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=11673
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 October 2011</td>
<td>Fixed misspelling in $CVPNDIR</td>
</tr>
<tr>
<td>16 December 2010</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 R75 Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to Mobile Access</td>
<td>8</td>
</tr>
<tr>
<td>Mobile Access Applications</td>
<td>8</td>
</tr>
<tr>
<td>Mobile Access Management</td>
<td>9</td>
</tr>
<tr>
<td>SSL Network Extender</td>
<td>9</td>
</tr>
<tr>
<td>SSL Network Extender Network Mode</td>
<td>9</td>
</tr>
<tr>
<td>SSL Network Extender Application Mode</td>
<td>9</td>
</tr>
<tr>
<td>Commonly Used Concepts</td>
<td>9</td>
</tr>
<tr>
<td>Authentication</td>
<td>10</td>
</tr>
<tr>
<td>Authorization</td>
<td>10</td>
</tr>
<tr>
<td>Endpoint Compliance Scanner</td>
<td>10</td>
</tr>
<tr>
<td>Secure Workspace</td>
<td>10</td>
</tr>
<tr>
<td>Protection Levels</td>
<td>10</td>
</tr>
<tr>
<td>Session</td>
<td>11</td>
</tr>
<tr>
<td>Mobile Access Security Features</td>
<td>11</td>
</tr>
<tr>
<td>Server Side Security Highlights</td>
<td>11</td>
</tr>
<tr>
<td>Client Side Security Highlights</td>
<td>11</td>
</tr>
<tr>
<td>User Workflow</td>
<td>12</td>
</tr>
<tr>
<td>Signing In</td>
<td>12</td>
</tr>
<tr>
<td>First time Installation of ActiveX and Java Components</td>
<td>12</td>
</tr>
<tr>
<td>Language Selection</td>
<td>13</td>
</tr>
<tr>
<td>Initial Setup</td>
<td>13</td>
</tr>
<tr>
<td>Accessing Applications</td>
<td>13</td>
</tr>
<tr>
<td>Getting Started with Mobile Access</td>
<td>14</td>
</tr>
<tr>
<td>Recommended Deployments</td>
<td>14</td>
</tr>
<tr>
<td>Simple Deployment</td>
<td>14</td>
</tr>
<tr>
<td>Deployment in the DMZ</td>
<td>14</td>
</tr>
<tr>
<td>Cluster Deployment</td>
<td>14</td>
</tr>
<tr>
<td>Basic SmartDashboard Configuration</td>
<td>15</td>
</tr>
<tr>
<td>The Mobile Access Wizard</td>
<td>15</td>
</tr>
<tr>
<td>Setting up the Mobile Access Portal</td>
<td>16</td>
</tr>
<tr>
<td>Managing Access to Applications</td>
<td>17</td>
</tr>
<tr>
<td>Configuring Mobile Access Policy</td>
<td>17</td>
</tr>
<tr>
<td>Applications for Clientless Access</td>
<td>19</td>
</tr>
<tr>
<td>Protection Levels</td>
<td>19</td>
</tr>
<tr>
<td>Using Protection Levels</td>
<td>19</td>
</tr>
<tr>
<td>Defining Protection Levels</td>
<td>20</td>
</tr>
<tr>
<td>Web Applications</td>
<td>20</td>
</tr>
<tr>
<td>Mobile Access Web Applications</td>
<td>21</td>
</tr>
<tr>
<td>Web Applications of a Specific Type</td>
<td>21</td>
</tr>
<tr>
<td>Configuring Web Applications</td>
<td>21</td>
</tr>
<tr>
<td>Link Translation</td>
<td>27</td>
</tr>
<tr>
<td>Link Translation Domain</td>
<td>30</td>
</tr>
<tr>
<td>Web Application Features</td>
<td>31</td>
</tr>
<tr>
<td>File Shares</td>
<td>34</td>
</tr>
<tr>
<td>File Share Viewers</td>
<td>34</td>
</tr>
<tr>
<td>Configuring File Shares</td>
<td>34</td>
</tr>
<tr>
<td>Using the $$\text{user}$ Variable in File Shares</td>
<td>36</td>
</tr>
<tr>
<td>Citrix Services</td>
<td>37</td>
</tr>
<tr>
<td>Citrix Deployments Modes - Unticketed and Ticketed</td>
<td>37</td>
</tr>
<tr>
<td>Configuring Citrix Services</td>
<td>37</td>
</tr>
<tr>
<td>Web Mail Services</td>
<td>40</td>
</tr>
</tbody>
</table>
Protection Levels for Native Applications

Single Sign On ............................................................................................................ 44
Supported SSO Authentication Protocol................................................................. 44
HTTP Based SSO ........................................................................................................ 44
  HTTP Based SSO Limitation .................................................................................. 45
Web Form Based SSO ................................................................................................. 45
  Application Requirements for Easy Configuration ................................................. 46
  Web Form Based SSO Limitations ........................................................................ 46
Application and Client Support for SSO ................................................................. 46
Mobile Access Client Support for SSO ................................................................. 47
Basic SSO Configuration .......................................................................................... 47
Basic Configuration of Web Form SSO ................................................................. 48
Advanced Configuration of SSO .............................................................................. 48
  Configuring Advanced Single Sign On ............................................................... 48
  Configuring Login Settings .................................................................................. 49
Advanced Configuration of Web Form SSO ............................................................. 50
Sign In Success or Failure Detection .................................................................... 50
Credential Handling .................................................................................................. 51
Kerberos Authentication Support .......................................................................... 51
VPN Clients ................................................................................................................ 53
  SSL Network Extender ....................................................................................... 53
  SSL Network Extender Network Mode ............................................................. 54
  SSL Network Extender Application Mode ......................................................... 54
Configuring VPN Clients ......................................................................................... 56
  Office Mode ........................................................................................................ 56
Configuring SSL Network Extender Advanced Options ........................................ 58
  Deployment Options ............................................................................................ 58
  Encryption .......................................................................................................... 58
  Launch SSL Network Extender Client .............................................................. 58
Endpoint Application Types ..................................................................................... 59
  Application Installed on Endpoint Machine ....................................................... 59
  Application Runs Via a Default Browser .......................................................... 59
  Applications Downloaded-from-Gateway .......................................................... 59
Configuring Authorized Locations per User Group .............................................. 60
  Ensuring the Link Appears in the End-User Browser .......................................... 61
Configuring a Simple Native Application ............................................................ 61
  General Properties ............................................................................................... 61
  Authorized Locations .......................................................................................... 61
  Applications on the Endpoint Machine ............................................................. 61
  Completing the Native Application Configuration ............................................ 62
Configuring an Advanced Native Application ..................................................... 62
  Configuring Connection Direction ...................................................................... 62
  Multiple Hosts and Services .............................................................................. 63
  Configuring the Endpoint Application to Run Via a Default Browser ................ 63
  Automatically Starting the Application ............................................................. 63
  Making an Application Available in Application Mode ..................................... 64
  Automatically Running Commands or Scripts .................................................. 64
Protection Levels for Native Applications .............................................................. 65
  Protection Levels in R71 and Higher Gateways .................................................. 65
  Defining Protection Levels ................................................................................... 66
Configuring the Secure Workspace Policy ...................................................... 108
Secure Workspace End-User Experience ....................................................... 110
Endpoint Compliance Updates ........................................................................ 111
Working with Automatic Updates .................................................................. 112
Performing Manual Updates ......................................................................... 112

**Advanced Password Management Settings** .............................................. 113
Password Expiration Warning ........................................................................ 113
Managing Expired Passwords ........................................................................ 113
Configuring Password Change AfterExpiration ............................................. 113

**Mobile Access Blade Configuration and Settings** .................................. 115
Interoperability with Other Blades .................................................................. 115
IPS Blade ......................................................................................................... 115
Anti-virus and Anti-malware Blade ................................................................. 116
IPSec VPN Blade ............................................................................................ 117
Portal Settings ................................................................................................ 117
Portal Accessibility Settings ........................................................................... 117
Portal Customization ....................................................................................... 118
Localization Features ....................................................................................... 119
Alternative Portal Configuration ...................................................................... 120
Server Certificates .......................................................................................... 120
Obtaining and Installing a Trusted Server Certificate .................................. 120
Viewing the Certificate ................................................................................... 122
Web Data Compression .................................................................................... 122
Configuring Data Compression ....................................................................... 122
Using Mobile Access Clusters ......................................................................... 123
The Sticky Decision Function ......................................................................... 123
How Mobile Access Applications Behave Upon Failover .............................. 123

**Troubleshooting Mobile Access** ................................................................. 125
Troubleshooting Web Connectivity ................................................................. 125
Troubleshooting Outlook Web Access ............................................................. 125
Troubleshooting OWA Checklist ..................................................................... 125
Unsupported Feature List ................................................................................ 126
Common OWA problems ................................................................................ 126
Troubleshooting Authentication with OWA .................................................... 126
Troubleshooting Authorization with OWA ...................................................... 127
Troubleshooting Security Restrictions in OWA .............................................. 128
Troubleshooting Performance Issues in OWA ................................................. 128
Saving File Attachments with OWA ............................................................... 130
Troubleshooting File Shares ......................................................................... 131
Troubleshooting Citrix .................................................................................... 131
Troubleshooting Citrix Checklist ................................................................... 131

**Index** ........................................................................................................ 133
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.

In This Chapter

Mobile Access Applications 8
Mobile Access Management 9
SSL Network Extender 9
Commonly Used Concepts 9
Mobile Access Security Features 11
User Workflow 12

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.

- 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 (on page 19).
For information about native applications, see Native Applications for Client-Based Access (on page 53).

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.
Commonly Used Concepts

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. Two factor authentication with a DynamicID one time password can also be configured.

Authorization

Authorization determines if and how remote users access the internal applications on the corporate LAN. If the remote user is not authorized, he/she will not be granted access to the services provided by the Mobile Access gateway.

After being authenticated, the user will attempt to use an application. To access a particular application, the user must be authorized to do so. The user must belong to a group that has been granted access to the given application. In addition, the user must satisfy the security requirements of the application, such as authentication method and endpoint health compliance.

For more information, refer to Managing Access to Applications (on page 17)

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 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.

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 both 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.

For more information, refer to Endpoint Compliance Enforcement (on page 89).

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.

For more information, refer to Secure Workspace (on page 102).

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.

For more information, refer to Protection Levels (on page 19).
Session

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.

For more information refer to Session Settings (on page 86).

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.
   For more information, see the R75 IPS Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11663).
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.
   For more information, refer to Endpoint Compliance Enforcement (on page 89).
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.
   For more information, refer to Secure Workspace (on page 102).
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.
   For more information, refer to the Web Application - Protection Level page ("Web Application — Protection Level Page" on page 25).
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**

The user workflow comprises the following 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**

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

> **Note** - Various popup blockers may interfere with various aspects of portal functionality. You should recommend to users that they configure popup blockers to allow pop-up 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.

Once 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

See Localization Features (on page 119) for more details.

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.
Chapter 2

Getting Started with Mobile Access

In This Chapter

Recommended Deployments 14
Basic SmartDashboard Configuration 15
Setting up the Mobile Access Portal 16
Managing Access to Applications 17

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 an 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.

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.
Basic SmartDashboard Configuration

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

1. **Enable the Mobile Access blade on a Security Gateway or Security Gateway cluster:** In the **General Properties** page of a Security Gateway, in the **Network Security** tab, select **Mobile Access**.
   
   **Note** - The Mobile Access blade can only be enabled on Security Gateways running on the SecurePlatform Operating System.

2. When you enable the Mobile Access blade:
   - You are automatically given a 30 day trial license for 10 users.
   - The Mobile Access Wizard (on page 15) opens. Follow the instructions to easily 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.
   - A rule allowing HTTPS (TCP/443) traffic is automatically added to the rule base as an Implied Rule.
   - For easier end user access, it is recommended that the Security Gateway accept HTTP (TCP/80) traffic.
   - Mobile Access requires access to DNS servers in most scenarios.
   - The Security Gateway may need access to: WINS servers, LDAP, RADIUS, or ACE servers for authentication, 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**.

The Mobile Access Wizard

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

Essentially, the Wizard guides you through the process of:

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

**Step 1: Configure a Web Application**

Configure a Web application that users will connect to remotely.

If you have an internal Web application, for example, an organizational intranet site or Microsoft Outlook Web Access, it is recommended to configure access to that site. Enter its **URL** and, optionally, a **display name**, which is how the application will appear in the portal, for example, Company Intranet.

**Note** - Domino Web Access (iNotes) applications cannot be defined as the internal Web application using the First Time Wizard.

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

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

**Step 2: Configure Authorized Users**

Configure the user or user groups that are allowed to access the Web application/s that you configured in Step 1.
Make a selection to choose which users or groups can access the configured application:

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

### Configuring Users or Groups from an Active Directory

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

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

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

Under **Authorized Users**, select one of the following:

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

### Step 3: Configure the Web Portal

Enter the primary URL for the portal. The default is the `<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 authentication. All portals on the same IP address use the same certificate.

### The Mobile Access Wizard is Complete

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

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

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

### 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 by entering https://<Gateway_IP>/sslvpn, where `<Gateway_IP>` is:

- Either the FQDN that resolves to the IP address of the Security Gateway
- or
- The IP address of the Security Gateway
If remote users enter http://<Gateway_IP>/sslvpn, they will automatically be redirected to the portal using HTTPS.

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

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

To change the IP address used for the user portal:
From the properties of the Gateway object, select Mobile Access > Portal Settings.

Managing Access to Applications

Once remote users are authenticated (recognized and approved), Mobile Access allows the users to access the appropriate applications for that user. This process is called Authorization.

Authorization is done by enforcing an access control policy in the Policy page of the Mobile Access tab. Access control policies are applied to groups, not individual users.

Remote users, once authenticated, can only access those applications that have been authorized for their groups. In other words, for access to be granted, Mobile Access checks for:

- **Access rights** - Does the remote user belong to a group which is allowed to access the application?
- **Security requirements** - Does the remote user meet the security restrictions as defined in the application's Protection Level?

For example, a Web application for ordering office supplies is less sensitive than an application that controls money transfers. All remote users can be given access to the office-supplies application, identifying themselves with a user name and password. However, the money transfer application may be restricted to an exclusive group of remote users and require them to authenticate using certificates. In this way, the level of security surrounding an application is based on the application’s Protection Level and the user group.

Configuring Mobile Access Policy

Configure Access Control in Mobile Access using SmartDashboard by:

- Defining users and assigning them to user groups
- Defining applications and associating them with the user groups.

In addition, Mobile Access associates each application with a Protection Level, a security requirement that the remote user must satisfy before being given access to the application.

To configure access to applications:

1. Define Mobile Access applications that you want to make accessible to remote users: Web applications, file shares, Citrix services, Web mail applications and/or native applications.
   In the definition, you may associate a Protection Level with the application.
2. Define users (if necessary), user groups, and (if necessary) associate users with groups.
   Note - Nested user groups are not supported by the Mobile Access policy.
3. Define the Policy rules, to associate user groups, applications, and Mobile Access gateways:
   a) Go to the Policy page of the Mobile Access tab.
b) Click **Add**. The **Access to Applications** window opens.

c) In the **User Groups** tab, click **Add** to add one or more user groups.

d) In the **Applications** tab, click **Add** to add one or more Mobile Access applications.

e) In the **Install On** tab, click **Add** to add one or more Mobile Access gateways or Mobile Access clusters.

Note -

- **All Users** means all User Groups. If users are not assigned to a user group, they will not be able to access any applications, even if **All Users** is selected for that application.
- *Any means all*. For example, an All Users/*Any/*Any rule means all user groups can access all of the defined applications on all of the defined Mobile Access gateways.

4. Install the policy.
Chapter 3

Applications for Clientless Access

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.

In This Chapter

Protection Levels 19
Web Applications 20
File Shares 34
Citrix Services 37
Web Mail Services 40
Native Applications 41
DNS Names 42

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 an Mobile Access application:
1. From the Properties window of an 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 via a default browser, and so cannot be defined as a Web application. If that is the case, use a native application.
Mobile Access Web Applications

When creating a Mobile Access Web application, you give the application a name, define servers using host or DNS names, specific directories, specific services, and an associated Protection Level. For example, the definition in the table below turns the "Example" website into a single Web application.

<table>
<thead>
<tr>
<th>Name</th>
<th>DNS name or Host IP</th>
<th>Directories</th>
<th>Services</th>
<th>Endpoint Compliance Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>Any</td>
<td>HTTP, HTTPS</td>
<td>Permissive</td>
</tr>
</tbody>
</table>

Note - You can define an application using a DNS name suffix, such as *.example.com, rather than a specific DNS name. This means that every URL ending with example.com is included in this application. In this case, the match is only for *.example.com, not **.example.com. Also, *.a.b will match to c.a.b, but not to c.d.a.b.

The same host with a different directory could be a separate Web 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.

The following 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, and 2007.

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.

   ![General Properties Page](image)

   **General Properties**
   - **Name:** WebCalendar
   - **Color:** 
   - **Comment:**
   - **Application type**
     - [ ] This application has a specific type:
       - [ ] Domino Web Access
       - [ ] Outlook Web Access

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.

   Authorized Locations

   Allow access to these locations only

   Servers:
   - Host or DNS name: [WebCalendarServer]
   - Multiple hosts

   Directories:
   - Allow access to any directory
   - Allow access to specific directories

      Directory

      New... Edit... Delete

   [ ] Application directories are case sensitive

   Services:
   - Default
     - [ ] http
     - [ ] https
   - Advanced

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.
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 — Single Sign-On Page

- Go to the Single Sign-On page.

For configuration details, see Single Sign On (on page 44).
**Web Application — Protection Level Page**

1. Go to the Protection Level page.

   ![Protection Level](image)

   **Security Requirements for Accessing this Application**
   - [ ] This application relies on the security requirements of the gateway
   - [x] This application has additional security requirements, specified by the following protection level:
     - [ ] Permissive
     - [ ] Manage...

   **Browser Caching on the Endpoint Machine**
   - [ ] Allow caching of all content
   - [ ] Allow caching of these content types:
     - [x] Images
     - [x] Scripts
     - [ ] HTML
   - [ ] Prevent caching of all content

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.
   - **Browser Caching on the Endpoint Machine** allows you to control caching of web application content in the remote user's browser.
     - [ ] Allow caching of all content
     - [ ] Prevent caching of all content

**Configuring Web Content Caching**

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

However, 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 allow opening such files, perform the following steps:**

1. Configure the Protection Level to **Allow caching of all content**.
2. To allow caching Microsoft Office documents, add them to the HTML caching category by editing the Apache configuration file `$CVPNDIR/conf/httpd.conf` and uncommenting the `CvpnCacheGroups` directives dealing with Microsoft Office documents. Perform the following steps:
   a) Run: `cvpnstop`
   b) Backup and edit the `httpd.conf` file.
   c) In cluster setups, repeat these steps for all cluster members.
   d) Run: `cvpnstart`
3. Install Policy.

**Web Application — Link Translation Page**

1. Go to the **Link Translation** page.

   - **Link Translation**
     
     | Translation Methods |
     |---------------------|
     | Links on pages returning from this application will be translated: |
     | Using the method defined on the gateway accessing this application. |
     | Using the following method: |
     | URL Translation. |
     | Hostname Translation (must be supported by the gateway). |

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** is the Link translation method that will always be used for this application. Either
     - **URL Translation**, which is supported by the Mobile Access gateway with no further configuration, or
     - **Hostname Translation**, for which further configuration is required. See Preparing Mobile Access for Hostname Translation (on page 29).

**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 36).

**Completing the Configuration of the Web Application**

1. Go to the **Policy** page of the Mobile Access tab.
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 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 two methods of Link Translation: URL Translation and Hostname Translation.

- URL Translation works by default, out of the box, and can handle the large majority of websites.
- Hostname Translation provides dramatically improved performance for Mobile Access gateways and end users, resulting in faster Web access and fewer connectivity issues. Additionally, Hostname Translation allows Mobile Access to access a wider range of websites, due to enhanced support for HTML pages, JavaScript, VBscript, and Web applications (such as the SAP Portal).

How Translated URLs Appear in a Browser

The following example compares how a URL appears to users in their browser with Hostname Translation versus with URL Translation. In this example, an HTTP request, sent via a gateway located at ssl.example.com to the destination URL http://www.example.com/path, appears as follows:

- URL With Hostname Translation:
  https://c-ds1q-itfgppae7oq.ssl.example.com/path
  Note that the seemingly random character string, c-ds1q-itfgppae7oq, represents the destination URL.
- URL With URL Translation:
  https://ssl.example.com/Web/path,CVPNHost=www.example.com,CVPNProtocol=http
**Link Translation Per Gateway or Per Application**

For the majority of websites and Web applications, Hostname Translation is the preferred method of performing Link Translation. Many sites work better (or only) with Hostname Translation. However, a few sites may work better (or only) with URL Translation.

Link Translation can be configured to accommodate the distinctive requirements of the Web application or the gateway through which the applications are accessed. It is possible, for example, to configure a particular Mobile Access application to work with URL translation, while all other applications supplied by the gateway use Hostname Translation.

The workflow for configuring Link Translation is as follows:

1. **Configure the Link Translation methods that are supported by Mobile Access.** URL translation is always supported by the gateway. Hostname Translation requires further configuration in order to be supported.

2. **Configure the default Link Translation method used by Mobile Access.** When Hostname Translation has been enabled on Mobile Access, the default Link Translation method used by Mobile Access applications can be chosen. Each Mobile Access application can be configured override the default translation method.

3. **Configure the Links Translation method used by the Web application.** This can be the method specified by the gateway through which the application is accessed. Alternatively, the application can be configured to always use a particular translation method.

**About Hostname Translation**

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.

Hostname Translation is an optional feature, which is disabled by default and requires additional (one time) configuration. For most Mobile Access deployments, Hostname Translation works well with its default configuration.

In order to use Hostname Translation, it is necessary to add a record to your organization's DNS server. Additionally, defining a wildcard SSL certificate for the Mobile Access gateway is strongly recommended.

**Wildcard SSL Certificates**

Using wildcard SSL certificates with Hostname Translation eliminates certificate warnings generated when browsers attempt to access URLs pointing to different sub-domains behind a gateway. For example, If a gateway is located at ssl.example.com (the FQDN), you should purchase a certificate issued to *.ssl.example.com. This certificate covers the fully qualified sub-domains of the parent domain, such as a.ssl.example.com and b.ssl.example.com.

When Mobile Access uses a fixed domain certificate, or a self-signed certificate, client browsers issue certificate warnings whenever they attempt to access Web applications in a sub-domain behind the Mobile Access gateway. This occurs because each Web application's URL is translated to a different Mobile Access host name.

**Wildcard DNS Server Records**

In order to use Hostname Translation, you must configure the DNS server to resolve Mobile Access sub-domains (such as *.ssl.example.com) to the Mobile Access IP address. For example, If a gateway is located at ssl.example.com (the FQDN), configure the DNS to resolve *.ssl.example.com to the Mobile Access IP address. This wildcard includes all sub-domains of the parent domain, such as a.ssl.example.com and b.ssl.example.com. The parent domain ssl.example.com must also be defined as a separate DNS record.

**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 as well: portal.ssl.example.com.
Configuring Link Translation

Preparing Mobile Access for Hostname Translation

To prepare your Mobile Access gateway to use Hostname Translation:
1. Obtain and install a wildcard SSL certificate for the Mobile Access gateway (recommended).
   It is strongly recommended that you obtain a wildcard SSL certificate (for example, *.ssl.example.com) from a trusted (well-known) certificate authority for the Mobile Access domain. A certificate for Mobile Access from a trusted CA allows users to log in to Mobile Access without receiving certificate warning pop-up. For instructions, see Obtaining and Installing a Trusted Server Certificate (on page 120).
2. Add sub-domain records to the DNS server.
   Configure the DNS Server used to resolve the Mobile Access host name in order to:
   • Resolve all Mobile Access sub-domains to the Mobile Access IP Address (for example, *.ssl.example.com).
   • Resolve the parent domain (such as ssl.example.com) to the same IP address. This allows users to browse directly to the Mobile Access portal by using its FQDN.

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. It is possible, for example, to configure a particular Mobile Access application to work with URL translation, while all other applications supplied by the gateway use Hostname Translation.

To configure Link Translation:
1. Configure the supported link translation methods:
   a) In the Mobile Access tab, select Additional Settings > Link Translation.
   b) Select a gateway and click Edit.
      The Link Translation page of the Mobile Access gateway opens.
   c) To enable support for Hostname Translation, under Supported Translation Methods, select Hostname Translation (leave URL Translation (always supported) selected.)
   d) Create or select a DNS Name object that specifies the parent DNS names of the Mobile Access gateway. Do not include the wildcard prefix (i.e. "*") in the DNS name. For example, configure "ssl.example.com" as the DNS Name object. For further information, refer to DNS Names (on page 42).
2. Configure the default link translation method used by Mobile Access:
   Under Default Translation method, select the default link translation method for accessing Web applications. This method is used unless a different method is specified in the application itself. Select either
   • URL translation or
   • Hostname Translation.
3. Configure the Link Translation method used by the application:
   a) In the Link Translation page, Link Translation Method Settings on Applications section, select an application and click Edit.
      The Link Translation page of the Mobile Access application opens.
   b) Select the Translation methods. Either
      ▪ Use the method specified in the Mobile Access gateway through which this application is accessed (as chosen in step 2), or
      ▪ Select the method that will always be used to access this application.
   c) If necessary, click Advanced Hostname Translation Settings....
      The Advanced Hostname Translation Settings window opens.
   d) Select the appropriate Cookies Handling Mode:
      ▪ On the gateway is the default setting. 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.
Web Applications

- **On the endpoint machine** can be used if the default setting causes the JavaScript (from the internal servers that run on the client browser) that handles HTTP cookies to fail. With this setting, Mobile Access passes HTTP cookies to the browser.

  e) Click OK twice.

4. Examine the Link Translation configuration summary on the **Link Translation** page.

**Portal Access with Hostname Translation**

When Hostname Translation is enabled and configured, users access the Mobile Access Portal by entering the URL in their browser in any of the following formats. These examples assume that the Mobile Access FQDN is ssl.example.com.

- http://ssl.example.com/
- http://portal.ssl.example.com/
- https://portal.ssl.example.com/
- https://ssl.example.com/

**Note** - The last option results in a certificate warning stating that the certificate does not match the destination host. This is due to a limitation of the SSL Protocol.

**Link Translation Issues**

The following Link Translation configuration tips apply to Web applications.

- To allow Web sites that use ActiveX and streaming media to work with Hostname Translation, configure Mobile Access Web applications to **Allow caching of all content**. This is configured in the **Endpoint Compliance** 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,
  ```
  
  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 "About Hostname Translation" on page 28)). 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.
To use the feature, 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.

**Configuring the Link Translation Domain**

The Link Translation Domain is configured in GuiDBedit, the Check Point Database Tool. Select Connectra_Global_Properties and search for translation_domain.

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 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** - Be sure to 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 may want to 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.

**Performance Enhancement Features**

The following features boost Mobile Access’s performance and increase security when using Web Applications in Mobile Access. The features are activated through changes in the configuration files.

  **Note** - It is strongly recommended to back up your configuration files before making any changes.

**Optimize Authorization Cache**

The Optimize Authorization Cache feature boosts performance for Web applications. When the feature is enabled, the authorization history of users is stored in a cache. Mobile Access can use the stored authorization information instead of looking it up again. For example, if a user was already authorized to
access a specific location, then Mobile Access allows the user to access the same location again without looking up the authorization rules again.

By default, Optimize Authorization Cache is enabled for all applications, whether they use URL Translation or Hostname Translation. To change the settings, edit the \$CVPNDIR/conf/http.conf configuration file.

The Optimize Authorization Cache setting options are as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CvpnBoostPerformance On</td>
<td>Feature is enabled for all applications (default)</td>
</tr>
<tr>
<td>CvpnBoostPerformance Off</td>
<td>Feature is disabled for all applications</td>
</tr>
<tr>
<td>CvpnBoostPerformance UT</td>
<td>Feature is only enabled for applications using URL Translation</td>
</tr>
<tr>
<td>CvpnBoostPerformance HT</td>
<td>Feature is only enabled for applications using Hostname Translation</td>
</tr>
</tbody>
</table>

Optimize Authorization Cache for Domino Web Access or Outlook Web Access applications will only be effective when Reuse TCP Connections is also enabled.

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.

Reuse TCP Connections

The Reuse TCP Connections feature allows the network to reuse TCP connections that would otherwise be closed. Specifically, 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.

Statically Obscuring DNS Host Names

In versions prior to R66.1, when using Hostname Translation, each time a website is visited, the DNS host is dynamically obscured in a different way. With R66.1 and later, the default is that the obscured host is always the same for each user. This utilizes the browser cache and optimizes Web browsing.

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 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 set useStaticObscureKey true

You will be asked whether to first back up the current $CVFNDIR/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.

**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 “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. 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, or ignore as the value.

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 the cluster object table.

**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 to complete the certificate Export Wizard.

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.

### Authorized Locations

![Image](https://via.placeholder.com/150)

**Servers**
- **Host or DNS name**: FileServer
- **Multiple hosts**: Edit...

**File Shares**
- Allow access to any file share
- Allow access to specific file shares

<table>
<thead>
<tr>
<th>File Share</th>
<th>Pub</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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**, **$$user**, or **My_share$**, without any slashes. Do not specify a subdirectory inside a share. The **$$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 \myserver\alice.

**Note** - When two or more overlapping file share applications are configured (for example, one for any share and one for a specific share on the same host), it is undefined which application settings are in effect.

### 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. However, the IP address of the host is resolved by the DNS Server that is defined on Mobile Access itself (and 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.

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

For more information, see Single Sign On (on page 44).

File Share Application — Protection Level Page

1. Go to the Protection Level page of the File Share Application object.

<table>
<thead>
<tr>
<th>Protection Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Requirements for Accessing this Application</td>
</tr>
<tr>
<td>This application relies on the security requirements of the gateway</td>
</tr>
<tr>
<td>This application has additional security requirements, specified by the following protection level:</td>
</tr>
<tr>
<td>Permissive ▼ Manage...</td>
</tr>
</tbody>
</table>

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 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

It is possible to configure personalized user locations that use the login name of the currently logged in user. To do this, use the $$user$$ variable 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$$ is resolved for user Alice as \host\Pub\Alice and for user Bob as \host\Pub\Bob.
For more information about the `$$user` variable, see Using the Login Name of the Currently Logged in User (on page 26).

## 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.

**Note** - 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. The following subsections explain the fields in each page.

### Before Configuring Citrix Services

Mobile Access's server certificate must be Fully Qualified Domain Name (FQDN)-based i.e. issued to Mobile Access's FQDN, for example `www.example.com`.

Before configuring Citrix Services, change the Mobile Access server certificate to one that was issued to the Fully Qualified Domain Name (FQDN). This is required in order to comply with the accepted Citrix standards for server certificates. Additionally, end-users must browse to Mobile Access using its FQDN, and the FQDN must be routable from their network.

For instructions about how to install server certificates, see Mobile Access Server Certificates (see "Server Certificates" on page 120).

If your Web Interface server is configured to deploy ICA Web clients and Mobile Access's server certificate is issued by a private CA, the certificate's public key must be installed on the client side browser in order for ICA Web Client to function properly. Mobile Access's 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. Obtain 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, Thus, using STA servers is not necessary.

To retrieve the host name or IP
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 retrieve 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 — Presentation Servers Page
- Go to the Presentation servers page of the Citrix Service object.
  In this page you can either allow access to all Presentation Servers or restrict access to defined Presentation Servers.
  
  Note: 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**

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.

For more information, see Single Sign On (on page 44).

**Citrix Service — Protection Level Page**

1. Go to the Protection Level page of the Citrix 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.

   ![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. Obtain 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, Thus, using STA servers is not necessary.

**To retrieve the Host name/IP:**
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 retrieve 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, choose 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 (on page 44).

**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 53).
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.

Also, 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.

Note - The resolving of DNS Name is done using the DNS server specified on Mobile Access itself (by using the sysconfig command from the console).

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:

- In SmartDashboard, in the Mobile Access tab, in the Additional Settings > Network Accessories > Name Resolution page.

- From Mobile Access itself, using either the console, or the SecurePlatform Web User Interface.
  - To define the DNS server using the Mobile Access console, run sysconfig, and select 3) Domain Name Servers.
  - To define the DNS server using the SecurePlatform Web User Interface, connect your browser to the SecurePlatform Administration Portal, and go to the Network > DNS page.

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 36).
Chapter 4

Single Sign On

Single Sign On (SSO) eliminates the need to reauthenticate to an application when accessing it for a second time — either during an existing Mobile Access session, or even between Mobile Access sessions.

The authentication credentials used for logging in to the Mobile Access portal can be re-used automatically by Mobile Access 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 back in from a different client machine.

In This Chapter

- Supported SSO Authentication Protocol
- HTTP Based SSO
- Web Form Based SSO
- Application and Client Support for SSO
- Basic SSO Configuration
- Advanced Configuration of SSO
- Advanced Configuration of Web Form SSO
- Kerberos Authentication Support

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:

**Figure 4-2** HTTP Authentication Browser-Specific Credential Request Form

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.

**Figure 4-3** Web Form Based SSO Example

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.

**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>
</tbody>
</table>
Basic SSO Configuration

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 Connectra tab, select the Additional Settings > Single Sign On page.

   **Single Sign On**

   **Single Sign On Settings on Applications**

<table>
<thead>
<tr>
<th>Name</th>
<th>Single Sign On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Services</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>CitrixOffice</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>Corporate Email</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>Library</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>Web Calendar</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>Web Documentation</td>
<td>Off</td>
<td></td>
</tr>
</tbody>
</table>

   - [New...](#)  [Edit...](#)  [Delete](#)

2. In the Single Sign On page, select an application and click **Edit**. The Single Sign On page of the application window opens.

   **Single Sign On**

   - **Turn on Single Sign On for this application.**
     - Application Single Sign On Method
       - When a user signs in to this application:
         - Prompt users for their credentials, and store them for future use
         - Advanced:

   - [Edit...](#)

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 Connectra 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.

**Advanced Configuration of SSO**

The following configuration instructions apply to both HTTP based SSO and 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 50).

**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....

The Single Sign On Methods table summarizes the available single sign on methods.
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>Prompt users for their credentials, and store them for future use</td>
<td>On</td>
<td>No</td>
<td>Yes</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>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>
</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 along with the user name and password, but if one of the Accept the portal credentials from the gateway... Single Sign On methods are selected, Mobile Access does not know the domain because the user does not supply it with the portal credentials. Therefore, 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
  Users accessing the application login page for the first time see a popup message saying that their credentials will be stored for future access.
- Allow the users to specify that their credentials for this application will not be stored
  Users accessing the application login page for the first time see a popup 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:
- No HTTP redirect (301, 302) upon authentication success
  OR
- No redirect upon authentication failure.
You can specify different criteria for:
- Sign In Success or Failure Detection (on page 50).
- Credential Handling (on page 51).

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.
   Use the following URL format:
   <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 with the following information:
   • 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 the following two macros:
     ▪ $USER NAME resolves to the user name stored on Mobile Access.
     ▪ $PASSWORD resolves to the password stored on Mobile Access.

Note - 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 authentication protocol, which allows people and computers to securely identify themselves over a non-secure network. It is the Microsoft default authentication protocol in Windows 2000 and later versions. Microsoft IIS, and other web servers, can use Kerberos via the Negotiate method in HTTP authentication headers.

Kerberos Authentication is supported for Web Applications (HTTP(S)). Mobile Access can authorize against Kerberos servers on behalf of users.

By default, Kerberos support is turned off.
To turn on support for Kerberos:

1. Replace `/etc/krb5.conf` with a file suitable for the domain. The file must have the following template. Replace any string containing “your” with the appropriate values:

   ```
   [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
   ```

   • 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.
   • For each realm you can have more than one domain controller, in this case, instead of the admin_server statement, use several statements of the form:

2. 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.

3. Check that Kerberos is configured correctly.
   a) From the Mobile Access gateway command line, type:
      ```
      kinit your-ad-username
      ```
      If there are several realms, the kinit syntax works for 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:**
   b) Type the password and press Enter.
      There should be no error messages
   c) Type `klist`
      You should get a listing of something called "Ticket cache", with one ticket in it.
   d) You must delete the list. To do so, type `kdestroy`

4. Use the cvpnd_settings command to enable Kerberos:
   ```
   cvpnd_settings set useKerberos true
   cvpnd_settings listAdd kerberosRealms YOUR.AD.NAME
   cvpnd_settings listAdd kerberosRealms YOUR.OTHER.AD.NAME
   ```

5. Restart the Mobile Access services by running cvpnrestart.

6. For a cluster setup, repeat step 1 to step 5 on each cluster member.
Chapter 5

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.

In This Chapter

VPN Clients 53
Configuring VPN Clients 56
Configuring SSL Network Extender Advanced Options 58
Endpoint Application Types 59
Configuring a Simple Native Application 61
Configuring an Advanced Native Application 62
Protection Levels for Native Applications 65
Adding New Downloaded-from-Gateway Endpoint Applications 67
Configuring Downloaded-from-Gateway Endpoint Applications 71

VPN Clients

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.

Note - Beginning with version R71, Endpoint Connect, SecureClient Mobile, and Abra are only available through the IPSec VPN blade. To use these VPN clients, you must have the IPSec VPN blade activated.

SSL Network Extender

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

Once you have enabled the Mobile Access blade on a gateway, SSL Network Extender only works through Mobile Access and its policy should be configured 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 can work from the IPSec VPN blade and its policy should be configured in the main security rule base.
Note - 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.

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 12).

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 or Network 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.

For the latest information, see http://www.opsec.com/solutions/snx_support.html (http://www.opsec.com/solutions/snx_support.html).
<table>
<thead>
<tr>
<th>Partner/ Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Telnet / SSH</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Microsoft Telnet (Command Line)</td>
<td>2000 XP</td>
</tr>
<tr>
<td>Microsoft</td>
<td>HyperTerminal</td>
<td>5.1</td>
</tr>
<tr>
<td>Putty</td>
<td>Putty</td>
<td>0.55</td>
</tr>
<tr>
<td>VanDyke</td>
<td>SecureCRT</td>
<td>4.1</td>
</tr>
<tr>
<td><strong>Database Clients</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rational</td>
<td>ClearQuest</td>
<td>2003.06.00.436.000</td>
</tr>
<tr>
<td>Siebel</td>
<td>Siebel Client</td>
<td>7</td>
</tr>
<tr>
<td><strong>TN3270</strong></td>
<td></td>
<td></td>
</tr>
<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>
<tr>
<td><strong>FTP</strong></td>
<td></td>
<td></td>
</tr>
<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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td><strong>E-Mail (POP3, IMAP, SMTP)</strong></td>
<td></td>
<td></td>
</tr>
<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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2003 SP1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.5.3</td>
</tr>
<tr>
<td><strong>Web Browser (HTTP, HTTPS, Passive FTP)</strong></td>
<td></td>
<td></td>
</tr>
<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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.0.4</td>
</tr>
<tr>
<td><strong>Terminal Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Remote Desktop Connection</td>
<td>XP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2000</td>
</tr>
<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>
</tbody>
</table>
Configuring VPN Clients

Configure SSL Network Extender in Gateway Properties > Mobile Access > SSL Clients. SSL Network Extender is automatically enabled when the Mobile Access blade is turned on.

Choose from the following options:

- **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.

### 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, but 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.

See the [R75 VPN Administration Guide](http://supportcontent.checkpoint.com/documentation_download?ID=11675) for more information about Office Mode.

---

<table>
<thead>
<tr>
<th>Partner/ Company</th>
<th>Client</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<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><strong>Productivity Suites</strong></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. This is due to the fact the mail is encrypted in SSL before the scanning takes place.
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 Connectra 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 a New Downloaded-from-Gateway Endpoint Application (see "Adding New Downloaded-from-Gateway Endpoint Applications" on page 67).

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:

<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>
</tbody>
</table>
### Endpoint Application Types

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 71).

### 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:

#### Downloaded-from-Gateway Add-On 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 queueing, browsing the LAN for Windows shares, and more</td>
</tr>
</tbody>
</table>

For configuration details, see Configuring Downloaded-from-Gateway Endpoint Applications (on page 71).

### 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](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 Machine

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:
       - 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*. 

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.
• If the location of the application is in the path of the endpoint machine, only the application name need be entered. For example ftp.exe
• Parameters are used to pass additional information to the applications on the endpoint machine, and to configure the way they are launched. Can include $$user, which represents the user name of the currently logged-in user.

Completing the Native Application Configuration

If necessary, configure VPN clients. See Configuring VPN Clients (on page 56).

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 one of the following options 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 allows you 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).

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 option should not be used to launch applications that require connectivity to the organization.

Note that this problem only occurs with SSL Network Extender Application Mode. In Network Mode, applications automatic start of applications when SSL Network Extender is disconnected works correctly.
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 allows you to 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:

1. Who connect with Application Mode do not see it in their list of applications.
2. With SecureClient Mobile clients 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 64).

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 65).

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). Adding a New Downloaded-from-Gateway Endpoint Application (see "Adding New Downloaded-from-Gateway Endpoint Applications" on page 67).
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. In the Automatically start this application section of the Advanced page, check 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 page 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.

**Figure 5-4** Protection Level Page of the File Share Application Object

### 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.

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

1. From the Properties window of an 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.

**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 New Downloaded-from-Gateway Endpoint Applications

It is possible to 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.

Procedure: Adding a New Downloaded-From-Gateway Application

To add a new downloaded-from-gateway application you must first place the application in the relevant directory on the gateway, and then use the Database Tool (GuiDBedit) to specify the properties of the new downloaded-from-gateway application.

Proceed as follows:
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 $CVPNDIR/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.
   You will now see the embedded_applications table.
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 as follows:

<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 Edit Endpoint Application window.</td>
</tr>
</tbody>
</table>
Adding New Downloaded-from-Gateway Endpoint Applications

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>embedded_application_type</td>
<td>The type of downloaded-from-gateway application. Choose one of the options in the Valid Values 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 $CVPNDIR/htdocs/SNX/CSHELL (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 Edit Endpoint Application window.</td>
</tr>
<tr>
<td>pre_custom_params</td>
<td>Parameters concatenated before the server_name_required_params 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 server_name_required_params field. Can be left blank.</td>
</tr>
<tr>
<td>type</td>
<td>Leave as embedded_application.</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

The following 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.

Proceed as follows:

1. Compress the ssh2.jar and WinSsh2.exe application files into ssh2.cab and WinSsh2.cab
   Do this by running:
   ```
   # 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, you must save the files ssh2.jar and WinSsh2.exe to $CVPNDIR/htdocs/SNX/CSHELL with the proper permissions.

3. Place 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 as follows: SSH2 Java Application
Adding New Downloaded-from-Gateway Endpoint Applications

### Field Name | Value
--- | ---
*display_name* | *Jssh2 Client*
*embedded_application_type* | *java_applet*
*file_name* | *ssh2.jar*
*post_custom_params* | *Empty*
*pre_custom_params* | *ssh2.Main*
*server_name_required_params* | *true*
*type* | *embedded_application*

**SSH2 Windows Executable**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>display_name</em></td>
<td><em>Essh2 Client</em></td>
</tr>
<tr>
<td><em>embedded_application_type</em></td>
<td><em>windows_executable</em></td>
</tr>
<tr>
<td><em>file_name</em></td>
<td><em>WinSsh2.exe</em></td>
</tr>
<tr>
<td><em>post_custom_params</em></td>
<td><em>Empty</em></td>
</tr>
<tr>
<td><em>pre_custom_params</em></td>
<td><em>Empty</em></td>
</tr>
<tr>
<td><em>server_name_required_params</em></td>
<td><em>true</em></td>
</tr>
<tr>
<td><em>type</em></td>
<td><em>embedded_application</em></td>
</tr>
</tbody>
</table>

When configuring either of the new downloaded-from-Mobile Access applications in SmartDashboard (*Jssh2 Client* and *Essh2 Client*), 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 69)
2. **Create a CAB Package from the Profile** (on page 70)
3. **Configure the Package Downloaded-from-Gateway Application** (on page 70)
4. **Configure the Link to the Remote Desktop Application** (on page 71)
5. **Configure the Remote Desktop Profile to Start Automatically** (on page 71)
6. **Assign the Native Application to the User Group** (on page 71)

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*.
Adding New Downloaded-from-Gateway Endpoint Applications

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.

1. 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:

- Configuring the Telnet Client (Certified Application) (on page 72)
- Configuring the SSH Client (Certified Application) (on page 72)
- Configuring the TN3270 Client (Certified Application) (on page 72)
- Configuring the TN5250 Client (Certified Application) (on page 73)
- Configuring the Remote Desktop Client (Add-On Application) (on page 73)
- Configuring the PuTTY Client (Add-On Application) (on page 74)
- Configuring the Jabber Client (Add-On Application) (on page 75)
- Configuring the FTP Client (Add-On Application) (on page 75)

7. Continue with Completing the Native Application Configuration (on page 62).

### Configuring the Telnet Client (Certified Application)

**Telnet Client Configuration**

<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)

**SSH Client Configuration**

<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)

**TN3270 Client Configuration**

<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>
</tbody>
</table>
## Configuring the TN5250 Client (Certified Application)

**TN5250 Client Configuration**

<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>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 <a href="http://tn5250j.sourceforge.net/quick.html">http://tn5250j.sourceforge.net/quick.html</a>.</td>
</tr>
<tr>
<td>Parameters usage</td>
<td><code>[Server [options]]</code></td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Configuring the Remote Desktop Client (Add-On Application)

**Remote Desktop Client Configuration**

<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>Must contain the server name or its IP address.</td>
</tr>
</tbody>
</table>
Parameters usage

```
[options] server[:port]
```

For example: `g 800x600 -l WARN RDP_Server. The following options are available:

- **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 the terminal server for different 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

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

### Putty Client Configuration

<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>`([-ssh</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)

**Jabber Client Configuration**

<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)

**FTP Client Configuration**

<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>
User Authentication in Mobile Access

In This Chapter

User Authentication to the Mobile Access Portal 76
Two-Factor Authentication with DynamicID 77
Session Settings 86

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. See the [R75 VPN Administration Guide](http://supportcontent.checkpoint.com/documentation_download?ID=11675) for more details on User Certificates.
- **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. See the [R75 Firewall Administration Guide](http://supportcontent.checkpoint.com/documentation_download?ID=11660) for details on configuring a Security Gateway to use a RADIUS server.
- **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. See the [R75 Firewall Administration Guide](http://supportcontent.checkpoint.com/documentation_download?ID=11660) for details on configuring a Security Gateway to use SecurID.

A user who tries to authenticate with an authentication scheme that is not configured for the Mobile Access gateway will not be allowed Mobile Access access 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.
  
  If you do not make a selection on the Mobile Access > Authentication page, the Security Gateway takes authentication settings for Mobile Access from the gateway Legacy Authentication page.

- 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 Users and Authentication > Authentication > Authentication to Gateway to see an overview of the Mobile Access gateways and their allowed 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.

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 SmartDirectory (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.

Advantages of a search based on the authentication scheme include:

- Faster results
- You can have users with the same username 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:

- One of the authentication methods that is enabled in the Gateway Properties > Legacy Authentication page of the gateway.
Two-Factor Authentication with DynamicID

- 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 the main Authentication page of the 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 the following:

**Figure 6-5** Mobile Access Login with SMS Secondary Authentication

![Mobile Access Login with SMS Secondary Authentication](image)

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 button appears. 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. For details, see Two-Factor Authentication Per Application (on page 84).

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. See Two Factor Authentication per Gateway ("Two-Factor Authentication per Gateway" on page 84).

**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**

Obtain your SMS service provider settings from your SMS provider. The following are required:

- 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)

*Note* - If DynamicID is configured to work with email only, an SMS Service Provider is not necessary.

**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 the following syntax:

   `<user name | Full DN> <phone number | email address>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>user name or Full DN</td>
<td>Either a user name or, for users that log in using a certificate, the full DN of the certificate.</td>
</tr>
<tr>
<td>phone number</td>
<td>All printable characters can be used in the phone number, excluding the space character, which is not allowed. Only the digits are relevant.</td>
</tr>
<tr>
<td>email address</td>
<td>A valid email address in the format <a href="mailto:user@domain.com">user@domain.com</a></td>
</tr>
</tbody>
</table>

**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**

To configure the option for users to choose from multiple phone numbers when resenting the verification code, do one of these:
- 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**

To configure DynamicID settings in SmartDashboard:
2. In the Authentication Schemes page, select Challenge users to provide an OTP received at their mobile device via SMS.
   This makes two-factor authentication a requirement for logging in to all Mobile Access gateways with authentication settings (configured in the Additional Settings > Authentication page of the Mobile Access gateways) of Use the global settings, configured in the Mobile Access tab, under “Authentication to Mobile Access”).
3. Fill in the SMS Provider and Email Settings field using one of the following formats:
   a) To allow the DynamicID code to be delivered by SMS only, use the following syntax:

   ```
   https://api.example.com/http/sendmsg?api_id=$APIID&use=r=
   $USERNAME&password=$PASSWORD&to=$PHONE&text=$MESSAGE
   ```
b) To allow the DynamicID code to be delivered by email only, without an SMS service provider, use the following syntax:

```
mail:TO=$EMAIL;SMTPSERVER=smtp.checkpoint.com;FROM=ssl
vpn@example.com;BODY=$RAWMESSAGE
```

c) To allow the DynamicID code to be delivered by SMS or email, use the following syntax:

```
sms:https://api.example.com/sendsms.php?username=$USER
NAME&password=$PASSWORD&phone=$PHONE&smstext=$MESSAGE
mail:TO=$EMAIL;SMTPSERVER=smtp.checkpoint.com;FROM=ssl
vpn@example.com;BODY=$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>$EMAIL</td>
<td>The email address of the user as found in Active Directory or in the local file on the gateway. If the email address should be different than the listed one, it can be written explicitly.</td>
</tr>
<tr>
<td>$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.
   See Advanced Two-Factor Authentication Configuration Options for more information.
6. Install the policy. Select Policy > Install.

**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:
  Users who choose skip are allowed to log in, but are denied access to applications that require two-factor authentication.
  
  Please type the verification code sent to your phone:

  ![Image showing a screen with options to submit, skip, or cancel]

- **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.

  **Template Fields for the DynamicID One Time Password Message**

<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\R75\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.

<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><code>true</code>: match word provided&lt;br&gt;<code>false</code>: match word not provided (default)</td>
</tr>
<tr>
<td>Resend message</td>
<td>Enable_end_user_re_transmit_message</td>
<td><code>true</code>: enable resend SMS feature (default)&lt;br&gt;<code>false</code>: disable resend SMS feature</td>
</tr>
<tr>
<td>Display multiple phone numbers</td>
<td>enable_end_user_select_phone_num</td>
<td><code>true</code>: enable option to choose from multiple phone numbers or email addresses when resending the verification code (default)&lt;br&gt;<code>false</code>: one phone number or email address from the LDAP server or local file is used automatically without choice</td>
</tr>
<tr>
<td>Conceal displayed phone numbers</td>
<td>Edit both:&lt;br&gt;reveal_partial_phone_num&lt;br&gt;number_of_digits_revealed</td>
<td><code>true</code>: conceal part of the phone number or email address (default)&lt;br&gt;<code>false</code>: 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>
</tbody>
</table>

After editing the values in GuiDBedit, save the changes, connect to SmartDashboard, and install the policy.
Two-Factor Authentication with DynamicID

**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:

```
cvpnd_settings 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.

To configure two-factor authentication **Globally on, with custom settings per gateway**:

1. Set up basic two-factor authentication.
2. Turn on two-factor authentication in the **Users and Authentication > Authentication to Gateway** page.
3. For each gateway, go to Gateway Properties > Mobile Access Authentication.
4. Do one of the 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.
5. Repeat step 3 to step 4 for all other gateways.
6. 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. Set up basic two-factor authentication. See Basic Two-Factor Authentication Configuration.
2. Configure the Protection Level. See Defining Protection Levels. In the **Authentication** page, 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 19).

**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, once configured in SmartDashboard, DynamicID is enforced for all authentication types. Therefore the default enforceSMSforAuthTypes parameter in the cvpnd.C configuration file is:

```plaintext
:enforceSMSforAuthTypes (  
  : (USER_PASS)  
  : (CERT)  
  : (RADIUS)  
  : (SECURID)  
)
```

To enforce DynamicID only for certain authentication types, remove the authentication types after which DynamicID enforcement is not required. For example, to require DynamicID when a user authenticates using a certificate or user name and password, but not using SECURID or RADIUS authentication, edit the lines:

```plaintext
:enforceSMSforAuthTypes (  
  : (USER_PASS)  
  : (CERT)  
)
```

**DynamicID Authentication for Certain Methods and by Protection Level**

If, in SmartDashboard, you have configured a Protection Level to require two-factor authentication using DynamicID, the settings configured in the cvpnd.C configuration file will override the Protection Level Authentication settings in SmartDashboard.

For example: You have configured the Restrictive Protection Level to require DynamicID for users authenticating with Certificate authentication, but you have removed CERT from the enforceSMSforAuthTypes parameter. In this case, DynamicID authentication will not be required for anyone using Certificate authentication, even when accessing an application assigned to the Restrictive Protection Level.
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. By default, user requests are denied if sent from a different IP address than that used for login.

Note - Users connected via SSL Network Extender can always change IP address while connected, irrespective 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 that is logged in to the Mobile Access portal can open a new browser window and receive the access of the earlier session and browse directly to the Mobile Access portal without re-entering the login credentials.

Note - To ensure their authentication credentials are not stolen by others, you should recommend to users that they log off or close all browser windows after they have finished using the 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 in 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.

Note - Simultaneous login prevention is available for Connectra NGX R66 and higher and Mobile Access.

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

  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

  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 7

Endpoint Security On Demand

In This Chapter

- Endpoint Compliance Enforcement
- Configuring Endpoint Compliance
- Endpoint Compliance Scanner End-User Workflow
- Completing the Endpoint Compliance Configuration
- Secure Workspace
- Endpoint Compliance Updates

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 Licensing**

To use Endpoint Compliance, a valid Endpoint Security On Demand license is required for the Mobile Access gateway. At least as many Endpoint Security On Demand users as Mobile Access users must be installed.

**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.

Customizable protection is available for a wide variety of spyware threats, as shown in the following table:

<table>
<thead>
<tr>
<th>Spyware Types</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</td>
<td>Commercially developed software that allows remote system access and control.</td>
</tr>
<tr>
<td>Spyware Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</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>
<tr>
<td>Screen Logger</td>
<td>Software that record what a user's monitor displays.</td>
</tr>
<tr>
<td>Tracking Cookie</td>
<td>Cookies that are used to deliver information about the user's Internet activity to marketers.</td>
</tr>
<tr>
<td>Browser Plug-in</td>
<td>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.</td>
</tr>
</tbody>
</table>

It is possible to define an exception list of spyware software. For example, you can specify that a specific spyware signature is not blocked (see Excluding a Spyware Signature from a Scan (on page 99)).

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.

### 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 98).)
   - **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 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:
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>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>

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.
   - 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. See Endpoint Compliance Policy Rule Types (on page 90).
   - To add a previously defined rule, click Add. The Add Enforcement Rules page opens. Select a rule and click OK.
   - To create a rule, click New Rule, and select the rule type
   - To edit a previously defined rule, select the rule and click Edit.
7. Define the rules.
   
   Note - For explanations of the meanings of particular fields in the Endpoint Compliance rule configuration windows, 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:**

1. On the **Mobile Access** tab of SmartDashboard, select **Endpoint Security On Demand > Endpoint Compliance** from the navigation tree. The **Endpoint Compliance** page appears.

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 96)
   - **Advanced Approach**: Configuring a Threshold Policy for the Portal, Hardened for Specific Applications (on page 96)
   - **Very Advanced Approach**: Configuring Individual Policies for Each Application (on page 97)

**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 98).

**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… For details, see Defining Protection Levels.

7. Click OK.
8. Continue with Configuring Endpoint Compliance Logs (on page 98).

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.
   To define a new Protection Level, click Manage…. For details, see Defining Protection Levels.

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.

6. Repeat steps step 3 to step 5 for all Mobile Access applications that require hardened endpoint security.
7. Click OK.

Configuring Advanced Endpoint Compliance Settings by Operating System

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 allows you to configure “Platform-Based Bypass” per application.
Enabling Platform Based Bypass per Protection Level

To configure different access permissions for various Protection Levels for Endpoint Compliance scanning, run:

```bash
cvpnd_settings 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, under Additional Settings > Protection Level, you can 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 name `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:

```bash
cvpnd_settings listAdd ICSRelaxedModeProtectionLevelNames ESOD_Relaxed_PL
```

You can add other Protection Levels as well.

To restore a Protection Level from being Bypassed

To restore a Protection Level from being "Bypassed", for Endpoint Compliance:

1. Run:
   ```bash
cvpnd_settings listRemove ICSRelaxedModeProtectionLevelNames
```
2. Follow the on-screen instructions.

Finalize the Configuration

To finalize the configuration of granular platform-based bypass for Endpoint Security On Demand:

1. Restart the Mobile Access services by running cvpnrestart.
   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 92).

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.
2. 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 as follows:

- **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.
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 takes place if Endpoint compliance is configured for any Mobile Access application in a portal, even if accessing the portal itself does not require compliance with any policy.
```

The Endpoint Compliance Scanner 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 12).

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 scan results are presented to the user and the administrator as log entries in the Traffic Log. Each log entry lists the user name, his/her user group, the 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:
Completing the Endpoint Compliance Configuration

1. 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 figure below shows:
   - One Mobile Access gateway that is configured to scan endpoint machines, with a high security policy required on the gateway.
   - Six Mobile Access applications, two of which have a Partial Level of Enforcement (require High security Endpoint Compliance policy on the gateway). Two of the applications have a Full Level of Enforcement (also require compliance with a High security endpoint compliance policy when accessing the application).

2. 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 files, cookies, registry changes, browser credentials, and so on. It deletes this folder and all other session data when the session terminates.

Secure Workspace severely restricts user’s ability to write to "real" workspace folders. However, in order to allow certain applications to run properly, Secure Workspace policy may be configured to permit write access to specific files and folders in the "real" workspace.

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 an Mobile Access gateway:**

1. On the SmartDashboard **Mobile Access** tab, select **Endpoint Security On Demand > Secure Workspace**.
2. To configure the Secure Workspace policy, click **Edit policy**. For details, see Configuring the Secure Workspace Policy (on page 108).
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 the **Endpoint Security On Demand > Secure Workspace** page, in the **Advanced Secure Workspace Settings** section, click **Edit**. The **Advanced Secure Workspace Settings** window opens.

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 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 protections 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 listAdd ISWRelaxedModeProtectionLevelNames ESOD_Relaxed_PL
```

You can add other Protection Levels as well.

**Restoring a Protection Level from being Bypassed**

To restore a Protection Level from being "Bypassed", for Secure Workspace:

1. Run:

```
cvpnd_settings listRemove ISWRelaxedModeProtectionLevelNames
```

2. Follow the on-screen instructions.

**Finalize the Configuration**

To finalize the configuration of granular platform-based bypass for Secure Workspace:

1. Restart the Mobile Access services by running `cvpnrestart`.
   - 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.
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 proper application crash handling.</td>
</tr>
<tr>
<td>igfxssvc.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>ieinstål.exe</td>
<td>Internet Explorer</td>
<td>Microsoft Internet Explorer web browser</td>
</tr>
<tr>
<td>conime.exe</td>
<td>Microsoft Console IME</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>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. This program is important for the stable and secure running of the computer 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>Application Name</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>-------</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 Windows update. This process handles Windows Ink Services and often runs 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. This program is important for the stable and secure running of endpoint 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 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 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 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 Windows OS. It manages 32-bit DLLs and other services and cannot be stopped or restarted manually.</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>Process Name</td>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</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 SNX 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>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.
For some applications, you may also need to 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 the Endpoint Security Administrator Guide ([http://supportcontent.checkpoint.com/documentation_download?ID=8065](http://supportcontent.checkpoint.com/documentation_download?ID=8065)). 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:**

1. On the SmartDashboard Mobile Access tab, select **Endpoint Security On Demand > Secure Workspace**.
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**

- **Prevent endpoint from printing 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

- **Prevent endpoint from switching between Secure Workspace and 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. The ICSInfo tool (see Using the ICSInfo Tool (on page 94)) can be used to calculate the hash function of an application. Alternatively, MD5 calculators are freely available on the Internet.

  **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 Allowed Save Locations

- **Allowed Save locations** are locations where the application is 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. Save locations for the default approved applications are predefined.

  A good way of finding out the required save locations is to note the locations specified when installing an application. If after defining an application you are unable to use it, examine Secure Workspace log, which records attempts to save files or access locations that are not allowed.

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. At a minimum, define a rule that allows loopback traffic to 127.0.0.1. Also, take into account all ports required by the allowed protocols.
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).

Testing the Secure Workspace Policy


Secure Workspace End-User Experience

This section provides an overview of the Secure Workspace workflow.

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 12).
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, 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.

**Running Secured Programs**

Secured programs (those with *execute* privileges) run normally. Administrators can configure the Secure Workspace policy to include such programs in the **Secured Programs** entry on the **Start** menu. Secured programs display the Secure Workspace icon in the upper right-hand corner of the application window title bar.

**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 <strong>Start &gt; Program</strong> 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) 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.

**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 8

Advanced Password Management Settings

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.

In This Chapter

Password Expiration Warning 113
Managing Expired Passwords 113

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 continue to have Mobile Access access. 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 > SmartDirectory (LDAP).
2. Under SmartDirectory (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

See the R75 Security Management Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11667) for more information on LDAP and user management.
Chapter 9

Mobile Access Blade Configuration and Settings

In This Chapter

Interoperability with Other Blades  115
Portal Settings  117
Server Certificates  120
Web Data Compression  122
Using Mobile Access Clusters  123

Interoperability with Other Blades

The Mobile Access blade is fully integrated with the other software blades in the SmartConsole. Any R71 or higher Security Gateway running on SecurePlatform with the Firewall blade enabled can also have the Mobile Access blade enabled.

See the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647) for detailed information on supported platforms.

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-FLI/lib/libModWI.so
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 116).
2. From the CLI, run:
   ```
cvpnd_settings 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:
   ```
cvpnd_settings 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

Certain Anti-virus settings configured for a Security Gateway in the Security Gateway > HTTP page of the Anti-virus tab also apply to Mobile Access traffic. In order to activate Anti-virus protection, enable the Anti-virus and Malware blade on the Security Gateway.

The following settings apply to Mobile Access traffic:
- **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.

Mobile Access Anti-virus protections always work in **proactive mode** regardless of which option you select.

**Note** - Once SSL Network Extender traffic is rerouted to the Security Gateway, Anti-virus inspects the traffic as it does to any other unencrypted traffic.

### 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 by entering https://<Gateway_IP>/sslvpn, where `<Gateway_IP>` is:
- Either the FQDN that resolves to the IP address of the Security Gateway
- The IP address of the Security Gateway

If remote users enter http://<Gateway_IP>/sslvpn, they will automatically be redirected to the portal using HTTPS.
Note - If you use Hostname Translation as your method for link translation, you must enter an FQDN as the portal URL and not an IP address.

You 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 maximum logo width is 300 pixels. Larger images are resized.

Note - If the custom logo is changed, end users must refresh their browser cache in order 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 the following languages:

- English (the default language)
- Bulgarian
- Chinese- Simplified
- Chinese- Traditional
- Finnish
- French
- German
- Italian
- Japanese
- Polish
- Romanian
- Russian
- Spanish

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 a 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.

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 that is signed by a known certificate authority (CA) for a gateway.

Generating the Certificate Signing Request

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

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

1. From the gateway command line, log in to expert mode.
2. Run:
   ```bash
copenssl req -new -out <CSR file> -keyout <private key file> -config $CFDIR/conf/openssl.cnf
   ```

   This command generates a private key. You see this output:
Generating a 2048 bit RSA private key
...+++
writing new private key to 'server1.key'
Enter PEM pass phrase:

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

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

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

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

### Generating the P12 File

After you get the Signed Certificate for the gateway from the certificate Authority, generate a P12 file that contains the Signed Certificate and the private key.

1. Get the **Signed Certificate** for the gateway from the certiﬁcate authority.
   - If the signed certificate is in P12 or P7B format, convert these files to PEM (Base-64) format.
2. Make sure that the `.crt` file contains the full certificate chain up to a trusted CA. Usually you get the certificate chain from the signing CA. Sometimes it is in a separate file.
   - If the signed certificate and the trust chain are in separate files, use a text editor to combine them into one 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 in Generating the Certificate Signing Request (on page 120).
   a) Run:

```
copenssl pkcs12 -export -out <output file> -in <signed cert chain file> -inkey <private key file>
```
   - For example:

```
copenssl pkcs12 -export -out server1.p12 -in server1.crt -inkey server1.key
```
   b) Enter the certificate password when prompted.

### Installing the Signed Certificate

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

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

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 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 the View button 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:

Note - In a cluster, perform the following steps on the cluster object.

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.

For more information on using clusters, see the ClusterXL Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10641).

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.

<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. 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>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 “Go to the login page” 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>Application</td>
<td>Survives failover?</td>
<td>User experience upon failover</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------</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</td>
<td>Mode dependant</td>
<td>Network Mode — Survives failover. Application Mode — Does not survive failover.</td>
</tr>
<tr>
<td>Access applications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10

Troubleshooting Mobile Access

In This Chapter

Troubleshooting Web Connectivity 125
Troubleshooting Outlook Web Access 125
Common OWA problems 126
Troubleshooting File Shares 131
Troubleshooting Citrix 131

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 20).
2. Check the Mobile Access Release Notes for additional information.
3. Go over the Troubleshooting OWA Checklist (on page 125).
4. Look for a description that matches your issues in Common OWA Problems (on page 126).

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. See Unsupported Feature List (on page 126)
Common OWA problems

- Client-side browsers are supported by OWA and by Mobile Access. See Unsupported Feature List (on page 126).
- 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.
- 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

The following sections describe issues that may arise when browsing to OWA through Mobile Access.

Note - Check your traffic logs for errors. The logs may help you 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 127) versus the setup in Microsoft Exchange server.
- **Alternative References to OWA** (on page 128).

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:

- **Exchange System Manager**

  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

  ![Exchange System Manager](image)

  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.

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 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:

- Mobile Access Logging Issue (see "Mobile Access Logging Issues" on page 129)
- OWA over SSL or OWA with Form Based Authentication Enabled (on page 129)
- Slow Network Problems (on page 129)
- Latency Overhead Problems (on page 129)
- Authorization Problems
- SSL Time-out Problems (on page 130)
**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 `$CVPNDIR/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 `$CVPNDIR/log` directory
2. Empty or delete the `mod_ws.log` file located in `$CVPNDIR/log` directory
3. Empty or delete the `mod_ws_boa.log` file located in `$CVPNDIR/log` directory
4. Delete all files located under `$CVPNDIR/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, do one of the following:**

1. If feasible, upgrade Internet Explorer by following the instructions in the relevant Microsoft articles below.
2. Alternatively, configure Mobile Access so that it does not use keep-alive packets when communicating with those hosts or paths.

**See the following Microsoft articles for more information:**

- [http://support.microsoft.com/kb/183110/](http://support.microsoft.com/kb/183110/)
- [http://support.microsoft.com/kbid=831167](http://support.microsoft.com/kbid=831167)
- [http://support.microsoft.com/?scid=kb;EN-US;Q305217](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](http://httpd.apache.org/docs/2.0/mod/core.html#locationmatch)

   ```
   <LocationMatch "CVPHost=IP or DNS namedelimited by dots"> 
   SetEnv nokeepalive
   </LocationMatch>
   ```

   For example:

   ```
   <LocationMatch "CVPHost=208.77.188.166"> 
   SetEnv nokeepalive
   </LocationMatch>
   ```

   .........

   ```
   <LocationMatch "CVPHost=myhost\example\.com|CVPHost=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:

```text
Bulletin1H.PDF,CVPNHost=192.168.201.6,CVPNProtocol=http,CVPNOrg=full ,CVPNExtension=.PDF
```

To solve this, configure the Web Application to use Hostname Translation. Refer to Configuring Link Translation (on page 29).
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 websites. 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 any problems with Citrix following the deployment of Mobile Access, take the following steps:

1. Read the relevant section on Citrix Services.

Troubleshooting Citrix Checklist

Follow the steps below to pinpoint the issue that may be causing trouble with Citrix.

Connectivity Issues - Make sure that:

1. 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. 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. 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. Mobile Access users have a network route to the Mobile Access machine.

Configuration Issues - Make sure that:

1. Citrix servers and clients are of those versions supported by Mobile Access.
2. All necessary STA servers are configured with corresponding Citrix Services on Mobile Access.
3. Mobile Access's server certificate is issued to Mobile Access's Fully Qualified Domain Name (such as www.example.com), is properly configured, and is trusted by the client-side.
Index

A
About Hostname Translation • 28
Accessing Applications • 13
Accessing Endpoint Applications in Secure Workspace • 111
Accessing Files and Applications on the Endpoint Computer • 110
Add Application • 109
Adding a Trusted Certificate Authority for Website Certification • 33
Adding New Downloaded-from-Gateway Endpoint Applications • 67
Add-on Applications • 60
Advanced Approach
Configuring a Threshold Policy for the Portal, Hardened for Specific Applications • 96
Advanced Configuration of SSO • 48
Advanced Configuration of Web Form SSO • 50
Advanced Password Management Settings • 113
Advanced Two-Factor Authentication Configuration • 81
Allowing Users to Save Files to the • 110
Alternative Portal Configuration • 120
Alternative References to OWA • 128
Anti-spyware Application Rule • 90
Anti-virus and Anti-malware Blade • 116
Anti-virus Application Rule • 90
Application and Client Support for SSO • 46
Application Installed on Endpoint Machine • 59
Application Requirements for Easy Configuration • 46
Application Runs Via a Default Browser • 59
Applications Downloaded-from-Gateway • 59
Applications for Clientless Access • 19
Applications on the Endpoint Machine • 61
Applications Permitted by Secure Workspace • 105
Assign Policies to Gateways and Applications • 99
Assign the Native Application to the User Group • 71
Authentication • 10
Authorization • 10
Authorization Example Scenario • 127
Authorized Locations • 61
Automatically Running Commands or Scripts • 64
Automatically Starting the Application • 63

B
Basic Approach
Configuring a Common Policy for the Portal and all Applications • 96
Basic Configuration of Web Form SSO • 48
Basic DynamicID Configuration for SMS or Email • 79
Basic SmartDashboard Configuration • 15
Basic SmartDashboard Configuration of DynamicID • 80
Basic SSO Configuration • 47
Before Configuring Citrix Services • 37

C
Certified Applications • 59
Changing the SMS Provider Certificates and Protocol • 85
Changing to an IPS Profile Configuration for Mobile Access • 116
Citrix Deployments Modes - Unticketed and Ticketed • 37
Citrix Service — Link in Portal Page • 38
Citrix Service — Presentation Servers Page • 38
Citrix Service — Protection Level Page • 39
Citrix Service — Single Sign On Page • 39
Citrix Service — STA Servers Page • 38
Citrix Service — Web Interface page • 38
Citrix Services • 37
Client Side Security Highlights • 11
Cluster Deployment • 14
Common OWA problems • 126
Commonly Used Concepts • 9
Completing the Configuration of the Citrix Service • 39
Completing the Configuration of the File Share Application • 36
Completing the Configuration of the Web Application • 26
Completing the Configuration of the Web Mail Service • 41
Completing the Endpoint Compliance Configuration • 102
Completing the Native Application Configuration • 62
Configure the Link to the Remote Desktop Application • 71
Configure the Package Downloaded-from-Gateway Application • 70
Configure the Remote Desktop Profile to Start Automatically • 71
Configuring a Proxy per Web Application • 27
Configuring a Secure Workspace Policy per Gateway • 110
Configuring a Simple Native Application • 61
Configuring Advanced Endpoint Compliance Settings by Operating System • 97
Configuring Advanced Secure Workspace Settings • 103
Configuring Advanced Single Sign On • 48
Configuring Allowed Save Locations • 109
Configuring an Advanced Native Application • 62
Configuring Approved Applications • 109
Configuring Authentication • 77
Configuring Authorized Locations per User Group • 60
Configuring Citrix Services • 37
Configuring Connection Direction • 62
Configuring Data Compression • 122
Configuring DNS Name Objects • 42
Configuring Downloaded-from-Gateway Endpoint Applications • 71