policy.

Secure Workspace

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the "real" workspace.

No data is allowed to leave this secure environment except through the Mobile Access portal. Also, Secure Workspace users cannot access any applications, files, system tools, or other resources from the virtual workspace unless they are explicitly permitted by the Secure Workspace policy.

Administrators can easily configure Secure Workspace policy to allow or prevent activity according to enterprise requirements.

Secure Workspace creates an encrypted folder called My Secured Documents on the virtual desktop that contains temporary user files. It deletes this folder and all other session data when the session terminates.

After enabling Secure Workspace, administrators can configure a gateway to either require all users to connect to the Mobile Access portal via Secure Workspace, or to give users the option of connecting via Secure Workspace or from their endpoint computers.

Enabling Secure Workspace

To enable Secure Workspace for a Mobile Access gateway:

2. To configure the Secure Workspace policy, click Edit policy.
   For details, see Configuring the Secure Workspace Policy (on page 157).
3. Select the Mobile Access gateway and click Edit.
   The Secure Workspace page of the Mobile Access gateway opens.
4. To enable Secure Workspace on the gateway, select This gateway supports access to applications from within the Secure Workspace.
5. Select any of the following options to choose the behavior of Secure Workspace when a user logs in to the Mobile Access portal:
   - Allow user to choose whether to use Check Point Secure Workspace
   - Users must use Check Point Secure Workspace
   - User must use Check Point Secure Workspace only if the following Endpoint Compliance policy is not satisfied - This option allows you to set a rule that if a certain Endpoint Compliance policy is not satisfied by the client connecting to the gateway, the client must use Secure Workspace. If the Endpoint Compliance policy is satisfied, using Secure Workspace is optional. This option is available on Security Gateways of version R71 or higher.
     - Select the Endpoint Compliance Policy that should be enforced on the gateway. If the criteria of the selected policy are not satisfied, the client connecting must use Secure Workspace.
6. Install the policy.

Configuring Advanced Secure Workspace Settings


In this window you can decide whether or not to allow access to the gateway and applications if Secure Workspace is not supported on the endpoint operating system.

To configure advanced operating system-specific settings, see sk34989 (http://supportcontent.checkpoint.com/solutions?id=sk34989).
Configuring Platform-Based Bypass Per OS in Secure Workspace

If you want to allow some endpoint operating systems to bypass Secure Workspace requirements, you must select the **Allow access** option in the **Advanced Secure Workspace Settings** window.

To configure different rules on endpoints with different operating systems, see sk34989 (http://supportcontent.checkpoint.com/solutions?id=sk34989).

Platform-Based Bypass Per Protection Level in Secure Workspace

Configuring Secure Workspace Settings per Protection Level allows you to configure “Platform-Based Bypass” per application.

By default all Advanced Secure Workspace Settings are taken from the SmartDashboard configuration, in the Advanced **Secure Workspace Settings** page.

Enabling Platform Based Bypass per Protection Level

To configure different access permissions for various Protection Levels for Secure Workspace, from the CLI run:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C set useISWRelaxedModeInProtectionLevel true
```

To return to the default setting, change `true` to `false` in the above command.

Configuring the Protection Levels that are Bypassed

In the Mobile Access tab of SmartDashboard, under **Additional Settings > Protection Levels**, is a list of Protection Levels. From this page you can edit the Authentication and Endpoint Security settings that are required for applications assigned to each Protection Level. You can also create new Protection Levels. If you select, **Applications using this protection level can only be accessed from within Check Point Secure Workspace**, all applications assigned to that Protection level will only be accessed from within Secure Workspace.

However, if you want to allow access to an application only from Secure Workspace, but you also need to accommodate the user connecting from an endpoint that does not support Secure Workspace (such as an iPhone), then:

1. Create or use a Protection Level named ESOD_Relaxed_PL which enforces Endpoint Compliance Policy policy1.
2. Assign the Protection Level to the application.
3. Configure the Protection Level as “Bypassed”.
   - To configure different access permissions for various Protection Levels for Secure Workspace, from the Mobile Access CLI, in expert mode, run:

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C listAdd ISWRelaxedModeProtectionLevelNames ESOD_Relaxed_PL
```

You can add other Protection Levels as well.
Restoring a Protection Level from being Bypassed for Secure Workspace

1. Run:
   ```bash
cvpnd_settings $CVPNDIR/conf/cvpnd.C listRemove ISWRelaxedModeProtectionLevelNames
   ```

2. Follow the on-screen instructions.

**Finalize the Configuration for Secure Workspace**

1. Restart the Mobile Access services by running `cvpnrestart`.
   
   If the Mobile Access gateway is part of a cluster, make the same change on each cluster member.
2. In SmartDashboard, assign the Protection Levels to the applications.
3. Install the policy.

**Applications Permitted by Secure Workspace**

In its default configuration, Secure Workspace allows access to a limited group of applications. This is likely to be sufficient for most end-users working with the Mobile Access Portal and retrieving information from network hosts.

The following table lists the latest version of applications that Secure Workspace permits by default.

**Applications Permitted by Secure Workspace by Default**

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DW20.EXE, dwwin.exe</td>
<td>Dr. Watson</td>
<td>A process offers support for application failure handling.</td>
</tr>
<tr>
<td>igfxsrvc.exe</td>
<td>Intel video card driver</td>
<td>A process offers support video card functional.</td>
</tr>
<tr>
<td>iedw.exe</td>
<td>Internet Explorer</td>
<td>Microsoft Internet Explorer web browser</td>
</tr>
<tr>
<td>unsecapp.exe</td>
<td>Microsoft Windows process</td>
<td>A process offers support towards compatibility issues.</td>
</tr>
<tr>
<td>ieuser.exe</td>
<td>Internet Explorer</td>
<td>Microsoft Internet Explorer web browser</td>
</tr>
<tr>
<td>ieinstal.exe</td>
<td>Internet Explorer</td>
<td>Microsoft Internet Explorer web browser</td>
</tr>
<tr>
<td>conime.exe</td>
<td>Microsoft Console IME (Input Method Editor)</td>
<td>A process is used when the locale of the computer is set to a non-western language.</td>
</tr>
<tr>
<td>runner.exe</td>
<td>CShell ActiveX component</td>
<td>A CShell process required on Windows Vista.</td>
</tr>
<tr>
<td>sndvol.exe</td>
<td>Microsoft Windows Volume Control</td>
<td>A process associated with the Microsoft Windows OS.</td>
</tr>
<tr>
<td>SearchIndexer.exe</td>
<td>Content indexing service</td>
<td>A Windows Vista service to index modified content.</td>
</tr>
<tr>
<td>Acrobat.exe</td>
<td>Adobe Acrobat Writer</td>
<td>A process is used to create and print PDF documents.</td>
</tr>
<tr>
<td>acrodist.exe</td>
<td>Adobe Acrobat Distiller</td>
<td>A process is used to create and print PDF documents.</td>
</tr>
<tr>
<td>acrotray.exe</td>
<td>Acrobat Traybar Assistant</td>
<td>A process provides a shortcut to additional configuration options for Adobe products and is used to create PDF documents.</td>
</tr>
<tr>
<td>telnet.exe</td>
<td>Microsoft Telnet Client</td>
<td>A terminal emulation program for TCP/IP networks.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Application</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hypertrm.exe</td>
<td>Microsoft HyperTerminal</td>
<td>A Windows utility that offers Telnet facilities.</td>
</tr>
<tr>
<td>Putty.exe</td>
<td>Putty</td>
<td>Free implementation of Telnet and SSH client.</td>
</tr>
<tr>
<td>SecureCRT.exe</td>
<td>SecureCRT</td>
<td>Telnet and SSH client implementation from VanDyke Software, Inc.</td>
</tr>
<tr>
<td>ptw32.exe</td>
<td>TN3270 Telnet Client</td>
<td>TN3270 telnet client.</td>
</tr>
<tr>
<td>pcsfe.exe</td>
<td>TN3270 Telnet Client</td>
<td>IBM Personal Communications Session Manager. A TN3270 telnet client.</td>
</tr>
<tr>
<td>ftp.exe</td>
<td>Microsoft FTP Client</td>
<td>Microsoft FTP Utility process that provides basic FTP access.</td>
</tr>
<tr>
<td>internat.exe</td>
<td>Predefined Application</td>
<td>Windows process that provides multi-lingual features in Microsoft Windows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This program is important for the stable and secure running of the computer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and should not be terminated.</td>
</tr>
<tr>
<td>Mstsc.exe</td>
<td>Microsoft Remote Desktop</td>
<td>Allows initiation of terminal services commands via command line.</td>
</tr>
<tr>
<td>Vncviewer.exe</td>
<td>VNC Viewer</td>
<td>Remote administration tool process from TWD Industries.</td>
</tr>
<tr>
<td>radmin.exe</td>
<td>RAdmin</td>
<td>Remote Administrator Server from Famatech Corp.</td>
</tr>
<tr>
<td>WISPTIS.EXE</td>
<td>Predefined Application</td>
<td>Process is installed alongside Microsoft office or comes packaged with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows update. This process handles Windows Ink Services and often runs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with Adobe Acrobat Reader.</td>
</tr>
<tr>
<td>MSOHELP.EXE</td>
<td>Predefined Application</td>
<td>Microsoft Office 2003 suite process.</td>
</tr>
<tr>
<td>MSTORDB.EXE</td>
<td>Predefined Application</td>
<td>Microsoft Office 2003 suite process.</td>
</tr>
<tr>
<td>imapi.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows Image Mastering API process, used for CD recording.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This program is important for the stable and secure running of endpoint</td>
</tr>
<tr>
<td></td>
<td></td>
<td>computers and should not be terminated.</td>
</tr>
<tr>
<td>OIS.EXE</td>
<td>Predefined Application</td>
<td>Microsoft Office Picture Manager process.</td>
</tr>
<tr>
<td>CPSWS.exe</td>
<td>Check Point Secure Workspace</td>
<td>Check Point Secure Workspace executable. This executable should be allowed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in order to enable Secure Workspace to start.</td>
</tr>
<tr>
<td>net.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows OS process that offers additional functions to the Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Area Network.</td>
</tr>
<tr>
<td>net1.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows OS process that offers additional functions to the Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Area Network.</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>Predefined Application</td>
<td>Generic Host Process for Win32 Services, an integral part of Microsoft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows OS. It manages 32-bit DLLs and other services and cannot be stopped</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or restarted manually.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Application</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rundll32.exe</td>
<td>Predefined Application</td>
<td>Process that executes DLLs and places their libraries into memory. This program is important for the stable and secure running of the computer.</td>
</tr>
<tr>
<td>msiexec.exe</td>
<td>Predefined Application</td>
<td>Windows Installer Component process. This program is important for the stable and secure running of the computer.</td>
</tr>
<tr>
<td>verclsid.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows OS process that verifies a COM object before the COM object is instantiated by Windows Explorer.</td>
</tr>
<tr>
<td>AcroRd32Info.exe</td>
<td>Predefined Application</td>
<td>Adobe Acrobat Reader process. This process starts automatically when opening a PDF file and collects information about this file.</td>
</tr>
<tr>
<td>MSOXMLED.exe</td>
<td>Predefined Application</td>
<td>Microsoft Office InfoPath process used by Microsoft Office to open and edit XML files.</td>
</tr>
<tr>
<td>java.exe</td>
<td>Predefined Application</td>
<td>Sun Microsystems Java Runtime component</td>
</tr>
<tr>
<td>javaw.exe</td>
<td>Predefined Application</td>
<td>Sun Microsystems Java Runtime component</td>
</tr>
<tr>
<td>jview.exe</td>
<td>Predefined Application</td>
<td>Microsoft Java Virtual Machine Command Line Interpreter</td>
</tr>
<tr>
<td>wjview.exe</td>
<td>Predefined Application</td>
<td>Microsoft Java Virtual Machine Command Line Interpreter</td>
</tr>
<tr>
<td>helpctr.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows OS process. Process is initiated when launching online Help in Windows 2000 or later versions.</td>
</tr>
<tr>
<td>unregmp2.exe</td>
<td>Predefined Application</td>
<td>Windows Media Player component. A process associated with the Microsoft Windows OS.</td>
</tr>
<tr>
<td>sndvol32.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows Volume Control. A process associated with the Microsoft Windows OS.</td>
</tr>
<tr>
<td>STAPProxy.exe</td>
<td>Predefined Application</td>
<td>Check Point SSL Network Extender Application Mode component.</td>
</tr>
<tr>
<td>ctfmon.exe</td>
<td>Predefined Application</td>
<td>Microsoft Office Suite process that activates the Alternative User Input Text Input Processor (TIP) and the Microsoft Office XP Language Bar.</td>
</tr>
<tr>
<td>mobsync.exe</td>
<td>Predefined Application</td>
<td>Microsoft Synchronization Manager. Process associated with Internet Explorer.</td>
</tr>
<tr>
<td>netsh.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows OS process that allows display or modification of the network configuration of a computer that is currently running.</td>
</tr>
<tr>
<td>notepad.exe</td>
<td>Microsoft Notepad</td>
<td>Microsoft Notepad</td>
</tr>
<tr>
<td>calc.exe</td>
<td>Microsoft Calculator</td>
<td>Microsoft Calculator</td>
</tr>
<tr>
<td>wordpad.exe</td>
<td>Microsoft Wordpad</td>
<td>Microsoft Wordpad</td>
</tr>
<tr>
<td>Process Name</td>
<td>Application</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>mspaint.exe</td>
<td>Microsoft Paint</td>
<td>Microsoft Paint</td>
</tr>
<tr>
<td>winword.exe</td>
<td>Microsoft Word</td>
<td>Microsoft MS Office Word</td>
</tr>
<tr>
<td>excel.exe</td>
<td>Microsoft Excel</td>
<td>Microsoft MS Office Excel</td>
</tr>
<tr>
<td>powerpnt.exe</td>
<td>Microsoft PowerPoint</td>
<td>Microsoft MS Office PowerPoint</td>
</tr>
<tr>
<td>acrord32.exe</td>
<td>Adobe Acrobat Reader</td>
<td>Adobe Acrobat Reader</td>
</tr>
<tr>
<td>netscape.exe</td>
<td>Netscape Navigator</td>
<td>Netscape Navigator web browser</td>
</tr>
<tr>
<td>mozilla.exe</td>
<td>Mozilla</td>
<td>Mozilla web browser</td>
</tr>
<tr>
<td>firefox.exe</td>
<td>Mozilla Firefox</td>
<td>Mozilla Firefox web browser</td>
</tr>
<tr>
<td>iexplore.exe</td>
<td>Internet Explorer</td>
<td>Microsoft Internet Explorer web browser</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>Predefined Application</td>
<td>Microsoft Windows Command Prompt</td>
</tr>
<tr>
<td>Citrix</td>
<td>Predefined Application</td>
<td>Citrix Presentation Server (XenApp) application pool.</td>
</tr>
</tbody>
</table>

**SSL Network Extender in Secure Workspace**

When using SSL Network Extender inside Secure Workspace, Secure Workspace traffic and traffic from outside the Secure Workspace are encrypted.

**Secure Workspace Policy Overview**

Secure Workspace governs access to applications and directories on endpoint computers according to a Secure Workspace policy.

Each Mobile Access gateway has its own, individual Secure Workspace policy. The policy:

- Grants or denies permission for users to run applications.
- Allows applications to save files to specific files and directories.
- Defines general portal protection security settings and user experience behavior.

Administrators can add to the list of *Approved Applications*, and can add, edit, or delete applications from the list.

You can define locations where the application is allowed to save files that remain after Secure Workspace shuts down. These locations are called *Allowed Save locations*. There is no need to define locations for files that are not needed after Secure Workspace shuts down. Temporary files are deleted when the Secure Workspace is closed.

Secure Workspace includes a built-in Firewall that allows you define *Outbound Firewall Rules*. These are the IP addresses and ports that approved applications are allowed to access. By default, desktop applications are allowed access to all addresses and ports.

Note that settings for the approved applications, save locations, and Outbound Firewall Rules are independent. For example, the save locations are not restricted to a particular application, and similarly, Outbound Firewall Rules apply to all applications.

**Integration with Check Point Program Advisor**

Secure Workspace can be configured to work together with a Check Point Program Advisor server to check whether an application that is not an approved application is legitimate. Program Advisor identifies programs according to their filename and MD5 hash.
For details of Program Advisor, see your version of the *Endpoint Security Administrator Guide*. If the Program Advisor is used, the sequence of Secure Workspace checks is as follows:

1. User selects a program to run in Secure Workspace.
2. Secure Workspace checks the policy. If the program is not allowed by the Secure Workspace policy, program execution is blocked.
3. If the program is allowed by the policy, Secure Workspace queries the Program Advisor server about the program.
4. Program Advisor returns one of three responses about the application: Trusted, Untrusted, or Unknown.
5. Secure Workspace allows or blocks the application according to the Program Advisor responses, in one the following ways, as defined in the policy:
   - Allow Trusted only.
   - Allow Trusted and Unknown.

### Configuring the Secure Workspace Policy

The Secure Workspace policy determines the permitted activities and behavior that end users will experience when working in Secure Workspace.

**To configure the Secure Workspace Policy:**

2. Configure the Secure Workspace policy. Click *Edit policy*.
   - The Secure Workspace Settings window opens.
3. Fill in the fields according to the explanations below.

#### Portal Protection Settings

- **Deny endpoint to print secure documents** prevents any documents in the Secure Workspace being printed.
- **Secure clipboard contents** prevents any item copied from inside Secure Workspace from being pasted or saved outside Secure Workspace.
- **Enable Program Advisor to validate the integrity of approved applications.** When a user starts an application that is not an Approved Application, Secure Workspace contacts a Check Point Program Advisor server and checks whether the application is legitimate. The server returns one of three responses: The application is trusted, The application is untrusted, or the application is unknown. Configure the Secure Workspace policy to handle Program Advisor responses in one the following ways:
  - Allow Trusted only
  - Allow Trusted and Unknown

#### User Experience Settings

- **Deny endpoint to switch from Secure Workspace to regular desktop** prevents the user from switching back and forth between these environments. Access to the regular desktop is only allowed if Secure Workspace is closed.
- **Enable welcome window** prevents the window that says "Welcome to Secure Workspace" from appearing on the endpoint machine.

### Configuring Approved Applications

Approved applications are available from Secure Workspace, and are allowed to run on endpoint computers. You can add, edit or remove applications from the list.

- **Application Name** is the name of the approved application.
- **File Name** is the path and filename corresponding to the application selected. If needed, specify more than one location per application. You can specify it using one of the following formats:
  - Absolute path in the following format: `<disk>:\<folder_path>\<binary_name>`. Secure Workspace allows the endpoint to run the binary from specified location only. The full path is needed if the location of the program does not appear in the PATH.
  - File name, for example: `\<binary_name>`. Secure Workspace allows the endpoint to run the binary with the specified name from any location on the disk. Use if the location appears in the PATH.
  - Path with environment variable, for example: `<path_with_env_variable(s)>\<binary_name>`. Secure Workspace resolves the environment variable on endpoint, and uses its value as part of the path to executable.

**Add Application**

- **Add shortcut to the Start Menu** adds a shortcut to the application to the Start Menu in the Secure Workspace. The shortcut is only added if the application exists on the client computer.

- **MD5 hash** is the signature of the application. It is possible to add several hashes, for example: one for each version of the application. You can use the ICSInfo Tool (see "Using the ICSInfo Tool" on page 143), or any MD5 calculator, to calculate the hash function of an application.
  
  **Note** - Check Point Program Advisor is a more maintainable and reliable way of checking the security and integrity of programs than manually adding MD5 hashes.

**Configuring Applications by Vendor**

You can configure which applications users can access from Secure Workspace. If a vendor is trusted then all applications from this vendor are trusted.

By default, users can access applications from these vendors. You cannot add a vendor to the list.

<table>
<thead>
<tr>
<th>Vendor ID</th>
<th>Vendor Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adobe</td>
<td>Signed by Adobe</td>
</tr>
<tr>
<td>2</td>
<td>Apple</td>
<td>Signed by Apple</td>
</tr>
<tr>
<td>3</td>
<td>Check Point</td>
<td>Signed by Check Point</td>
</tr>
<tr>
<td>4</td>
<td>Computer Associates</td>
<td>Signed by Computer Associates</td>
</tr>
<tr>
<td>5</td>
<td>Google</td>
<td>Signed by Google</td>
</tr>
<tr>
<td>6</td>
<td>IBM</td>
<td>Signed by IBM</td>
</tr>
<tr>
<td>7</td>
<td>Intel</td>
<td>Signed by Intel</td>
</tr>
<tr>
<td>8</td>
<td>Microsoft</td>
<td>Signed by Microsoft</td>
</tr>
<tr>
<td>9</td>
<td>Mozilla</td>
<td>Signed by Mozilla</td>
</tr>
<tr>
<td>10</td>
<td>Oracle</td>
<td>Signed by Oracle</td>
</tr>
<tr>
<td>11</td>
<td>Sun</td>
<td>Signed by Sun</td>
</tr>
<tr>
<td>12</td>
<td>Rare Ideas</td>
<td>Signed by Rare Ideas</td>
</tr>
<tr>
<td>13</td>
<td>Juniper</td>
<td>Signed by Juniper Networks</td>
</tr>
<tr>
<td>14</td>
<td>Citrix</td>
<td>Signed by Citrix Systems</td>
</tr>
<tr>
<td>15</td>
<td>VMware</td>
<td>Signed by VMware</td>
</tr>
</tbody>
</table>
Configuring Allowed Save Locations

*Allowed Save locations* are locations where applications are allowed to save files that remain after Secure Workspace shuts down. There is no need to define locations for temporary files that can be deleted after Secure Workspace shuts down.

Configuring Outbound Firewall Rules

*Outbound Firewall Rules* are IP addresses and ports that approved applications are allowed to access when they make outbound connections.

A default rule allows desktop applications to access to all addresses and ports. The default rule can be deleted and replaced with more restricted rules. However, configure the rules carefully.

Configuring a Secure Workspace Policy per Gateway

*Note* - Applies to centrally managed Mobile Access only.

A Secure Workspace policy that is configured in SmartDashboard is applicable for all Mobile Access gateways. To configure a Secure workspace policy that is applicable per gateway, see sk34939 ([http://supportcontent.checkpoint.com/solutions?id=sk34939](http://supportcontent.checkpoint.com/solutions?id=sk34939)).

**Secure Workspace End-User Experience**

This section provides an overview of the Secure Workspace workflow.

Disabling Internet Explorer Protected Mode

If users use Internet Explorer to open the SSL VPN portal on Windows Vista or Windows 7, they must disable Internet Explorer Protected Mode. If Protected Mode is not disabled, SSL VPN might run, but they can have unexpected errors.

On Windows 7, protected mode is enabled by default. You can see that it is enabled:

- In the *Internet Options > Security* tab. See that *Enable Protected Mode* is selected.
- In the bottom right of the Internet Explorer browser window, it says *Protected Mode On.*
If Endpoint Security on Demand is configured on the gateway, the scan detects that Protected mode is on and instruction to disable Protected mode open.

If Endpoint Security on Demand is not configured on the gateway, users are not alerted that they must disable Protected mode. However they must do the same steps to disable Protected mode so that they can access the SSL VPN portal without problems.

Here are the instructions that users get to disable Protected Mode. All users must do these steps even if they do not get the instructions automatically.
You are not allowed to access the portal, please review the report below for more information and solutions.

You must disable Protected Mode to allow Check Point Endpoint Security On Demand to run in order to access this Web site.

You can do this with the following steps:

1. In Internet Explorer browser click the Tools button and select Internet Options. The Internet Options window appears.

2. In the Internet Options window select the Security tab.

3. On the Security tab, please select Trusted Sites and ensure that Enable Protected Mode checkbox is not checked. Then click the Sites button. The Trusted Sites window appears.
4. In the Add this website to the Zone: type the portal web address and click the Add button. The portal web address should appear in the Websites area as shown in the figure.

5. Click the Close button to exit the Trusted Sites window.

6. Click OK to exit the Internet Options window.

After these steps, close all Internet Explorer windows. The next time you open Internet Explorer, Protected mode is off.

Logging on to the Mobile Access Portal Using Secure Workspace

Secure Workspace initializes when a user logs on to the Mobile Access Portal. If the administrator has configured the Mobile Access gateway to require Secure Workspace, this occurs automatically. If the administrator has configured the gateway to allow users to choose whether or not to use Endpoint Security On Demand, an option appears on the Login screen.

To log on using Secure Workspace,

1. Enter the Mobile Access Portal URL in your browser. If the Use Check Point Secure Workspace option appears on the login screen, enable it and log on normally.
2. Secure Workspace is installed on the endpoint machine by using ActiveX (for Windows with Internet Explorer), or Java. For more details see First time Installation of ActiveX and Java Components (on page 15).
3. The Mobile Access Portal appears in a browser window on the secure desktop.

Working with the Secure Workspace Virtual Desktop

The Secure Workspace virtual desktop looks and feels like a normal Windows desktop. The principal difference is that Secure Workspace only allows users to work with a limited number of pre-approved applications and files and, by default, does not allow users to print, customize the desktop or perform any system configuration activities. Since most users only use Secure Workspace to work with the Mobile Access Portal, these functions are rarely needed.
Start Menu and Taskbar

The virtual desktop Start menu and taskbar function in the same manner their "real" counterparts do. Configuration settings in the Secure Workspace policy determine which shortcuts and options are available to users.

Allowing Users to Save Files to the "Real" Desktop

Users occasionally need to download and save files from resources behind the Mobile Access gateway to "real" desktop folders. Conversely remote users may need to upload files to the corporate network from the endpoint computer.

To allow this, the administrator must configure the Secure Workspace policy to allow endpoints to switch between the secure and regular desktops. This is accomplished in the User Experience Settings section of the Secure Workspace policy editor.

Accessing Files and Applications on the Endpoint Computer

Generally, users can access files and run applications in Secure Workspace in the same manner as on the "real" desktop. Since, by default, users have read-only (access) privileges to all folders and files, they can freely navigate the file system using Windows Explorer. When attempting to run a program or open a file for which a user does not have Secure Workspace permission, an error message appears.

Likewise, if a user attempts to save a file to a "real" desktop folder without Secure Workspace permissions, an error message appears.

Accessing Endpoint Applications in Secure Workspace

When SSL Network Extender network mode users initiate a Secure Workspace session, permitted Endpoint Applications are available in the virtual desktop as follows:

<table>
<thead>
<tr>
<th>An Endpoint Application defined in the Native Application as...</th>
<th>... is available to Users as a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path and executable name (already installed)</td>
<td>Shortcut in the Windows Start &gt; Program menu.</td>
</tr>
<tr>
<td>Runs via default browser</td>
<td>Shortcut on the desktop.</td>
</tr>
<tr>
<td>Downloaded-from-Mobile Access application</td>
<td>Link in the Mobile Access Portal.</td>
</tr>
</tbody>
</table>

Note - During a Secure Workspace session, SSL Network Extender cannot toggle between the Network Mode and the Application Mode. User can change the mode, but must start a new Secure Workspace session after doing so.

Switching Between Secure Workspace and the "Real" Desktop

You can switch back and forth between the Secure Workspace virtual workspace and the "real" desktop at any time. To do so, click the lock icon, located in the tray area of the taskbar.

Exiting Secure Workspace

To exit Secure Workspace:

1. From the Windows Start menu, select Close Secure Workspace. A confirmation and reminder to save open files appears.
2. Click Yes, close it now to continue closing Secure Workspace.
Troubleshooting Secure Workspace

Secure Workspace logs are automatically saved in %temp%\IswTmp\Logs. If you have issues with Secure Workspace, you can examine these logs or send them to Check Point technical support.

If an application stops working, a Secure Workspace window opens to help you send technical information to Check Point. Users can manually open this window if a process hangs or they experience instability.

To send technical information to Check Point:
1. Press Ctrl+Alt+End.
   A Secure Workspace window opens to help you send technical information to Check Point.
2. Fill in the required information and click Collect and Send.

Endpoint Compliance Updates

Check Point provides Endpoint Compliance updates. You can download Endpoint Security On Demand updates from the Mobile Access tab in SmartDashboard.

You can configure Endpoint Security On Demand to retrieve updates automatically according to a defined schedule or you can manually download and install the updates.

Working with Automatic Updates

You can periodically check for and automatically download Endpoint Compliance updates. You can choose to download updates from the Check Point Download Center or you can install updates previously downloaded to your Security Management Server.

Note - Before performing an Endpoint Security On Demand update, install a policy at least once.

To configure automatic updates:
1. On the SmartDashboard Mobile Access tab, select Endpoint Security On Demand > Endpoint Compliance Updates from the navigation tree.
2. Select Enable Automatic Updates.
3. In the Update Configuration section, click Configure.
   The Automatic Updates window opens.
4. On the User Center Credentials tab, enter your User Center email address and password.
5. In the Endpoint Security On Demand tab, do the following:
   a) To install updates from the Download Center, select the Check Point website option.
   b) To install updates from your Security Management Server, select the My local Security Management Server option. If you want to install updates from the Download Center when the Security Management Server is unavailable, enable the indicated option.
   c) Select the interval, in minutes, after which Endpoint Security On Demand checks for available downloads.
6. In the Tracking Configuration tab, select the various tracking options from the lists. You can select logging events or a variety of alert types.
7. If there is a proxy server between the Security Management Server and the User Center, select the Proxy tab, and enter the proxy host name or IP address, and the proxy port number (for example: 8080).
8. Click OK to complete the definition.
9. Install the policy on the Mobile Access gateways.
Performing Manual Updates

To perform a manual Endpoint Security On Demand update:

1. In the SmartDashboard Mobile Access tab, select Endpoint Security On Demand from the navigation tree.
2. Click Update Databases Now.
3. Enter your Check Point User Center credentials and click Next.
4. Choose the All supporting gateways option to download to all available Mobile Access gateways. Alternatively, choose the Select option to select specific Mobile Access gateways for update, and then select the desired gateways in the left-hand list and then click Add.
5. Click Finish. A progress bar appears during the download.
6. Install policies on all affected gateways.
Chapter 11

Advanced Password Management Settings

In This Section:

- Password Expiration Warning ................................................................. 166
- Managing Expired Passwords ................................................................. 166

If your organization uses Microsoft Active Directory (AD) to manage users, you can use these password settings to allow continuous remote access for your users.

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

Password Expiration Warning

Administrators can configure SmartDashboard to tell users to change their passwords before they expire. This is an efficient way to ensure that users have continuous access to resources. See sk33404 (http://supportcontent.checkpoint.com/solutions?id=sk33404).

Managing Expired Passwords

Passwords expire in these cases:

- The password exceeds the maximum number of days set in the Active Directory Group Policy.
- The User must change password at next logon option in the Active Directory configuration is enabled.

When the password expires, a message tells the user that the login failed. The administrator can configure a setting in SmartDashboard to give users the option to enter a new password after the old one expired. Users whose passwords expired then receive a message: Your password has expired. Enter a new password. They must then enter and confirm a new password to enter the Mobile Access or VPN client portal.

Configuring Password Change After Expiration

You can configure password change after expiration on gateways of version R71 or higher. Make sure that the LDAP server is configured to work with LDAP over SSL.

To enable password change after expiration:

1. In SmartDashboard, select Global Properties > User Directory (LDAP).
2. Under User Directory (LDAP) Properties, select Enable Password change when a user’s Active Directory password expires.
3. In the LDAP Account Unit Properties window, make sure the assigned Profile is Microsoft_AD.
4. Make sure that the Login DN for the LDAP server, as configured in SmartDashboard, has sufficient permissions to modify the passwords of Active Directory users.
5. In the LDAP Server Properties window in the Encryption tab, select Use Encryption (SSL).
6. If the LDAP schema of the Active Directory is not extended with Check Point's LDAP schema, use GuiDBedit, the Check Point Database Tool to make these changes:
   - Select Managed Objects > LDAP > Microsoft_AD > Common
   - Find SupportOldSchema and change its value to 1

For more about LDAP and user management, see the *R77 Security Management Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=24830).

### Session Visibility and Management Utility

When the Session Visibility and Management Utility is enabled, each time a user connects remotely to an R77.30 or higher gateway, the data is recorded in an SQL database.

You can run queries on this database with the Session Visibility and Management Utility.

You can use the Utility to:
- Show session information based on constraints
- Terminate user sessions based on constraints

The main commands are described below. You can also edit the configuration XML file to create custom commands. See sk104644 (http://supportcontent.checkpoint.com/solutions?id=sk104644) for advanced configuration.

These Check Point clients are fully supported with the Session Visibility and Management Utility:
- Capsule Workspace for iOS and Android
- Mobile Access Portal with SSL Network Extender (Application and Network modes)
- Remote Access VPN as part of the Endpoint Security Suite
- Remote Access Clients: Endpoint Security VPN, Check Point Mobile for Windows, SecuRemote

These clients are supported but sessions on them cannot be terminated:
- Capsule Connect
- Capsule VPN
- Windows 8.1 Check Point VPN Plugin

### Enabling the Utility

By default the Session Visibility and Management Utility is disabled.

**To enable or disable the Session Visibility and Management Utility:**

1. For SecurePlatform only, run on the gateway:
   ```
   $CVPNDIR/bin/cvpnd_settings $FWDIR/conf/sessionIS.C set "database_conf:dataDir" "/var${FWDIR}/datadir/postgres/sessions" nobackup; chown cp_postgres /var$FWDIR/datadir/postgres/sessions/postgresql.conf
   ```
2. To enable: On the gateway, run: RAsession_util on
   - To disable: On the gateway, run: RAsession_util off
3. Run: cpstop
4. Run: cpstart
5. In a cluster environment, make the change on all cluster members.
Seeing the Number of Open Sessions

To see the number of sessions open at a given time:

```
RAsession_util show sessions_num
```

Disconnecting Remote Access Users

To disconnect a user:

```
RAsession_util terminate {all|byuser <user>|bysession_id <id>|custom <sql constraint>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Disconnect all Remote Access users</td>
</tr>
<tr>
<td>byuser</td>
<td>Disconnect a user by user name</td>
</tr>
<tr>
<td>bysession_id</td>
<td>Disconnect the session with the given session ID</td>
</tr>
<tr>
<td>custom</td>
<td>Disconnect users that match an SQL constraint</td>
</tr>
</tbody>
</table>

Examples:

```
# RAsession_util terminate all
# RAsession_util terminate byuser james_wilson
# RAsession_util terminate bysession_id 521bd4788
# RAsession_util terminate custom "src_ip='1.1.1.1'"
```

Seeing User Data

To see data of connected users:

```
RAsession_util show users {all | byuser <user_name> | where <where_clause>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Show all users</td>
</tr>
<tr>
<td>byuser</td>
<td>Show data of the given user name</td>
</tr>
<tr>
<td>where</td>
<td>Show users by constraint</td>
</tr>
<tr>
<td>certs</td>
<td>Show user certificates by constraints</td>
</tr>
</tbody>
</table>

Examples:

```
# RAsession_util show users all
# RAsession_util show users byuser "james_wilson"
# RAsession_util show users where "client_name='Mobile Access Portal’"

(This command shows all the users connected from the Mobile Access Portal.)
Using Constraints

To disconnect or see data of users that match a non-default definition, use constraints. First, become familiar with the Check Point scheme for Remote Access sessions. Then, use the field names or types to run a terminate or show users command on matching users.

To see valid constraint fields:

RAsession_util show scheme

Examples:

This command shows the given fields where the client is the Mobile Access Portal, and the results are ordered according to the creation time:

RAsession_util show custom -FIELDS
“session_Id,user_name,client_name,browser_name,machine_name,os_name” -WHERE
“client_name=’Mobile Access Portal’” -ORDERBY “creation_time”

This command shows the given fields where the client type is Capsule Workspace:

RAsession_util show custom -FIELDS
“user_name,sessionid,client_ver,client_build_number,os_name,os_ver,device_type”
-WHERE “client_name=’Capsule Workspace’”
Interoperability with Other Software Blades

The Mobile Access Software Blade is fully integrated with the other Software Blades. Any Security Gateway running on SecurePlatform or Gaia with the Firewall blade enabled can also have the Mobile Access blade enabled.

Most Network objects, Resources, and Users created in SmartDashboard also apply to Mobile Access and can be used when configuring Access to Applications. Similarly, any Network objects, Users and User Groups that you create or modify in Mobile Access appear in the SmartDashboard navigation tree and are usable in all of the SmartDashboard applications.

IPS Blade

When you enable Mobile Access on a Security Gateway certain IPS Web Intelligence protections are activated. The settings of these protections are taken from a local file and are not connected to the IPS profile. These IPS protections always apply to Mobile Access traffic only, even if the Security Gateway does not have the IPS blade enabled.

Disabling Protections for Advanced Troubleshooting

You should only disable the Mobile Access Web Intelligence protections for advanced troubleshooting.

Important - We do not recommend that you deactivate these protections because of potential security risks to the Security Gateway while the protections are off.

To disable the local Web Intelligence protections:

1. Backup the $CVPNDIR/conf/httpd.conf configuration file.
2. Edit $CVPNDIR/conf/httpd.conf by deleting or commenting out this line:
   LoadModule wi_module /opt/CPcvpn-<current version>/lib/libModWI.so

Note - <current version> is the Check Point version installed. For example, R75.20.
Changing to an IPS Profile Configuration for Mobile Access

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 certain 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 all of the protections listed in IPS Protections Crucial for Mobile Access (on page 171).
2. From the CLI, run:
   ```bash
cvpnd_settings $CVPNDIR/conf/cvpnd.C set use_ws_local_configuration false
   ```
3. When prompted, backup `$CVPNDIR/conf/cvpnd.C`
4. Restart the Check Point processes by running `cvpnstop`, `cvpnstart`.

   Note - If IPS is disabled, Mobile Access will use the local IPS configuration to ensure that the Security Gateway is protected. This is true regardless of the `use_ws_local_configuration` flag settings.

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

1. From the CLI, run:
   ```bash
cvpnd_settings $CVPNDIR/conf/cvpnd.C set use_ws_local_configuration true
   ```
2. Restart the Check Point processes by running `cvpnstop`, `cvpnstart`.

IPS Protections Crucial for Mobile Access

The protections listed below should always be active on Mobile Access traffic. They are included in the local IPS settings that are automatically activated when Mobile Access is enabled on a Security Gateway. See that most but not all are included in the `Recommended_Protection` IPS Profile.

<table>
<thead>
<tr>
<th>Protection Name</th>
<th>In Recommended_Protection Profile?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Format Sizes</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP Methods</td>
<td>yes</td>
</tr>
<tr>
<td>ASCII Only Request</td>
<td>yes</td>
</tr>
<tr>
<td>General HTTP Worm Catcher</td>
<td>yes</td>
</tr>
<tr>
<td>Directory Traversal</td>
<td>yes</td>
</tr>
<tr>
<td>Cross-Site Scripting</td>
<td>no</td>
</tr>
<tr>
<td>Command Injection</td>
<td>yes</td>
</tr>
<tr>
<td>Header Rejection</td>
<td>yes</td>
</tr>
<tr>
<td>Malicious Code Protector</td>
<td>no</td>
</tr>
<tr>
<td>Non Compliant HTTP</td>
<td>yes</td>
</tr>
</tbody>
</table>
Anti-Virus and Anti-Malware Blade


These settings apply to Mobile Access traffic when Traditional Anti-Virus is configured to scan traffic By File Direction:

- **Incoming files arriving to** - Inspects traffic that Mobile Access users upload to Mobile Access. (The drop-down menu is not relevant.)
- **Outgoing files leaving** - Inspects the traffic that Mobile Access users download from Mobile Access. (The drop-down menu is not relevant.)
- The Internal Files field is not relevant since Mobile Access uses an external interface.
- Exceptions are not supported.

If Traditional Anti-Virus is configured to scan traffic By IPs, all portal traffic is scanned according to the settings defined for the Mail, FTP and HTTP protocols in SmartDashboard.

Mobile Access Anti-Virus protections always work in **proactive mode** regardless of which option you select.

**Note** - After SSL Network Extender traffic is rerouted to the Security Gateway, Anti-Virus inspects the traffic as it does to any other unencrypted traffic.

Enabling Traditional Anti-Virus

The Anti-Virus blade and Traditional Anti-Virus can be activated on Security Gateways in your system.

**Note** - You cannot activate the Anti-Virus blade and Traditional Anti-Virus on the same Security Gateway.

To configure traditional Anti-Virus:

1. On the Firewall > Overview tab, double-click the required Security Gateway network object.
2. Select Other > More Settings > Enable Traditional Anti-Virus.
3. Click OK.
4. Define rules in the Firewall Policy Rule Base to permit specific services. Anti-Virus scanning is applied only to accepted traffic.
5. From Anti-Bot and Anti-Virus tab > Traditional Anti-Virus, select the services to scan using these options:
   a) From the Database Update page, configure when to perform automatic signature updates or initiate a manual signature update.
   b) From the Security Gateway > Mail Protocol page, configure Anti-Virus scanning options for Mail Anti-Virus, Zero Hour Malware, SMTP, and POP3 services.
   c) From the Security Gateway > FTP page, configure FTP traffic scanning options.
   d) From the Security Gateway > HTTP page, configure HTTP traffic scanning options.
   e) From the Security Gateway > File Types page, configure the options to scan, block or pass traffic according to the file type and configure continuous download options.
   f) From the Security Gateway > Settings page, configure options for file handling and scan failures.
IPsec VPN Blade

The IPsec VPN blade and Mobile Access blade can be enabled on the same gateways. They can be used in parallel to enable optimal site to site and remote access VPN connectivity for your environment.

Certain VPN Clients that worked with Mobile Access in previous versions do not work with the Mobile Access blade on R71 and higher gateways. They only work with the IPsec VPN blade. These are:

- Endpoint Connect
- SecureClient Mobile

SSL Network Extender works either with Mobile Access or with IPsec VPN, however, if the Mobile Access blade is enabled on a gateway, SSL Network Extender must be configured through Mobile Access. If you had SSL Network Extender configured through IPsec VPN and now you enabled the Mobile Access blade on the gateway, you must reconfigure SSL Network Extender policy in the Mobile Access tab of SmartDashboard. Rules regarding SSL Network Extender in the main security rule base are not active if the Mobile Access tab is enabled.

Office mode can be configured either with Mobile Access or with IPsec VPN.

Portal Settings

Each Mobile Access enabled gateway has its own Mobile Access portal that end users browse to for remote access. On the gateway you can configure:

- How the portal can be accessed.
- The look and feel of the portal.
- The default language of the portal.
- An alternative portal for specific user groups.

Portal Accessibility Settings

Configure how users access the Mobile Access portal.

Main URL

Each Mobile Access-enabled Security Gateway leads to its own Mobile Access user portal. Remote users log in to the portal using an authentication scheme configured for that Security Gateway.

Remote users access the portal from a Web browser with https://<Gateway_IP>/sslvpn, where <Gateway_IP> is one of these:

- FQDN that resolves to the IP address of the Security Gateway
- IP address of the Security Gateway

Remote users that use HTTP are automatically redirected to the portal using HTTPS.

Note - If Hostname Translation is the method for link translation, FQDN is required.

Set up the URL for the first time in the Mobile Access First Time Wizard.

Aliases

Click the Aliases button to Add URL aliases that are redirected to the main portal URL. For example, portal.example.com can send users to the portal. To make the alias work, it must be resolved to the main URL on your DNS server.

Certificate

Click Import to import a p12 certificate for the portal website to use. If you do not import a certificate, the portal uses a Check Point auto-generated certificate. This might cause browser warnings if the browser does not recognize the gateway’s management. All portals on the same IP address use the same certificate.
Accessibility
Click Edit to select from where the portal can be accessed. The options are based on the topology configured for the gateway.

- Through all interfaces
- Through internal interfaces
  - Including undefined internal interfaces
  - Including DMZ internal interfaces
- According to the Firewall policy - Select this if there is a rule that states who can access the portal.

Portal Customization
You can configure the look and feel of the default Mobile Access end user portal. There is a default end user portal for each Mobile Access gateway or cluster.

To customize the Mobile Access end user portal:
1. Go to the Portal Customization page of the gateway in one of these ways:
   - From the properties of the gateway, select Mobile Access > Portal Customization.
   - In the SmartDashboard Mobile Access tab, select the Portal Settings > Portal Customization.
     - Select a gateway or cluster object and click Edit.
   The Portal Customization page opens.
2. Make a selection in each field.

Title of the Portal
Title text (multi-language) of the end user portal, such as the name of your company, or any other text.

Localization
Default language (can be changed by user) localizes the end user portal to the selected language.

Logo in the Portal
Use custom logo image and browse to a location where logos are stored. The logo must be 165 x 35 pixels or smaller. Larger images are resized.

Note - If the custom logo is changed, end users must refresh their browser cache in order to see the new logo image.

Clicking the logo redirects to this URL is a URL that can serve as a starting point. It is often used for the URL of the organization's intranet home page.

Localization Features
Mobile Access localizes the user interface of the Mobile Access user portal and the Secure Workspace to multiple languages.

The Mobile Access user portal and the Secure Workspace can be configured by gateway in the Portal Settings > Portal Customization page to use these languages:

- English (the default language)
- Bulgarian
- Chinese - Simplified
- Chinese - Traditional
- Finnish
- French
- German
Auto Detection of User Language Preferences

Automatic language detection is an optional feature that gives priority to the language settings in the user’s browser over the language chosen by the administrator.

Automatic language detection is activated by configuring the `CVPN_PORTAL_LANGUAGE_AUTO_DETECT` flag in the `Main.virtualhost.conf` file on Mobile Access.

By default, the language preference in the user’s browser is not automatically detected. If automatic detection is configured, the language used in SmartDashboard is the first language supported by Mobile Access that is found in the Language Preference list defined in the user’s browser settings. If no supported language is found in the Language Preference list in the user’s browser, the language set by the administrator in SmartDashboard is used.

To activate automatic language detection, perform the following steps on each cluster member:

1. Open an SSH connection to Mobile Access, or connect to it via a console.
2. Log in to Mobile Access using your administrator user name and password.
3. Change to Expert mode by typing `expert` and supplying the password.
4. Edit the `$CVPNDIR/conf/includes/Main.virtualhost.conf` file, and change the following line from:
   
   SetEnv CVPN_PORTAL_LANGUAGE_AUTO_DETECT 0
   
   to:
   
   SetEnv CVPN_PORTAL_LANGUAGE_AUTO_DETECT 1
   
5. Run the command: `cvpnrestart`.

Language Selection by End Users

Any explicit language selection by the user in any of the portal pages overrides both the administrator’s default language setting, and the automatic language detection.

Users can select a language in the user portal sign-in page, in the Change Language To field.

Alternative Portal Configuration

It is possible to specify the portal that is presented to users when they sign in to Mobile Access. You can specify alternative portals for different user groups. Users that do not belong to any of these user groups reach the default Mobile Access portal.

**Note** - There should be an Mobile Access policy rule that includes the alternative portal as a Web application and allows its intended users to access it.

To specify an alternative user portal:

1. In the SmartDashboard Mobile Access tab, select Portal Settings > Alternative Portal.
2. Click Add. The Mobile Access Sign-In Home Page window opens.
3. In the User Groups tab, specify user groups that may access the alternative user portal.
4. In the Install On tab, specify the Mobile Access gateways and gateway clusters that host the alternative portal.
5. In the Sign-In Home Page tab, choose an alternative portal for users, in place of the Mobile Access user portal that users reach by default. **URL** is the location of the alternative user portal for the user group(s) specified in the **User Groups** tab.

When a user belongs to more than one group, the table in the **Alternative Portal** page acts as an ordered rule base. Users are directed to the alternative portal of the first group that they are part of.

**Concurrent Connections to the Gateway**

In the **Gateway Properties** > **Optimization** > **Capacity Optimization** section you can configure the maximum limit for concurrent connections.

When users connect to corporate resources through the Mobile Access blade, it creates multiple connections. For example, from the user to the gateway, and from the gateway to the internal server. Therefore, in an environment with over 1000 remote users, we recommend that you increase the maximum concurrent connections.

For example: The default maximum is 25,000. If you have 2000 mobile access users, increase the maximum to 29,000 (2 times 2000).

**Server Certificates**

For secure SSL communication, gateways must establish trust with endpoint computers by showing a **Server Certificate**. This section discusses the procedures necessary to generate and install server certificates.

Check Point gateways, by default, use a certificate created by the Internal Certificate Authority on the Security Management Server as their server certificate. Browsers do not trust this certificate. When an endpoint computer tries to connect to the gateway with the default certificate, certificate warning messages open in the browser. To prevent these warnings, the administrator must install a server certificate signed by a trusted certificate authority.

All portals on the same Security Gateway IP address use the same certificate.

**Obtaining and Installing a Trusted Server Certificate**

To be accepted by an endpoint computer without a warning, gateways must have a server certificate signed by a known certificate authority (such as Entrust, VeriSign or Thawte). This certificate can be issued directly to the gateway, or be a chained certificate that has a certification path to a trusted root certificate authority (CA).

The next sections describe how to get a certificate for a gateway that is signed by a known Certificate Authority (CA):

**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 computer, 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.
   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.

**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.
   a) Run:
      ```
      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.

**Generating Wildcard Certificates for Hostname Translation**

If you use Hostname Translation, you need a wildcard certificate. This lets clients access Web applications on sub-domains behind the gateway. If Mobile Access uses a fixed domain certificate, client browsers issue certificate warnings when users try to access Web applications in a sub-domain behind the Mobile Access gateway. This is because each Web application URL is translated to a different Mobile Access hostname.

Before you begin, make sure the Hostname Translation support is configured in the DNS server (see "Configuring HT" on page 44) and in the SmartDashboard ("SmartDashboard Configuration of Link Translation" on page 43).

To prepare a request a 3rd-Party wildcard server certificate:

1. In **Subject DN**, start with `CN= FQDN`.
   - For example: CN=sslvpn.example.com
2. In **Alternate Name**, enter two DNS names: the FQDN and the wildcard.
   - For example: sslvpn.example.com, *.sslvpn.example.com

To configure wildcard certificate generation:

1. Backup and edit the configuration file of the csr_gen script:
   - R66.x, R71.x, R75, R75.10 - `$CVPNDIR/conf/openssl.cnf`
   - R75.20 and higher - `$CPDIR/conf/openssl.cnf`
2. In the `[ req ]` section, uncomment the line:
   ```
   req_extensions = v3_req
   ```
3. In the `[ v3_req ]` section, add this line:
   ```
   subjectAltName=DNS: FQDN, DNS:* .ParentDomain
   ```
   - For example: `subjectAltName=DNS: sslvpn.example.com, DNS:* .sslvpn.example.com`
4. Save `openssl.cnf`.
5. Run `csr_gen` and create the CSR.
   To make sure the CSR was generated properly, run:
   - R75.x: `openssl req -in requestFile.csr -text`
   - earlier versions: `openssl req -in requestFile.csr -text`
6. When asked for the CommonName (CN), enter the FQDN. For example: `sslvpn.example.com`
7. Restore the `openssl.cnf` file from the backup.

## 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 > Platform Portal
   - Gateway Properties > Data Loss Prevention
   - Gateway Properties > Identity Awareness > Browser-Based Authentication > 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.

## Viewing the Certificate

To see the new certificate from a Web browser:

The Security Gateway uses the certificate when you connect with a browser to the portal. To see the certificate when you connect to the portal, click the lock icon that is next to the address bar in most browsers.

The certificate that users see depends on the actual IP address that they use to access the portal - not only the IP address configured for the portal in SmartDashboard.

To see the new certificate from SmartDashboard:

From a page that contains the portal settings for that blade/feature, click View in the Certificate section.

## Web Data Compression

Mobile Access can be configured to compress Web content. This can produce a much faster website for users. It also reduces bandwidth needs, and therefore, costs.

Most compression algorithms, when applied to a plain-text file, can reduce its size by 70% or more, depending on the content in the file.

Be aware that compression does increase the CPU usage of Mobile Access, which in itself does have some performance implications.

Most browsers can accept compressed data, uncompress it and display it.

If configured to compress data, Mobile Access compresses the data received from Web servers (the http or https response). If the Web browser at the endpoint compresses the http or https request, Mobile Access uncompresses it and sends it on to the server. This is illustrated in the figure below.
Mobile Access supports the gzip, deflate, and compress compression methods.

It is possible to specify the mime types that will be compressed.

### Configuring Data Compression

Web data compression is configured per gateway in GuiDBedit, the Check Point Database Tool.

**To configure data compression by Mobile Access:**

1. In GuiDBedit, go to network_objects > the table of the gateway.
2. Search for web_compression under connectra_settings and fill in the following parameters:
   - **enable_web_compression** - Enter true to enable data compression and false to disable it.
   - **compression_level** - Enter a value between 1 and 9. The higher the number, the more CPU is used. The default is 5.
   - **compress_specific_mime** - Enter true if you want to compress specific mime types and false if you do not.
   - **mime_types** - If you typed true for compress_specific_mime, enter the mime type, for example, text/html.
3. Save the changes in GuiDBedit and close it.

### Using Mobile Access Clusters

A remote access enabled gateway is a business critical device for an organization. A failure of a gateway results in immediate loss of remote access traffic in and out of the organization. Many of these sessions may be mission critical, and losing them will result in loss of critical data.

Using ClusterXL, you can set up a Load Sharing or High Availability clustering solution that distributes network traffic among Mobile Access cluster members.

A cluster including Mobile Access gateways provides:

- Transparent failover in case of cluster member failure.
- Zero downtime for mission-critical environments.
- Enhanced throughput (in Load Sharing mode).

All cluster members are aware of the sessions tracked through each of the other cluster members. The cluster members synchronize their sessions and status information across a secure synchronization network.

### The Sticky Decision Function

If you are using SSL Network Extender, you must enable the Sticky Decision Function.

A connection is sticky when all of its packets are handled, in either direction, by a single cluster member.

The Sticky Decision Function distributes sessions from client IPs between the cluster members, and ensures that connections from a given IP always pass through the same member.
## How Mobile Access Applications Behave Upon Failover

The table below summarizes the end-user experience upon failover for each Mobile Access application.

### How Applications Behave Upon Failover

<table>
<thead>
<tr>
<th>Application</th>
<th>Survives failover?</th>
<th>User experience upon failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browsing through the user portal</td>
<td>Yes</td>
<td>User is unaware of failover. If the failover happens while a user is clicking a link or waiting for a server response, user may be disconnected and may need to refresh the page.</td>
</tr>
<tr>
<td>Domino Web Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outlook Web Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Shares</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Mail</td>
<td>No</td>
<td>If failover occurs while a user is clicking a link or waiting for a server response, user sees an error page. By clicking the link &quot;Go to the login page&quot; the user returns to the Inbox, and the original session is lost.</td>
</tr>
<tr>
<td>Citrix</td>
<td>No</td>
<td>User is disconnected, and the Citrix session is lost. User must actively re-establish a connection.</td>
</tr>
<tr>
<td>Endpoint Compliance Scan</td>
<td>Yes</td>
<td>Re-scan may be required if user logs out of the portal, or needs to log in again.</td>
</tr>
<tr>
<td>Secure Workspace</td>
<td>Yes</td>
<td>User is unaware of failover. However, if the failover happens while a user is clicking a link or waiting for a server response, user may be disconnected and may need to refresh the page.</td>
</tr>
<tr>
<td>Multi challenge login</td>
<td>No</td>
<td>If user is in the middle of a multi-challenge login he/she is redirected to the initial login page.</td>
</tr>
<tr>
<td>SSL Network Extender Network Mode</td>
<td>Yes</td>
<td>The user may notice the connection stalling for a few seconds, as if there was a temporary network disconnection.</td>
</tr>
<tr>
<td>SSL Network Extender Application Mode</td>
<td>No</td>
<td>SSL Network Extender remains open and in a connected state. However, connections of applications using the VPN tunnel are lost. Some applications (such as Outlook) try to reopen lost connections, while others (Telnet for example) are closed (or exit).</td>
</tr>
<tr>
<td>SSL Network Extender—Downloaded-to-Mobile Access applications</td>
<td>Mode dependent</td>
<td>Network Mode — Survives failover. Application Mode — Does not survive failover.</td>
</tr>
</tbody>
</table>
Chapter 13

Troubleshooting Mobile Access

In This Section:

- Troubleshooting Web Connectivity ......................................................... 181
- Troubleshooting Outlook Web Access .................................................... 181
- Common OWA problems ........................................................................ 182
- Troubleshooting File Shares .................................................................. 186
- Troubleshooting Citrix ............................................................................ 187

Troubleshooting Web Connectivity

Web connectivity issues can occur in Mobile Access Web Applications, while working with applications that use/require HTTP cookies. This is because some cookies usually forwarded by Microsoft Internet Explorer to a Web server are not forwarded by Mobile Access in the same scenario. To solve this, see sk31636 (http://supportcontent.checkpoint.com/solutions?id=sk31636).

Troubleshooting Outlook Web Access

Note - This section applies to Outlook Web Access-related issues occurring when working through Mobile Access without SSL Network Extender.

If you have problems with Outlook Web Access (OWA) after deploying Mobile Access:

1. Read the relevant sections in this Administration Guide. See Web Applications (on page 37).
2. Go over the Troubleshooting OWA Checklist.
3. Look for a description that matches your issues in Common OWA Problems (on page 182).

Troubleshooting OWA Checklist

The following sections describe steps to take if you are experiencing problems using Outlook Web Access with Mobile Access.

1. Check your traffic logs for errors. The logs may help you to pinpoint the problem.
2. Reproduce the scenario without Mobile Access and ensure that the problem does not occur.
3. Verify connectivity. Make sure that:
   - The Mobile Access machine has a network route to all relevant Microsoft Exchange servers and relevant server ports are accessible, usually port 80 or 443.
   - HTTP and/or HTTPS packets must be able to reach Microsoft Exchange servers.
   - Mobile Access users have a network route to the Mobile Access machine.
4. Verify that your configuration is valid. Make sure that:
   - The Outlook Web Access version is supported by Mobile Access.
   - Client-side browsers are supported by OWA and by Mobile Access.
   - OWA Services are configured to use protocols acceptable by the servers in question. For example, if an Exchange server is configured to accept HTTPS traffic only, the corresponding OWA Web application on Mobile Access must utilize HTTPS.
   - Security restrictions are disabled (see "Troubleshooting Security Restrictions in OWA" on page 184).
• Users are authorized to access all necessary resources.
• OWA services are configured with correct paths, according to the specific version of the Microsoft Exchange server.

Unsupported Feature List
The following OWA features, platforms and product versions are not supported by Mobile Access:
• Outlook Web Access (OWA) 5.5.
• OWA 2000 on Microsoft Exchange 2003. (*)
• Outlook Mobile Access.

(*) These products and platforms have not been tested with Mobile Access. However, Mobile Access has been successfully integrated in such environments.

Note - According to Microsoft, only the following OWA configuration supports non-IE browsers: OWA 2000 / 2003 running on Microsoft Exchange 2003 using "Outlook Web Access Basic" scheme.

If you must utilize one of these features, use SSL Network Extender.

Common OWA problems
These sections describe issues related to browsing to OWA through Mobile Access.

Note - Examine your traffic logs for errors, to pinpoint the problem.

Troubleshooting Authentication with OWA
After users log in to Mobile Access, and attempt to access an OWA application, they are required by OWA to provide authentication credentials.

Outlook Web Access has two authentication schemes: the regular HTTP-based authentication (HBA), which is the default, and Form-Based authentication (FBA). In addition, Mobile Access supports single sign-on (SSO) through HBA and FBA.

HBA Problems
If an internal Web Server requests Integrated Windows Authentication (NTLM) or any other HTTP-based authentication, Mobile Access either displays a dialog box requesting login credentials, or tries to use the user's portal credentials, depending on the configuration of the Mobile Access Web application. HBA-related problems may result from the use of IIS web-based password management services.

IIS Web applications (such as Outlook Web Access) can be configured to use IIS Web-based password management services. These services make it possible for users to change their Windows NT passwords via a web server. These services use IIS HTR technology which is known to be vulnerable to attack, and can allow an attacker to run malicious code on the user system. Microsoft has long advocated that customers disable HTR on their Web servers, unless there is a business-critical need for the technology (Microsoft Security Bulletin MS02-028).

In keeping with the Microsoft recommendation, IPS protects against HTR exploits by default. If you wish to allow the use of the HTR mechanism, deactivate the "htr" worm pattern in the IPS General HTTP Worm Catcher protection. Install the Security policy from SmartDashboard after making these changes.

Single Sign On Problems
When troubleshooting, eliminate the possibility of Single Sign On problems by removing the OWA user credentials from the credentials list in the Mobile Access user portal.
Troubleshooting Authorization with OWA

The authorization mechanisms of Mobile Access allow administrators to grant access to various resources on a per-path, per-host and per-port basis. Mobile Access views Outlook Web Access as a Web application with special properties, connecting to a special Web server.

Authorization-related problems may result from:

- **Discrepancies in the OWA Web Application Configuration** (on page 183) versus the setup in Microsoft Exchange server.
- **Alternative References to OWA** (on page 183).

User experiences may vary widely. However, most authorization failures will result in the following error message: Error: Access denied. The destination of your request has not been configured, or you do not have authorization access to it. (401).

Discrepancies in the OWA Web Application Configuration

Possible discrepancies may occur in the configuration of the OWA port, protocol or paths versus the setup of the corresponding Microsoft Exchange server.

OWA Service must be configured in accordance with the Microsoft Exchange server configuration. Otherwise, Mobile Access will not be able to authorize access to the application.

**Authorization Example Scenario**

A user launches an OWA application, gets to the Form-Based Authentication (FBA) page and authenticates using his/her credentials. Subsequently, the user gets the "Access denied" page.

**Cause:** The Microsoft Exchange server side component (IIS or other) is configured to accept both HTTP and HTTPS traffic, whereas the Mobile Access OWA Web application is configured to authorize HTTP traffic only.

**Explanation:** The Form Based Authentication setting on the Microsoft Exchange server requires clients to use SSL, which means that some server-side component (be it IIS or other) must also accept SSL traffic. The following message is displayed to the Microsoft Exchange administrator upon FBA configuration:

```
Forms Based Authentication requires clients to use a SSL connection. If SSL encryption is not off-loaded to another source, complete the following steps:
- Configure SSL
- Restart the IIS service
```

This means that IIS is likely to be configured to work over SSL. However, in complex cases, such as SSL encryption being off-loaded to another source, and the IIS server itself allowing HTTP traffic, the Mobile Access administrator may not be aware of the need to authorize HTTPS traffic. As a result, discrepancies may occur.

**Note** - When FBA is in use, always set the OWA Web application to allow HTTPS traffic.

**Solution:** Make sure that the OWA application configuration on the Mobile Access blade matches the configuration requirements of the Microsoft Exchange server.

**Alternative References to OWA**

Some companies access their OWA applications via intermediary websites. These intermediary websites may reference the OWA server by its IP(s) or host name(s). If, when defining access to the OWA server, the intermediary website is ignored, it can cause an authorization failure in Mobile Access.
Troubleshooting Mobile Access

User experiences may vary. In some cases the problem may result in a run-time JavaScript error or OWA becomes unresponsive (see Insufficient User Permissions for more information).

To troubleshoot such problems, test OWA operations without using any mediator (such as proxies, gateways or websites).

Troubleshooting Security Restrictions in OWA

Mobile Access utilizes many built-in security features that screen inner networks from external threats. In addition, the Mobile Access endpoint security features protect the endpoint devices.

Occasionally, protection mechanisms may interfere with legitimate user activities. To eliminate this possibility, switch off all Web Intelligence protections during troubleshooting and the install the security policy.

User experiences may vary widely so they are not detailed here. Use the following steps to troubleshoot issues with security restrictions.

1. Check the traffic log to see if any relevant URL was blocked due to security restrictions.
2. To reduce the number of false-positives:
   - In SmartDashboard, in the IPS tab, go to Protections > By Protocol > Integrated > Web Intelligence and turn all Application Layer Protection Level settings to Low.
   - In the ASCII Only Request protection, clear Block non ASCII characters in form fields.
   - Install the Security policy from SmartDashboard.
3. If Step 2 did not solve the problem, try the following:
   - Modify the Endpoint Compliance page of the Mobile Access Web Application to Allow caching of all content.
   - In SmartDashboard, in the IPS tab, go to Web Intelligence and
     - In the HTTP Protocol Inspection > HTTP Methods protection, clear Block standard Unsafe HTTP methods.
     - In the Malicious Code > General HTTP Worm Catcher protection, disable the "htr" worm pattern.
   - Install the Security Policy from the administration portal.
4. If Step 3 did not solve the problem, try the following steps in order:
   a) Turn off all Web Intelligence protections.
   b) Turn off all IPS protections.
   c) Install the Security policy from SmartDashboard.

Troubleshooting Performance Issues in OWA

Performance issues may occur with OWA for the following reasons:

- Logging Issues (see "Mobile Access Logging Issues" on page 184)
- OWA over SSL or OWA with Form Based Authentication Enabled (on page 185)
- Slow Network Problems (on page 185)
- Latency Overhead Problems (on page 185)
- Authorization Problems
- SSL Time-out Problems (on page 186)

Mobile Access Logging Issues

Generations of Debug and Trace logs (that are accessed via the console), and the storage of these log records when they grow too big, may considerably degrade the performance of the machine.

Note - Traffic and event logs (that are accessible using the SmartConsole clients) do not degrade the performance of Mobile Access.
To get rid of these logs, turn off Debug logs, Trace logs and purge existing Debug logs and Trace logs.

To turn off Debug logs and Trace logs:

1. **Modify** `/etc/httpd/conf/httpd.conf as follows:**
   
a) Set the `LogLevel` parameter to `emerg`.
   
b) Make sure the following lines are commented. Commented lines are preceded by `#`:
   ```
   #CvpnTraceLogMaxByte 10000000
   #CvpnWsDebugSubjects ...
   ```

2. Run the `cvpnrestart` command

3. If you have a Mobile Access cluster, repeat on all cluster members.

To purge existing Debug logs and Trace logs:

1. Empty or delete all `httpd.log*` files located in `/etc/httpd/log` directory
2. Empty or delete the `mod_ws.log` file located in `/etc/httpd/log` directory
3. Empty or delete the `mod_ws_boa.log` file located in `/etc/httpd/log` directory
4. Delete all files located under `/etc/httpd/log/trace_log` directory
5. If you have a Mobile Access cluster, repeat on all cluster members.

**OWA over SSL or OWA with Form Based Authentication Enabled**

The Outlook Web Access service can be configured to work over SSL inside secure networks. This option is normally used if the Microsoft Exchange server is configured to accept SSL-encrypted traffic (HTTPS).

This is the case if OWA is configured to use Form Based Authentication (FBA). Upon enabling FBA, the Exchange administrator is prompted by the IIS to change the Web application to work over SSL.

Configuring OWA to use SSL inside secure networks may cause degradation in performance and browsing experience. This is because, in such a topology, the amount of SSL negotiations grows considerably. SSL negotiations are very CPU-intensive, and therefore may cause performance degradation.

**To solve this problem:**

- Change the topology to use HTTP instead of HTTPS inside secure networks.
- Use a stronger machine.

**Slow Network Problems**

Introducing Mobile Access into an OWA topology allows users to connect to enterprise resources from remote locations.

Users connecting from remote locations may be subject to temporary or permanent network problems. The rate of packet loss in those networks can vary widely, as can the throughput.

**Latency Overhead Problems**

Mobile Access inspects and modifies all HTTP traffic passing through the gateway. It takes time to process each particular packet of information.

There is therefore a difference in latency between connections passing through Mobile Access and those that do not. The overhead in absolute elapsed time is proportional to the amount of data passed through the network.

Latency and therefore performance problems when working through Mobile Access may be felt in particular by users with large numbers of emails, calendar events, task items and the like.

**To solve this problem:**

Minimize the latency overhead by increasing the performance of Mobile Access. You can do this by using a stronger machine.
SSL Time-out Problems

SSL time-out problems can occur with Internet Explorer while working through Mobile Access. They can cause slowness and even temporary or permanent unresponsiveness of the browser.

To solve this problem:
- If feasible, upgrade Internet Explorer by following the instructions in the relevant Microsoft articles below.
- Alternatively, configure Mobile Access so that it does not use keep-alive packets when communicating with those hosts or paths.

See these Microsoft articles for more information:
- http://support.microsoft.com/kb/183110/
- http://support.microsoft.com/?kbid=831167
- http://support.microsoft.com/?scid=kb;EN-US;Q305217

To configure Mobile Access to work without keep-alive packets to specific locations:

1. Supply additional LocationMatch directives for each host used by the Web Application in question. All directives go in the $CVPNDIR/conf/includes/Main.virtualhost.conf file, in the VirtualHost section.

   For more information, see: http://httpd.apache.org/docs/2.0/mod/core.html#locationmatch

   ```
   <LocationMatch "CVPNHost=<IP or DNS name delimited by dots>">
      SetEnv nokeepalive
   </LocationMatch>
   ```

   For example:

   ```
   <LocationMatch "CVPNHost=208.77.188.166">
      SetEnv nokeepalive
   </LocationMatch>
   ```
   ........
   ```
   <LocationMatch "CVPNHost=myhost.example.com|CVPNHost=myhost">
      SetEnv nokeepalive
   </LocationMatch>
   ```

2. Run `cpstop` and then `cpstart`.
3. Repeat for each Mobile Access cluster member (if any).

Saving File Attachments with OWA

When trying to save a file attachment with Outlook Web Access (OWA), Mobile Access adds the full path to the file name. For example, the file name appears something like:

```
Bulletin1H.PDF,CVPNHost=192.168.201.6,CVPNProtocol=http,CVPNOrg=full,CVPNExtension=.PDF
```

To solve this, configure the Web Application to use Path Translation or Hostname Translation ("Link Translation" on page 42).

Troubleshooting File Shares

- Mobile Access gives an informative error message when an attempt to access a file share fails. However, if a user tries to access a share that does not exist on the file server, Mobile Access cannot always distinguish this error from an Access Denied error. In this case the user may be presented with the credentials input form again, or get an Access Denied error.

- The Windows Explorer viewer can normally be used for browsing website. However, the Mobile Access SSL Network Extender window may not load properly when using it, and the user may be presented with the Mobile Access login page. It is recommended to use the Web-based viewer instead.
When browsing file shares through the Mobile Access user portal, users can open most files by clicking them. However, some files, for example .wmv extension files, cannot be opened that way, and must be downloaded to the local desktop and opened from there. When using the Mobile Access Web-based file viewer, download the file by right-clicking on the file and choosing "Save Target As...". When using the Windows File Explorer viewer, download the file by copying or drag-and-dropping it to the local desktop.

When accessing files via Mobile Access, the client application used to view a file depends on the file type. Some file types (such as jpg files) can be configured to be opened by a Web browser. In some client configurations, the result of opening such a file may show the Mobile Access login page instead of the requested file. If this happens, verify that the client uses the latest recommended browser version including all patches and fixes. Specifically, install Internet Explorer patch Q823353 on the endpoint.

Troubleshooting Citrix

Note - This Citrix troubleshooting section pertains to Citrix-related issues occurring when working through Mobile Access without the use of SSL Network Extender.

If you have issues with Citrix after the deployment of Mobile Access, see the section on Citrix Services (on page 51) and then try the troubleshooting checklist.

Troubleshooting Citrix Checklist

Follow the steps below to pinpoint the issue that may be causing trouble with Citrix.

Connectivity Issues

1. Make sure that Mobile Access has a network route to all Web Interface servers intended to be used and relevant server ports are accessible. Usually ports 80 or 443.
   HTTP and/or HTTPS protocols must be traversable towards Web Interface servers.
2. Make sure that Mobile Access has a network route to all Presentation servers intended to be used and relevant server ports are accessible. Usually ports 1494 or 2598.
   ICA protocol must be traversable towards Presentation servers.
3. Make sure that Mobile Access machine has a network route to all STA servers intended to be used, if any, and port 80 on STA servers is accessible, and HTTP protocol is traversable.
4. Make sure that Mobile Access users have a network route to the Mobile Access machine.

Configuration Issues

1. Make sure that Citrix servers and clients are of those versions supported by Mobile Access.
2. Make sure that all necessary STA servers are configured with corresponding Citrix Services on Mobile Access.
3. Make sure that the Mobile Access server certificate:
   - is issued to the Fully Qualified Domain Name (such as www.example.com) of the gateway.
   - is properly configured.
   - is trusted by the client-side.
Chapter 14

Mobile Access Commands

In This Section:

- cvpn_ver: Shows the version of the Mobile Access Software Blade. Use with `fw ver -k` to get all version details.
  Usage `cvpn_ver`

- listusers: Shows a list of end-users connected to the gateway, along with their source IP addresses.
  Usage `listusers`

- cvpnstop: Stops all Mobile Access blade services.
  Usage `cvpnstop`
  Notes: While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

- cvpnstart: Starts all Mobile Access blade services.
  Usage `cvpnstart`
cvpnrestart

**Description**  
Restarts all Mobile Access blade services.

**Usage**  
cvpnrestart [--with-pinger]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--with-pinger</td>
<td>Restarts the ‘pinger’ service, responsible for ActiveSync and Outlook Web Access push mail notifications.</td>
</tr>
</tbody>
</table>

**Notes:** While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

cvpnd_admin

**Description**  
A utility to change the behavior of the Mobile Access cvpnd process.

**Usage**  
cvpnd_admin [policy [hard] | [debug [off | set... | trace]]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td>Updates the Mobile Access services according to the current policy. For Apache services, each httpd process waits until its current request is finished, then exits.</td>
</tr>
<tr>
<td>policy hard</td>
<td>Updates the Mobile Access services according to the current policy. For Apache services, all httpd processes exit immediately, terminating current http requests.</td>
</tr>
</tbody>
</table>
| debug set TDERROR_ALL_ALL=5 | Enables all cvpnd debug output for the running cvpnd process. The output is in $CVPNDIR/log/cvpnd.elg.  
Note: Enabling all debug topics might have a small effect on performance. |
| debug off    | Disables all cvpnd debug output.                                             |
| debug trace on | The TraceLogger feature generates full captures of incoming and outgoing authenticated Mobile Access traffic. The output is in: $CVPNDIR/log/trace_log/. |
| debug trace users=username | Enables the TraceLogger feature for all users. |
|              | Enables the TraceLogger feature for a specified username                   |

**Important Notes:**

1. The TraceLogger feature has a major effect on performance, because all traffic is saved as files.
2. The feature uses a lot of disk space. After a maximum number of files is output, the oldest files are removed from the disk, which also has a performance cost.
3. TraceLogger creates a security concern: end-user passwords sent to internal resources might appear in the capture files.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appMonitor status</td>
<td>Shows the status of the Application Monitor feature. The application monitor is a software component that monitors internal servers to track their up time. If problems are found, a system alert log is created. This command lists the applications monitored by the Application Monitor and their status.</td>
</tr>
</tbody>
</table>

**cvpnd_settings**

**Description**  Changes a Mobile Access gateway’s local configuration file, cvpnd.C.

**Usage**  cvpnd_settings <conf_file_path> <get|set|add|listAdd|listRemove> <Attribute-Name> [Attribute-Value]

**Parameters**  Run: cvpnd_settings -h for a full explanation of the parameters.

⚠️ **Important** - Changes made by the cvpnd_settings command are not saved in gateway upgrades. Keep a backup of your cvpnd.C file after you make manual changes.

**deleteUserSettings**

**Description**  Deletes all persistent settings (favorites, cookies, credentials) of one or more end-users.

**Usage**  deleteUserSettings [-s] <username1> [<username2> ...]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>Runs in silent mode with no output to the end-user's screen.</td>
</tr>
</tbody>
</table>

**ics_updates_script**

**Description**  Manually starts an Endpoint Security on Demand (ESOD) update on the gateway. Use this script to troubleshoot ESOD updates.

**Usage**  $CVPNDIR/bin/ics_updates_script <ICS_updates_file_path>

**Notes:**

- The script requires an ESOD update package on the gateway.
- Usually this script is not necessary and you start updates from SmartDashboard. Go to Mobile Access tab > Endpoint Security on Demand > Endpoint Compliance Updates > Update Database Now.
- Be careful not to run other scripts with the name ics_updates_script, for example, the one in $FWDIR/bin/.

**rehash_ca_bundle**

**Description**  Imports all of the Certificate Authority (CA) files from the $CVPNDIR/var/ssl/ca-bundle/ directory into the Mobile Access trusted CA bundle.

The trusted CA bundle is used when the Mobile Access gateway accesses an internal server (such as OWA) through HTTPS. If the SSL server certificate of the internal server is not trusted by the gateway, the gateway responds based on the settings for the Internal Web Server Verification feature. The default setting is Monitor.

To accept certificates from a specified server, add its server certificate CA to the CA bundle.

**Usage**  rehash_ca_bundle
admin_wizard

Description
Tests connectivity to websites and Exchange server services.

- **For websites**: It tests connectivity to the website.
- **For Exchange servers**: It tests the response from an Exchange server. It also finds the address protocol (HTTP or HTTPS) and authentication method (Basic or NTLM) of the Exchange server services.

Usage

- **For websites**: `admin_wizard wizard <website address>`
- **For Exchange servers**: `admin_wizard exchange_wizard <Exchange server address> <user name> <password> [parameters]`

Parameters

To enter more than one item within a parameter, separate items with a comma. For example: `as,owa`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-t <as|ews|owa|all>]` | Select the services to test on the Exchange server:  
  - `as` - Test ActiveSync  
  - `ews` - Test Exchange Web Services  
  - `owa` - Search for the Outlook Web Application address of the Exchange server  
  - `all` - Test all of the above services (default) |
| `-d <dns servers>]` | Enter DNS servers |
| `-x <proxy servers>]` | Enter proxy servers |
| `-c <username:password>]` | Enter a user name and password for proxy authentication |
| `-n` | Allow only NTLM authentication instead of Basic and NTLM |
| `-m <domain name>]` | Enter a user domain name |
| `-s <ActiveSync path>]` | Test a specified ActiveSync service path (default: `/Microsoft-Server-ActiveSync`) |
| `-e <EWS path>]` | Test a specified Exchange Web Services service path, (default: `/EWS/Exchange.asmx`) |
| `-f <file name>]` | Write the results to a file |
| `-r` | Send a request with the configured: proxy, DNS, HTTP protocol, and authentication method.  
  If `-n` is included, then NTLM authentication method is used. If not, only Basic is used. |
| `-v` | Make the HTTP requests verbose. The verbose result files go to `$CVPNDIR/log/trace_log/` |
| `-p` | Validate the SSL certificate of the web server |
**fwpush**

This feature is supported in R77.10 and higher.

**Description:** Sends command interrupts to fwpushd process.

**Usage:** fwpush info|send|print|unsub

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td>Get data on notifications in the push queue:</td>
</tr>
<tr>
<td></td>
<td>- Number of items in queues</td>
</tr>
<tr>
<td></td>
<td>- Number of seconds the oldest item is in the queue</td>
</tr>
<tr>
<td></td>
<td>- Number of seconds the newest item is in the queue</td>
</tr>
<tr>
<td></td>
<td>- Number of seconds a batch waits in the queue</td>
</tr>
<tr>
<td></td>
<td>- Number of seconds to the sending of the next batch</td>
</tr>
<tr>
<td></td>
<td>- Number of batch errors and authentication request timeouts</td>
</tr>
</tbody>
</table>

**send** -token [<token>|<username>]| -os <OS> -msg "<notification message>"

Send an on-demand push notification from a command line, using a username or a token.

**print**

Show the push notifications queue and the pending batches.

**unsub** [<token>|<username>|<User-UID>]| -all

Unsubscribe a user:
- **token** - Delete the token from the User-Settings
- **User-Name or User-UID** - Unsubscribe the user from all business emails
- **User-Name or User-UID** -all - Delete all the user's tokens

⚠️ **Important** - Before you use the fwpush command with the send switch, make sure the user is registered on the Exchange Server and is connected.

**To see user connection status:**

Run: [expert@hostname:0]# UserSettingsUtil show_exchange_registered_users

Example output:

```
User Name: CN=JohnD,OU=USERS,OU=RND,OU=PO,OU=ISRAEL,DC=AD,DC=CHECKPOINT,DC=COM
User Settings id: c4b6c6fbb0c4a4ff4469265e93e0e372
Push Token: xxxxxxxxxxxxx65b48e424023eb7952fbc5ca22ea788cfb3cxxxxxxxxxx Device id: 46c5XXXcc1d1b4e18cf5a1ff3290f2
```

Use the value of the CN variable (JohnD in this example) for the username in the fwpush send command:
[expert@hostname:0]# fwpush send -uid JohnD -msg "hello push"

If you use a token, it must be taken from the output of the command:
UserSettingsUtil show_exchange_registered_users

For example:
[Expert@secure-GW]# UserSettingsUtil show_exchange_registered_users

If you use a different token, push notifications cannot work with the gateway.

✉️ **Note** - Users only get push notifications while logged in.
IPS Protections Crucial for Mobile Access • 169
IPsec VPN Blade • 170

K
Kerberos Authentication Support • 66
Kerberos Constrained Delegation • 69

L
Language Selection • 15
Latency Overhead Problems • 183
Launch SSL Network Extender Client • 77
Link Translation • 41
Link Translation Domain • 45
Link Translation Domains • 42
Link Translation Issues • 44
Link Translation Per Gateway or Per Application • 41
listusers • 186
Localization Features • 172
Logging on to the Mobile Access Portal Using Secure Workspace • 160

M
Making an Application Available in Application Mode • 83
Managing Capsule Workspace Settings • 102
Managing Client Certificates • 99
Managing Expired Passwords • 164
Manual Configuration for Kerberos • 68
Manually Defining HTTP Post Details • 66
Match Word • 122
MDM Cooperative Enforcement • 108
Mobile Access Applications • 11
Mobile Access Blade Configuration and Settings • 168
Mobile Access Client Support for SSO • 61
Mobile Access Commands • 186
Mobile Access for Smartphones and Tablets • 98
Mobile Access Logging Issues • 182
Mobile Access Management • 12
Mobile Access Security Features • 14
Mobile Access Web Portal • 21
Mobile Access Wizard • 30
Monitoring Push Notification Usage • 107
Monitoring WebSockets • 57
Multiple Hosts and Services • 82
Multiple Realms • 130

N
Native Applications • 55
Native Applications for Client-Based Access • 72

O
Obscuring Passwords in mdm.conf • 110
Obtaining and Installing a Trusted Server Certificate • 174
Obtaining the SMS Provider Credentials • 123
Office Mode • 75
OR Group of Rules • 139
Other Simultaneous Login Issues • 135
Outlook Web Access • 37

Overview of Mobile Access for Smartphones and Tablets • 98
OWA over SSL or OWA with Form Based Authentication Enabled • 183

P
Passcode Profiles • 104
Password Expiration Warning • 164
Performing Manual Updates • 162
Phone Number or Email Retrieval • 126
Planning the Endpoint Compliance Policy • 141
Platform-Based Bypass Per Protection Level • 145
Platform-Based Bypass Per Protection Level in Secure Workspace • 151
Policy Requirements for ActiveSync Applications • 96
Portal Accessibility Settings • 171
Portal Customization • 172
Portal Protection Settings • 156
Portal Settings • 171
Preparing for Capsule Connect • 33
Preparing for Capsule Workspace • 33
Preparing for Desktop Clients • 33
Preventing an Endpoint Compliance Scan Upon Every Login • 148
Preventing Portal Access with Unsupported Browsers • 149
Protection Levels • 13, 35
Protection Levels for Native Applications • 84
Providing Secure Remote Access • 18
Push Notifications • 105

R
Recommended Deployments • 25
rehash_ca_bundle • 188
Remote Access Solution Comparison • 19
Remote Wipe • 101
Requiring Certificates for Mobile Devices • 121
Reuse TCP Connections • 46
Revoking Certificates • 100
Roaming • 134

S
Sample Mobile Access Workflow • 30
Saving File Attachments with OWA • 184
Secure Connectivity and Endpoint Security • 19
Secure Workspace • 13, 150
Secure Workspace End-User Experience • 158
Secure Workspace Policy Overview • 155
SecureClient Mobile - Simultaneous Login Issues • 135
SecuRemote • 24
Securing Authentication Credentials • 134
Security Gateway Portals • 16
Seeing the Number of Open Sessions • 166
Seeing User Data • 166
Server Certificates • 174
Server Side Security Highlights • 14
Session • 14
Session Settings • 134
Session Timeout for Android Devices • 115
Session Timeouts • 134
Session Visibility and Management Utility • 165
Setting up the Mobile Access Portal • 32
Sign In Success or Failure Detection • 65
Signing In • 15
Simple Deployment • 25
Simultaneous Login Issues • 135
Simultaneous Logins to the Portal • 134
Single Sign On • 58
Single Sign On Problems • 180
Slow Network Problems • 183
SmartDashboard Configuration of Link Translation • 42
SmartDashboard Toolbar • 29
SMS Authentication Granularity • 123
Spyware Scan Rule • 139
SSL Network Extender • 12, 21, 72
SSL Network Extender Application Mode • 12, 73
SSL Network Extender in Secure Workspace • 155
SSL Network Extender Network Mode • 12, 73
SSO for Native Applications • 62
Start Menu and Taskbar • 161
Statically Obscuring DNS Host Names • 44
Summary of Remote Access Options • 21
Supported Application Mode Applications • 73
Supported SSO Authentication Protocol • 58
Switching Between Secure Workspace and the • 161
System Specific Configuration • 113

T
Testing MDM • 113
Testing Two-Factor Authentication • 125
The SMS Service Provider • 122
The Sticky Decision Function • 177
Tracking • 134
Tracking of Simultaneous Logins • 135
Troubleshooting • 70, 132
Troubleshooting Authentication with OWA • 180
Troubleshooting Authorization with OWA • 181
Troubleshooting Citrix • 185
Troubleshooting Citrix Checklist • 185
Troubleshooting File Shares • 184
Troubleshooting Mobile Access • 179
Troubleshooting Outlook Web Access • 179
Troubleshooting OWA Checklist • 179
Troubleshooting Performance Issues in OWA • 182
Troubleshooting Secure Workspace • 161
Troubleshooting Security Restrictions in OWA • 182
Troubleshooting Web Connectivity • 179
Two-Factor Authentication for Certain Authentication Methods • 129, 133
Two-Factor Authentication per Application • 128
Two-Factor Authentication per Gateway • 128
Two-Factor Authentication with DynamicID • 122
Types of Solutions • 18

U
Unsupported Feature List • 180
User Authentication in Mobile Access • 120
User Authentication to the Mobile Access Portal • 120
User Experience Settings • 156
User Workflow for Mobile Access Portal • 15
Using Constraints • 166
Using Endpoint Security On Demand with Unsupported Browsers • 149
Using Mobile Access Clusters • 177
Using Protection Levels • 35
Using the $user Variable in File Shares • 50
Using the $user Variable in Native Applications • 81
Using the ICSInfo Tool • 142
Using the Login Name of the Currently Logged in User • 39, 56
Using WebSockets • 57

V
Vendor Options • 110
Very Advanced Approach
  Configuring Individual Policies for Each Application • 145
Viewing the Certificate • 176

W
Web Application — Authorized Locations Page • 37
Web Application — General Properties Page • 37
Web Application — Link in Portal Page • 38
Web Application — Link Translation Page • 39
Web Application — Protection Level Page • 38
Web Application Features • 46
Web Applications • 36
Web Applications of a Specific Type • 36
Web Data Compression • 176
Web Form Based SSO • 59
Web Form Based SSO Limitations • 60
Web Mail Service — General Properties Page • 54
Web Mail Service — Link in Portal Page • 54
Web Mail Service — Protection Level Page • 54
Web Mail Service — Single Sign-On Page • 54
Web Mail Services • 53
Web Mail Services User Experience • 53
Website Certificate Verification • 46
WebSockets • 56
Where DNS Name Objects are Used • 55
Windows Security Rule • 138
Workflow • 130
Working with Automatic Updates • 162
Working with the Secure Workspace Virtual Desktop • 160