QUANTUM

17 April 2024

# MOBILE ACCESS

## R80.40

Administration Guide

# Check Point Copyright Notice

© 2020 - 2024 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

# Important Information

### Latest Software

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

### Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

### Check Point R80.40

For more about this release, see the R80.40 home page.

### Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

### Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

### Revision History

| Date | Description |
|---|---|
| 03 December 2023 | Moved documentation of SSL Network Extender (SNX) to the new SSL Network Extender (SNX) Administration Guide. |
| 09 January 2023 | Updated:<br>■ *"User Authentication in Mobile Access" on page 146* |
| 13 November 2022 | Updated:<br>■ *"Getting Started with Mobile Access" on page 32* - aded the link to sk168353 |
| 03 October 2022 | Updated:<br>■ *"User Authentication in Mobile Access" on page 146* |
| 15 June 2022 | In the HTML version, added glossary terms to the text |
| 09 December 2021 | Updated *"User Authentication in Mobile Access" on page 146* |
| 26 January 2020 | First release of this document |

# Table of Contents

# Introduction to Mobile Access

## Mobile Access

Check Point Mobile Remote Access VPN Software Blade is the safe and easy solution to connect to corporate applications over the internet with your mobile device or PC. The solution provides enterprise-grade remote access with both Layer 3 VPN and SSL VPN. It gives you simple, safe and secure connectivity to your email, calendar, contacts and corporate applications. At the same time, it protects networks and endpoint computers from threats.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet.

Check Point Mobile Apps enables secure encrypted communication from unmanaged smartphones and tablets to your corporate resources.

## 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 is a set of URLs that are used in the same context and that are accessed through a Web browser. For example, an application for inventory management, or HR management.
- A file share is a collection of files, made available across the network through a protocol 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 device support:

    - Access to Web applications.
    - Access to email, calendar, and contacts.
    - Multi-factor authentication.
- Mobile Access supports IPv6 for access to:
    - The Mobile Access Portal.
    - Capsule Workspace.

  Notes:
    - SSL Network Extender is not supported with IPv6.
    - IPv6 is supported for inbound connections to the Security Gateway only. It is not supported for outbound connections from the Security Gateway, even with an external interface.
- SSL Network Extender support for macOS as part of Capsule Workspace Access.
- Mobile Access supports all native applications, through SSL Network Extender. A native application is an 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 Security Gateway. The Security Gateway authenticates users based on one or more of the configured authentication methods, such as user name and password, certificates, or SecurID. Users have access to applications based on the Mobile Access policy.

For information about Web applications, file shares, Citrix services, Web mail see *"Mobile Access Applications" on page 55*.

For information about native applications, see the SSL Network Extender (SNX) Administration Guide.

# Mobile Access Management

- The Security Management Server that manages all Check Point Security Gateways, also manages Mobile Access Security Gateways.
- Configure Mobile Access from the Mobile Access tab of SmartDashboard and in the Access Control Rule Base.
- Mobile Access users and related network objects are shown in SmartConsole.
- See Mobile Access logs in SmartLog from the SmartConsole **Logs & Monitor** view.

- Mobile Access supports SNMP. See the *R80.40 Gaia Administration Guide* > Chapter *System Management* > Section *SNMP*.

# Commonly Used Concepts

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

## Authentication

All remote users that access the Mobile Access Portal must be authenticated by one or more of the supported authentication methods. Multiple login options for users and multi-factor authentication are supported. See *"User Authentication in Mobile Access" on page 146*.

## Authorization

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

After authentication, the user can open an application based on the Mobile Access policy.

## Endpoint Compliance Scanner

The Check Point Endpoint Security on Demand scanner scans the endpoint machine to see if it complies with the endpoint compliance policy. For example, an endpoint compliance policy can make sure that the endpoint clients have updated Anti-Virus signatures and an active Firewall. If the endpoint is compliant with the endpoint compliance policy, the user is allowed to access the portal.

## 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. Afterward, it cleans the protected session cache, eliminating any exposure of proprietary data that would have been inadvertently left on public PCs.

## Protection Levels

Protection Levels maintain a balance between connectivity and security. The Protection Level is a security requirement that users must meet before they can access the resource. For example, an application can have a Protection Level that requires users to use a specified authentication method. Mobile Access has three pre-defined Protection Levels: Permissive, Normal, and Restrictive. You can edit Protection Level settings, and define new Protection Levels.

## Session

After authentication, remote users are assigned a Mobile Access *session*. The session is the period of communication with the Security Gateway until the user logs out or the connection times out.

## SSL Network Extender

The SSL Network Extender client makes it possible to access native applications through 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 transports application traffic through a secure, encrypted, and authenticated SSL tunnel to the Mobile Access Security Gateway.

For more information, see the SSL Network Extender (SNX) Administration Guide.

# Server Side Security Highlights

Mobile Access 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. These are some of the security features available on Mobile Access Gateways:

- **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.

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

- **Anti-Virus** - Many Anti-Virus settings enabled on the Security Gateway also apply to Mobile Access traffic to prevent virus infection for end users and the enterprise.

- **Granular authorization policy** - Limits which users are granted access to which applications based on: authentication, encryption, and client security requirements.

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

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

# Client Side Security Highlights

These are some of the security features available on the client side:

- **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 *"Endpoint Security on Demand" on page 186*.
- **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. It encrypts all files and deletes data from the computer at the end of the user session. The administrator can use Protection Levels to force end users to use Secure Workspace to access the user portal or sensitive *"Endpoint Security on Demand" on page 186*.
- **Controls browser caching** - You can disable browser caching or decide which web content can be cached by browsers when users access *"Mobile Access Applications" on page 55*.
- **Captures cookies sent to the remote client by the internal Web server** - In most configurations, Mobile Access captures cookies and keeps them on the Security Gateway. Mobile Access attaches the cookie information, stored on Mobile Access, to the request that Mobile Access makes to the internal Web server to simulate user or web server cookie transmission.
- **Supports multi-factor authentication methods and multiple log-in options** - For example, use SecurID tokens, or SSL client certificates in combination with a one-time DynamicID password.

# Check Point Remote Access Solutions

## Secure Remote Access

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

## Types of Solutions

All of Check Point's Remote Access solutions provide:

- Enterprise-grade, secure connectivity to corporate resources.
- Strong user authentication.
- Granular access control.

**Factors to consider when choosing remote access solutions for your organization:**

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

## Client-Based vs. Clientless

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

- **Client-based** - Client application installed on endpoint computers and devices. The client supplies access to most types of corporate resources according to the access privileges of the user.
- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.
- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

## Secure Connectivity and Endpoint Security

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

- **Secure Connectivity** - Traffic is encrypted between the client and VPN Security Gateway and strong user authentication is supported. All Check Point solutions supply this.

  These solutions require licenses based on the number of users connected at the same time.
- **Security Verification for Endpoint computers** - Makes sure that devices connecting to the Security Gateway meet security requirements. Endpoint machines that are not compliant with the security policy have limited or no connectivity to corporate resources. Some Check Point solutions supply this.
- **Endpoint Security**:
  - **Desktop Firewall** - Protects endpoint computers at all times with a centrally managed security policy. This is important because remote clients are not in the protected network and traffic to clients is only inspected if you have a Desktop Firewall. Some Check Point solutions supply this
  - **More Endpoint Security Capabilities** - Check Point solutions can include more Endpoint Security capabilities, such as Anti-Malware, disk encryption and more.

  These solutions require licenses based on the number of clients installed.

# Remote Access Solution Comparison

Details of the newest version for each client and a link for more information are in sk67820.

| SSL VPN Portal and Clients | Supported Operating Systems | Client or Clientless | Encryption Protocol | Security Verification for Endpoint Devices | Desktop Firewall on Endpoint Devices | IPv6 Support |
|---|---|---|---|---|---|---|
| Capsule Workspace for iOS (previously Mobile Enterprise) | iOS | Client | SSL |  Jailbreak & Root Detection MDM Cooperative Enforcement (sk98201) | |  |
| Capsule Workspace for Android (previously Mobile Enterprise) | Android | Client | SSL |  Jailbreak & Root Detection MDM Cooperative Enforcement (sk98201) | |  |

| Layer 3 VPN Tunnel Clients | Supported Operating Systems | Client or Clientless | Encryption Protocol | Security Verification for Endpoint Devices | Desktop Firewall on Endpoint Devices | IPv6 Support |
|---|---|---|---|---|---|---|
| Capsule Connect for iOS (previously Mobile VPN) | iOS | Client | IPsec / SSL | MDM Cooperative Enforcement (sk98201) | | |
| Capsule VPN for Android (previously Mobile VPN) | Android | Client | IPsec/SSL | MDM Cooperative Enforcement (sk98201) | | |

| Layer 3 VPN Tunnel Clients | Supported Operating Systems | Client or Clientless | Encryption Protocol | Security Verification for Endpoint Devices | Desktop Firewall on Endpoint Devices | IPv6 Support |
|---|---|---|---|---|---|---|
| Check Point VPN Plugin for Windows 8.1 | Windows 8.1 | Pre-installed client | SSL | | | |
| Check Point Capsule VPN for Windows 10 | Windows 10 | Client | SSL | | | |
| Check Point Mobile for Windows | Windows | Client | IPsec | ✓ | | |

| Layer 3 VPN Tunnel Clients Integrated with Endpoint Security | Supported Operating Systems | Client or Clientless | Encryption Protocol | Security Verification for Endpoint Devices | Desktop Firewall on Endpoint Devices | IPv6 Support |
|---|---|---|---|---|---|---|
| Endpoint Security VPN for Windows | Windows | Client | IPsec | ✓ | ✓ | |
| Endpoint Security VPN for Mac | macOS | Client | IPsec | | ✓ | |

| Layer 3 VPN Tunnel Clients Integrated with Endpoint Security | Supported Operating Systems | Client or Clientless | Encryption Protocol | Security Verification for Endpoint Devices | Desktop Firewall on Endpoint Devices | IPv6 Support |
|---|---|---|---|---|---|---|
| Endpoint Security Suite Remote Access VPN Blade | Windows, macOS | Client | IPsec | ✓ | ✓ | |

| Additional Remote Access Solutions | Supported Operating Systems | Client or Clientless | Encryption Protocol | Security Verification for Endpoint Devices | Desktop Firewall on Endpoint Devices | IPv6 Support |
|---|---|---|---|---|---|---|
| SecuRemote | Windows | Client | IPsec | | | |

# Summary of Remote Access Options

Below is a summary of each Remote Access option that Check Point offers. All supply secure remote access to corporate resources, but each has different features and meets different organizational requirements.

Details of the newest version for each client and a link for more information are in sk67820.

**Capsule Connect for iOS**

Capsule Connect is a full Layer 3 tunnel app that gives users network access to all mobile applications. It supplies secure connectivity and access to all types of corporate resources. It was previously called Mobile VPN.

**Required Licenses** - Mobile Access Software Blade on the Security Gateway and a mail license on the Security Management Server

**Supported Platforms** - iOS 6.0 +

**Where to Get the Client** - Apple App Store

### Capsule VPN for Android

Capsule VPN for Android devices is an Layer 3 VPN client. It supplies secure connectivity and access to corporate resources using Layer 3 IPSec/SSL VPN Tunnel. It was previously called Mobile VPN.

**Required Licenses** - Mobile Access Software Blade on the Security Gateway

**Supported Platforms** - Android 4 + (ICS+)

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

### Check Point VPN Plugin for Windows 8.1

Check Point VPN Plugin for Windows 8.1 is an Layer 3 VPN client. It supplies secure connectivity and access to corporate resources using Layer 3 SSL VPN Tunnel.

**Required Licenses** - Mobile Access Software Blade on the Security Gateway

**Supported Platforms** - Windows 8.1

**Where to Get the Client** - Pre-installed with Windows.

### Check PointCapsule VPN for Windows 10

Check Point Capsule VPN for Windows 10 is an Layer 3 VPN client. It supplies secure connectivity and access to corporate resources using Layer 3 SSL VPN Tunnel.

**Required Licenses** - Mobile Access Software Blade on the Security Gateway

**Supported Platforms** - Windows 10

**Where to Get the Client** - Microsoft Software & Apps store.

### Check Point Mobile for Windows

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

The client gives computers:

- Secure Connectivity
- Security Verification

**Required Licenses** - IPsec VPN and Mobile Access Software Blades on the Security Gateway.

**Supported Platforms** - Windows

**Where to Get the Client** - Check Point Support Center - sk67820.

### Endpoint Security VPN

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

The client gives computers:

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

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

**Supported Platforms** - Windows

**Where to Get the Client** - Check Point Support Center - sk67820.

**Note** - Endpoint Security VPN on macOS includes a Desktop Firewall, but not Security Verification.

### Endpoint Security VPN for macOS

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

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

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

**Supported Platforms for Users** - macOS

**Where to Get the Client** - Check Point Support Center - sk67820.

### Endpoint Security Suite

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

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

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

**Supported Platforms** - Windows, macOS

**Where to Get the Client** - Check Point Support Center - sk67820.

### SecuRemote

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

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

**Supported Platforms** - Windows

**Where to Get the Client** - Check Point Support Center - sk67820.

# Getting Started with Mobile Access

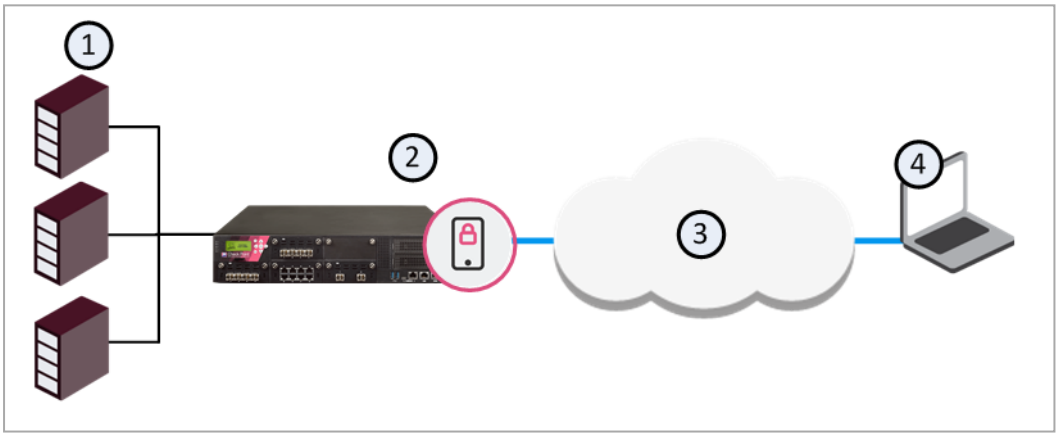
## Recommended Deployments

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 Security Gateway machine for easy and secure remote access.



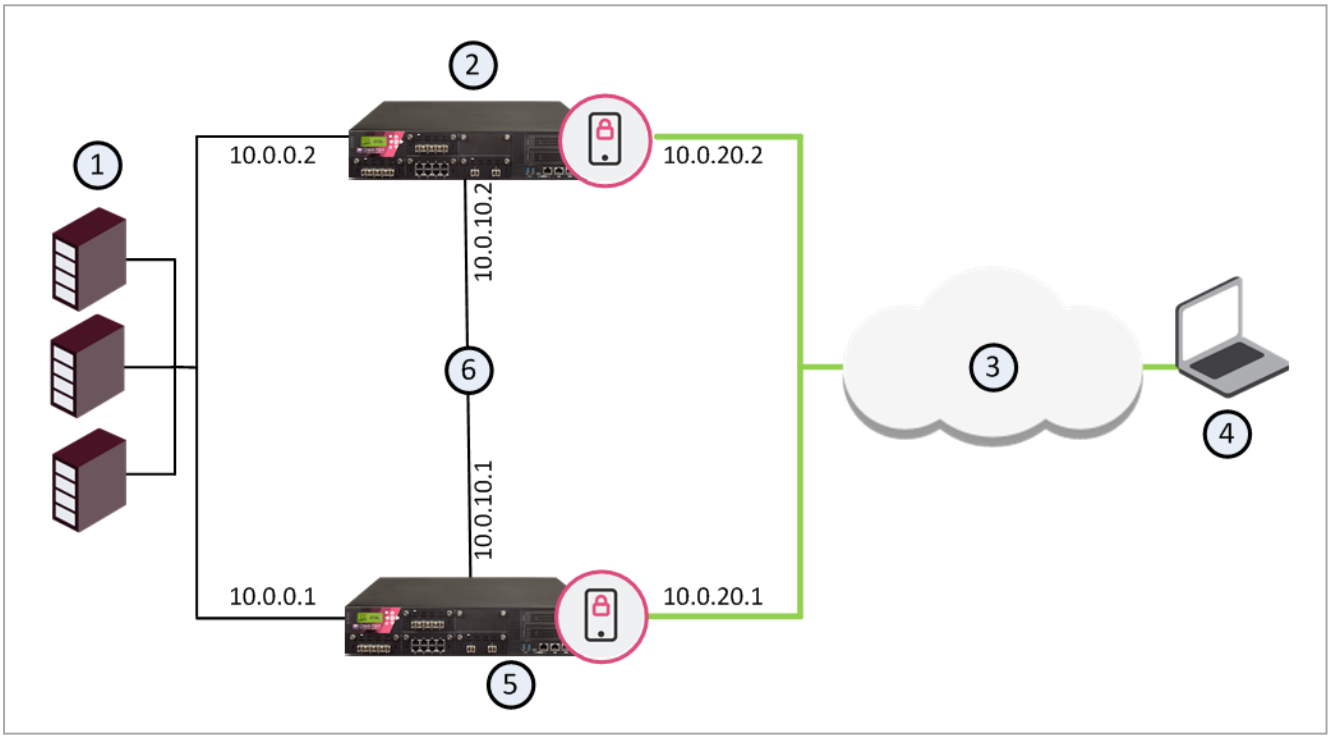

| Item | Description |
|---|---|
| 1 | Internal servers |
| 2 | Security Gateway with Mobile Access enabled |
| 3 | SSL Tunnel through Internet |
| 4 | Remote User |

# Deployment in the DMZ

When a Mobile Access enabled Security Gateway is put 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 Security Gateway. You must configure the Access Control Policy to allow traffic from the user to the Mobile Access server, where SSL termination, IPS and Anti-Virus inspection, authentication, and authorization take place. The Security Gateway forwards requests to the internal servers.

# 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.




| Item | Description |
|---|---|
| 1 | Internal servers |
| 2 | Mobile Access enabled cluster member B |
| 3 | Internet |
| 4 | Remote User making SSL connection through Internet |
| 5 | Mobile Access enabled cluster member A |

| Item | Description |
|---|---|
| 6 | Secure Network (Sync) |

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

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

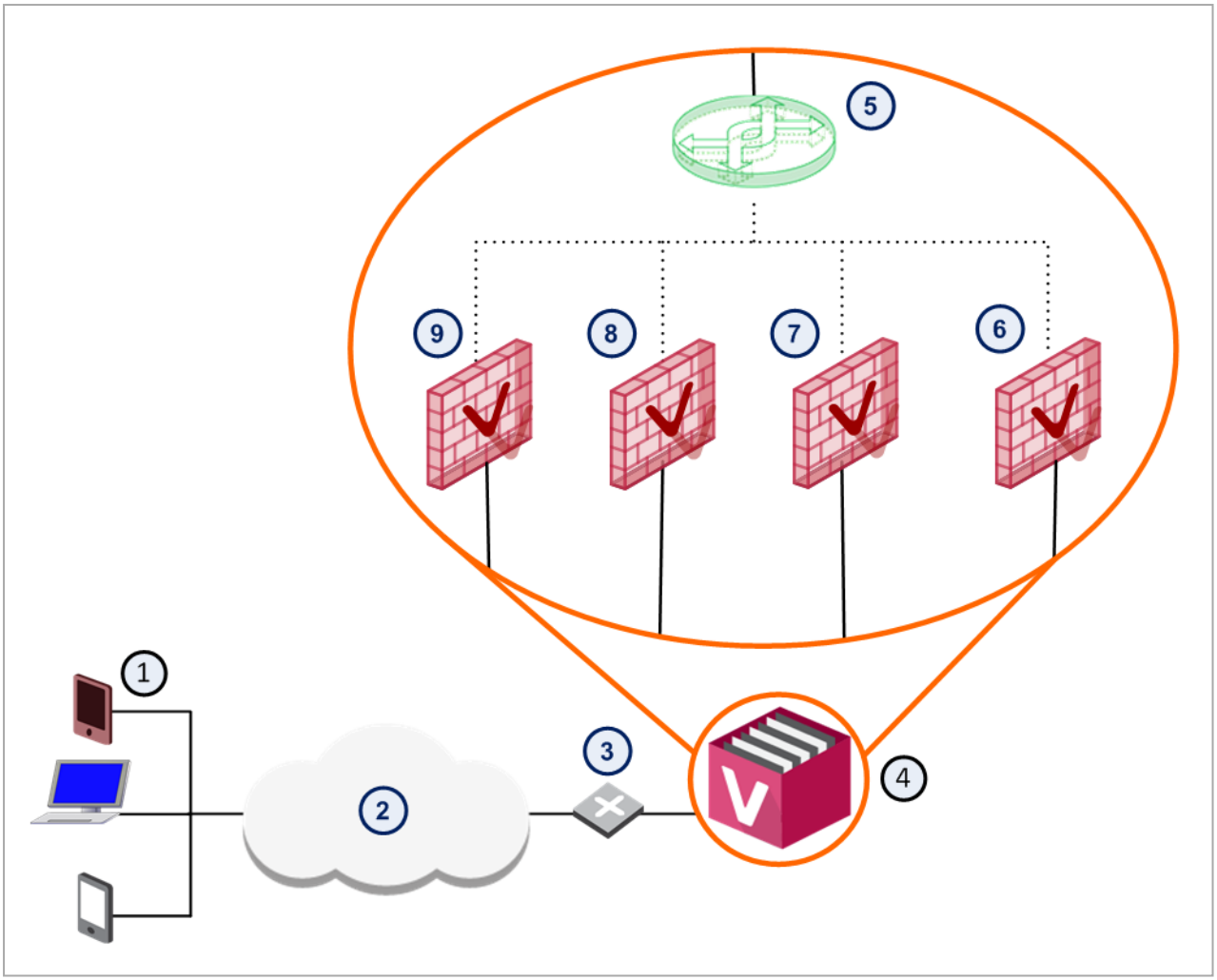
# Deployments with VSX

You can enable the Mobile Access Software Blade on VSX Virtual Systems.

This feature is supported in R77.10 and above.

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

For example, in the picture below, a VSX Gateway has four Virtual Systems with Mobile Access enabled. Each Virtual System has Mobile Access configured with different settings to meet the company's needs for different users.




| Item | Description | Example Mobile Access Portal URL |
|---|---|---|
| 1 | Remote Users | |
| 2 | Internet | |
| 3 | Router | |
| 4 | VSX Gateway | |
| 5 | Virtual Switch | |
| 6 | Virtual System 4 with Mobile Access enabled | https://guest.company.com/sslvpn |
| 7 | Virtual System 3 with Mobile Access enabled | https://finance.company.com/sslvpn |
| 8 | Virtual System 2 with Mobile Access enabled | https://sales.company.com/sslvpn |

| Item | Description | Example Mobile Access Portal URL |
|---|---|---|
| 9 | Virtual System 1 with Mobile Access enabled | https://dev.company.com/sslvpn |

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

| Virtual System | Users | Clients Allowed | Authentication Schemes | Endpoint Health Checks | Applications Configured |
|---|---|---|---|---|---|
| Virtual System 9 | Development team | Mobile Access Portal, SSL Network Extender, Capsule Workspace | Certificate + AD Password | Mobile Access Portal ESOD check for company Endpoint Security requirements Jail broken or rooted devices not allowed | Development applications |
| Virtual System 8 | Sales team | Capsule Workspace, Capsule Connect | SecurID + AD password | Jail broken or rooted devices not allowed | Sales applications |
| Virtual System 7 | Finance team | Mobile Access Portal, Capsule Workspace | SecurID + AD password | Cooperative enforcement with company MDM server | Finance applications |
| Virtual System 6 | Contractors | Mobile Access Portal | Certificate that expires after 30 days | Mobile Access Portal ESOD check for commercial AV solution and recent AV signature updates | Contractor internal applications |

## Deployment as a Reverse Proxy

You can configure a Mobile Access Security Gateway to be a reverse proxy for Web Applications on your servers, using Mobile Access. Reverse Proxy users browse to an address (URL) that is resolved to the Security Gateway IP address. Then the Security Gateway passes the request to an internal server, according to the Reverse Proxy rules. You control the security level (HTTP or HTTPS) of connections between users and resources.

See *"Reverse Proxy" on page 226*.

You can also enable Single Sign-On for Capsule Workspace with Capsule Docs users. See the *R80.40 Harmony Endpoint Security Server Administration Guide* for details.

# Sample Mobile Access Workflow

This is a high-level workflow to configure remote access to Mobile Access applications and resources.

1. Use SmartConsole to enable the Mobile Access Software Blade on the Security Gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
   a. Select mobile clients.
   b. Define the Mobile Access Portal.
   c. Define applications, for example Outlook Web App.
   d. Connect to the AD server for user information.
3. Select the policy type:
   - The default is to use the Legacy Policy, configured in the **Mobile Access** tab in SmartConsole.
   - To include Mobile Access in the **Unified Access Policy**, select this in **Gateway Properties** > **Mobile Access**.
4. Add rules to the Policy:
   - For Legacy Policy: Add rules in SmartConsole. Select **Security Policies** > **Shared Policies** > **Mobile Access** > **Open Mobile Access Policy in SmartConsole**.
   - For Unified Access Policy: Add rules in SmartConsole > **Security Policies Access Control Policy**.
5. Configure the authentication settings in **Gateway Properties** > **Mobile Access** > **Authentication**.
6. Install the Access Control Policy on the Security Gateway.

Users can access mobile applications through the configured Mobile Access Portal with the defined authentication method.

7. Optional: Give secure access to users through the Capsule Workspace app with certificate authentication.
    a. In the Security Gateway, **Mobile Access** > **Authentication**, click **Settings**, and select **Require client certificate**.
    b. Use the Certificate Creation and Distribution Wizard (in the **Security Policies** view > **Client Certificates** > **New**.
    c. Users download the Capsule Workspace app.
    d. Users open the Capsule Workspace app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.

# Mobile Access Wizard

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

See *"Check Point Remote Access Solutions" on page 24* to understand more about the remote access clients mentioned in the wizard. Many of the settings in the wizard are also in **Gateway Properties** > **Mobile Access**.

## Mobile Access

Select from where users can access the Mobile Access applications:

- **Web** - Through a browser on any computer. SSL Network Extender can be downloaded by users when necessary to access native applications.
- **Mobile Devices** - Through an iOS or Android Mobile device. Devices must have a Check Point app installed.
    - **Capsule Workspace** - Use Check Point Capsule Workspace app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
    - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.
- **Desktops/Laptops** - Check Point clients for PCs and Macs that use a Layer 3 tunnel to provide access to internal network resources.

# Mobile Access Portal

Enter the primary URL for the Mobile Access Portal.

The default URL is:

`https://<IP address of the Security Gateway>/sslvpn`

You can use the same IP address for all portals on the Security Gateway with a variation in the path.

You can import a p12 certificate for the portal to use for SSL negotiation. All portals on the same IP address use the same certificate.

**Note** - For information about Mobile Access Portal Clients Release Updates, refer to sk168353.

# Applications

Select the applications that will be available to web or mobile device users:

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

# Active Directory Integration

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

# Authorized Users

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

## What's Next?

This window helps you understand steps that are required to complete the automatic configuration done by the Mobile Access wizard. Depending on the selections you made, you might see these steps:

- **Edit the Access Control policy and add a rule for Remote Access Community** - To work with Desktop Remote Access Clients or Capsule Connect clients, the Mobile Access Wizard automatically includes this Security Gateway in the Remote Access VPN community. Remote Access Clients get access rules from the Firewall Rule Base.
- **Install policy on this security gateway** - When you install policy, the changes made by the Mobile Access Wizard become active.
- **Log in to the Web portal (usually https://<ip address>/sslvpn)** - This is the web portal that you configured. Log in to see and use it.

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

  Remote users access the portal from a Web browser with `https://<Gateway_IP>/sslvpn`, where *<Gateway_IP>* is one of these:

  - FQDN that resolves to the IP address of the Security Gateway
  - IP address of the Security Gateway

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

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

  Set up the URL for the first time in the Mobile Access First Time Wizard.
- **Install Check Point Capsule Workspace App and Desktop VPN client** - Install an App or VPN client to start using it. Prepare for mobile devices and for desktop clients (see the "Preparing for Capsule Workspace" section).
- **Easily deploy client certificates to your users with the new client certificates tool** - If you use authentication with client certificates, configure the client certificates (see the "Managing Client Certificates" section).

# Setting up the Mobile Access Portal

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

Remote users access the portal from a Web browser with `https://<Gateway_IP>/sslvpn`, where *<Gateway_IP>* is one of these:

- FQDN that resolves to the IP address of the Security Gateway
- IP address of the Security Gateway

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

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

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

## Customizing the User Portal

**To change the IP address used for the user portal:**

From the properties of the Security Gateway object, select **Mobile Access > Portal Settings**.

**To configure the look and feel of the portal:**

From the properties of the Security Gateway object, select **Mobile Access > Portal Customization**.

# Configuring Mobile Access Policy

Users can access Mobile Access applications remotely as defined by the policy rules.

On Security Gateways R80.10 and higher, there are different policy options:

- **Unified Access Policy** - Configure all rules for the Security Gateway in the Unified Access Policy. This option is only available for Security Gateways R80.10 and higher. See *"Mobile Access and the Unified Access Policy" on page 45*.
- **Legacy Policy** - Configure all rules for the Security Gateway in the shared Mobile Access Policy in the SmartDashboard. This option is available for Security Gateways of all versions and is the default for all Security Gateways.

For Security Gateways R77.30 and lower, use the Legacy Mobile Access Policy in the **Policy** page of the **Mobile Access** tab in SmartDashboard.

For all policy types, rules include these elements:

- Users and User Groups - In the Unified Access Policy, these are included in Access Roles.
- Applications that the users can access.
- The Security Gateways, to which the rule applies.

You can also include VPN and Remote Access clients in rules to define which client users can use to access the application.

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

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

# Including Mobile Access in the Unified Access Policy

**To make an R80.x Mobile Access Security Gateway use the Unified Access Policy:**

1. In SmartConsole, from the left navigation panel, click **Gateways & Servers** and double-click the Mobile Access Security Gateway object.
2. From the tree, select **Mobile Access**.
3. In the **Policy Source** area, select **Unified Access Policy**.
4. Click **OK**.
5. Install policy.

**To create rules for Mobile Access in the Unified Access Policy:**

See *"Mobile Access and the Unified Access Policy" on page 45*.

# Creating Mobile Access Rules in the Legacy Policy

The order of the rules in the Legacy Policy is not important.

**To create rules in the Mobile Access Rule Base:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Policy**.
3. Right-click the rule and select **New Rule > Below**.
4. In the **Users** column, right-click the cell and select **Add Users**.
5. In the User Viewer that opens, you can:
   - Select a user directory, either internal or an Active Directory domain.
   - Search for and select individual users, groups, or branches.
6. In the **Applications** column, right-click the cell and select **Add Applications**.
7. In the Application Viewer that opens, you can:

- Select an application from the list.
- Click **New** to define a new application.

8. If you create a New application:
   a. Select the type of application.
   b. In the window that opens enter a **Display Name** to show to end-users. For example, "Corporate Intranet".
   c. Enter the URL or path to access the application according to the example shown.
9. In the **Install On** column, right-click the cell and select **Add Objects** and select the Security Gateways for the rule.
10. Click **Save** and then close SmartDashboard.
11. In SmartConsole, install policy.

# Preparing for Capsule Workspace

**To enable devices to connect to the Security Gateway with Capsule Workspace:**

1. In SmartConsole, enable and configure Mobile Access on the Security Gateway.
2. From the **Gateway Properties**, click **Mobile Access**, and select **Mobile Devices** and **Capsule Workspace**.
3. In **Gateway Properties** > **Mobile Access** > **Authentication**, select how users authenticate to the mobile device.

   If necessary, manage certificates for authentication between the devices and the Security Gateway (see the "Configuring Client Certificates" section).
4. **Optional:** Configure ESOD Bypass for Mobile Applications (see the "ESOD Bypass for Mobile Apps" section).
5. Make sure you have rules in the Access Control Policy that allow traffic for mobile devices. For example, access to Exchange and application servers from the Security Gateway.
6. Download a Capsule Workspace App from the App Store or Google Play to mobile devices.
7. Give users instructions to connect, including the:
   - Site Name
   - Registration key (if you use certificate authentication)

If you use certificate authentication, we recommend that you include this information in the client certificate distribution email.

# Configuring Client Certificates

If you use certificates for mobile and desktop clients, use the **Client Certificates** page in SmartConsole to manage certificates for authentication between the devices and the *"Mobile Access for Smartphones and Tablets" on page 112*.

**To configure client certificates:**

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. In the **Client Certificates** pane, click **New**.

   The **Certificate Creation and Distribution** wizard opens
3. From the navigation tree click **Client Certificates**.
4. Create and distribute the certificates.
5. Install Policy.

For more details see *"Mobile Access for Smartphones and Tablets" on page 112*.

# Mobile Access and the Unified Access Policy

## Overview of Mobile Access in the Unified Policy

When you include Mobile Access in the Unified Policy, you configure all rules related to the Mobile Access Portal, Capsule Workspace, and on-demand clients in the Access Control Policy.

In the Access Control Rule Base, you can configure rules that:

- Apply to all Mobile Access Security Gateways, or some of them.
- Apply to one or more Mobile Access clients, such as the Mobile Access Portal or Capsule Workspace.

Mobile Access features such as Protection Levels, Secure Workspace, and Endpoint Compliance also apply.

Note that when you use the **Unified Access Policy**, some Mobile Access features and settings are still configured in the SmartDashboard > **Mobile Access** tab.

## Configuring Mobile Access in the Unified Policy

- You can include Mobile Access rules in Policy Layers and Inline Layers. You must enable Mobile Access on each Layer that contains rule with Mobile Access applications.

  See the *R80.40 Security Management Administration Guide* for more about layers.
- To make a Mobile Access application show in the Mobile Access Portal or in Capsule Workspace, you must put the application in the **Services & Applications** column.
  - If you put **Any** in the **Services & Applications** column, the application does not show in the portal but it is allowed. You can open it from the Mobile Access Portal if you manually enter the URL, but not from Capsule Workspace. You can change this behavior. See sk112576 for details.
  - If you put an application's service, such as HTTPS, in the **Services & Applications** column, it does not match Mobile Access https applications.
- In the **Services & Applications** column, you must use Mobile Access Application objects in rules to match Mobile Access traffic. You can define these applications in:

- In SmartConsole: **CustomApplications/Sites** > **Mobile Access and the Unified Access Policy**
- In SmartDashboard > **Mobile Access** tab > define an application

Application objects defined for Application Control, for example, are not supported in Mobile Access rules.

- When you enable Mobile Access on a Security Gateway, the Security Gateway is automatically added to the **RemoteAccess** VPN Community. Include that Community in the **VPN** column of the rule or use **Any** to make the rule apply to Mobile Access Security Gateways. If the Security Gateway was removed from the VPN Community, the **VPN** column must contain **Any**.
- Use Access Roles as the **Source** or **Destination** for a rule to make the rule apply to specified users or networks. You can also use an Access Role to represent Mobile Access or other remote access.

  You must enable Identity Awareness on each Security Gateway that is an installation target for rules with Access Roles.

# Creating Mobile Access Rules in the Unified Access Policy

**Create Mobile Access rules in the Access Control Policy with these requirements:**

| Column | Value | Explanation |
|---|---|---|
| **No** | Make sure that the rule position is logical. | The order of rules in the Rule Base is important. The first rule that matches the traffic is enforced. |
| **Name** | All | We recommend that you use a descriptive name. |
| **Source** | Access Role | Create an Access Role that includes the Users, User Groups, or Mobile/Remote Access Client that the rule applies to. See the "Mobile Access and the Unified Access Policy" section. |
| **Destination** | The internal server on which the Mobile Access application is set. | Mobile Access Applications are defined in the **Services & Applications** column. |

| Column | Value | Explanation |
|---|---|---|
| **VPN** | **Any** or a Remote Access Community that includes the Mobile Access Security Gateway | When you enable the Mobile Access or IPsec Software Blade on a Security Gateway, the Security Gateway is automatically added to the default **RemoteAccess** VPN Community. By default the community also contains a user group that contains all users. If you remove the Security Gateway from the VPN Community, you must select **Any**. |
| **Services & Applications** | Mobile Applications<br>Do not include applications or service objects that are not specified as Mobile Access. | To create a Mobile Application: Click + > click ✳ > **Mobile Applications** > select an application type and define it.<br>To select an existing Mobile Application: Click + > ***All** > **Mobile Applications** and select one.<br>Mobile Applications only show in the list if Mobile Access is enabled on the Layer |
| **Content** | **Any** | Content Awareness is not relevant for Mobile Access rules. |
| **Action** | **Accept** or **Drop** | Only **Accept** and **Drop** are supported. **Reject** is also supported but acts the same as **Drop**. You can also select **Inline Layer** to send all traffic that matches the rule to a "Mobile Access and the Unified Access Policy". |
| **Track** | All log options | Right-click in the cell and select **More** > **Extended log** |
| **Install On** | One or more Security Gateways | Each Security Gateway must have Mobile Access and Identity Awareness enabled and have **Unified Access Policy** selected as the **Policy Source**. |

## Mobile Access Applications in the Unified Access Policy

To use a Mobile Access application in the Unified Access Policy, you must define it as a **Mobile Application** from the SmartConsole or define it in the in SmartDashboard > **Mobile Access** tab.

Other application objects, such as URL Filtering applications, are not relevant for Mobile Access. For example: To authorize Facebook as a web application in Mobile Access, you must create a new Web Application and specify Facebook's URL. You cannot use the URL Filtering Facebook application, because it is not for Mobile Access.

### Creating Mobile Applications for the Access Control Policy

**To create a Mobile Application object to use in the Access Control Policy:**

1. In SmartConsole, expand the **Objects** pane.
2. Select **New** > **More** > **Custom Application/Site** > **Mobile Application**.
3. Select a type of Mobile Application.
4. Define the **General Properties** and **Authorized Locations**.
5. Optional: Define more settings for the Application.
6. Click **OK**.

## Access Roles for Remote Access

Create a rule in the Access Control Rule Base that handles remote access connections.

1. Go to **Security Policies** and right-click the cell in the VPN column.
2. Select **Specific VPN Communities**.
3. Choose the community and click +.
4. Close the VPN community window.
5. Define **Services & Applications** and **Actions** columns.
6. Install the policy.

**Example:**

To allow remote access users to access the organization's SMTP server, called SMTP_SRV, create the following rule:

| Source | Destination | VPN | Service | Action | Track |
|---|---|---|---|---|---|
| Any | SMTP_SRV | Remote_Access_ Community | SMTP | Accept | Log |

# Including Mobile Access in the Unified Policy

After you configure rules for Mobile Access in the Unified Access Policy, configure the Security Gateway to use the **Unified Access Policy**.

**To make an R80.x Mobile Access Security Gateway use the Unified Access Policy:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Mobile Access Security Gateway object.
2. From the tree, select **Mobile Access**.
3. In the **Policy Source** area, select **Unified Access Policy**.
4. Click **OK**.
5. Install policy.

# Enabling Access Control Features on a Layer

**To enable Mobile Access on an Ordered Layer:**

1. In SmartConsole, click **Security Policies**.
2. Under **Access Control**, right-click **Policy** and select **Edit Policy**.
3. Click options  for the Layer.
4. Click **Edit Layer**.

   The **Layer Editor** window opens and shows the **General** view.
5. Select **Mobile Access**.
6. Click **OK**.

**To enable Mobile Access on an Inline Layer:**

1. In SmartConsole, click **Security Policies**.
2. Select the Ordered Layer.
3. In the parent rule of the Inline Layer, right-click the **Action** column, and select **Inline Layer** > **Edit Layer**.
4. Select **Mobile Access**.
5. Click **OK**.

# Best Practices for Mobile Access in the Unified Policy

When you include Mobile Access in the Unified Access Policy, these are some factors that you need to be aware of:

- How to use layers
- How the content of rules affects your policy
- How rule order can affect your policy

## Best Practices with Layers

We recommend that you make an Inline Layer for Mobile Access rules, to easily manage the Mobile Access policy.

To use an Inline Layer effectively, define a parent rule in the main layer. The parent rule matches all Mobile Access traffic and sends the traffic to the Inline Layer. It requires an Access Role that includes all Mobile Access client types or traffic in the **Source** column.

When a rule contains **Inline Layer** in the **Action** column, an Inline Layer is automatically created below it and it becomes a parent rule.

| No | Name | Source | Destination | VPN | Services & Applications | Action | Track |
|---|---|---|---|---|---|---|---|
| 1 | Network rules | My_ network | GW | Any | Any | Accept | Log |
| 2 | Mobile Access Inline Layer Entry Point | All Mobile Access traffic | Any | Any | Any | Mobile Access Inline Layer | Extended Log |
| 2.1 | Capsule Workspace rule | Capsule Workspace traffic | Any | Any | Business Mail Corporate Ordering | Accept | Extended Log |
| 2.2 | Special access rule | Managers | Any | Any | Internal App | Accept | Extended Log |
| 2.3 | Mobile Access Inline Layer Cleanup rule | Any | Any | Any | Any | Drop | Extended Log |

| No | Name | Source | Destination | VPN | Services & Applications | Action | Track |
|---|---|---|---|---|---|---|---|
| 3 | Cleanup rule | Any | Any | Any | Any | Drop | Log |

**To make a rule that sends all Mobile Access traffic to a Mobile Access Inline Layer:**

1. From the **Source** column of a rule in the Access Control Policy, create a new Access Role that includes all Mobile Access client types:
   a. In the New Access Role window, click **Remote Access Clients**.
   b. Select **Specific Client** and create a **New > Allowed Client** for all Mobile Access Portals or clients that are used in your environment. These can include: Capsule Workspace, Mobile Access Portal, ActiveSync, and SSL Network Extender.
2. Make sure the **VPN** column contains **Any** or the **RemoteAccess** VPN Community that contains your Mobile Access Security Gateways.
3. In the **Action** column, select **Inline Layer** > **New Layer**.
4. In the **Layer Editor**:
   - Enter a name for the layer, such as **Mobile Access Inline Layer**.
   - In the **Blades** area, select Mobile Access.
   - Optional: To use this Mobile Access Inline Layer in multiple policies, in the **Sharing** area, click **Multiple policies and rules can use this layer**.

**To configure rules in the Inline Layer:**

1. Click the **Cleanup** rule in the Inline Layer that was created automatically and the click the **Add Rule Above** icon.
2. Configure rules for the Mobile Access policy as required. See the "Mobile Access and the Unified Access Policy" section.
3. Make sure that the Cleanup rule stays at the end of the layer and that the Action is Drop.
4. Right-click in the **Track** cell and select **More** > **Extended log**.

## Mobile Access with Ordered Layers

If you work with Ordered Layers, you can configure a Mobile Access Inline Layer in any Ordered Layer.

Make sure to create a *bypass* rule for Mobile Access traffic in all layers that come before the Mobile Access layer. For example, if your Mobile Access Inline Layer is in the third layer, you must create a bypass rule in the first and second Ordered Layers.

The bypass rule matches the Mobile Access traffic in the layer and allows the traffic. The traffic then moves to the next layer, until it gets to the Mobile Access Inline Layer.

To create a bypass rule, use the Access Role for all Mobile Access users in the **Source** column and **Accept** in the **Action** column.

# Best Practices for Rules

- Do not use a Security Gateway as the **Destination** in a Mobile Access rule. The rules authorize a user's access to an internal resource. Use **Any** or the internal hosts of relevant applications in the **Destination** column.
- Do not use **Any** in the **Services & Applications** column. To make an application show in the Mobile Access Portal or Capsule Workspace, it must be Mobile Access application object that is used explicitly in the Rule Base.

  If you do use **Any** to represent all Mobile Access applications, configured Mobile Access applications are authorized, but they do not show in the portal or Capsule Workspace. Users can enter the URL of the App in the **Address** field of the Mobile Access Portal.

  To change the behavior when **Any** is used to represent Mobile Access applications, see sk112576.

# Best Practices for Rule Order

In the Unified Access Policy, put Mobile Access rules that authorize applications above rules that contain a related service. For example, put a rule to allow a web application above a rule that allows or blocks HTTP/HTTPS. If the HTTP/HTTPS rule is first, the user will not see the Mobile Access Web application in the portal or in Capsule Workspace and will not be able to access it.

For example, this Rule Base allows Outlook Web Access (OWA), a web-based Mobile Access application. It also allows HTTPS traffic:

**Correct way to allow the HTTPS service and also Mobile Access HTTPS applications:**

| No | Name | Source | Destination | Services & Applications | Action | Track |
|---|---|---|---|---|---|---|
| 1 | Network rule | My_ network | GW_1 | Any | Accept | Log |

| No | Name | Source | Destination | Services & Applications | Action | Track |
|---|---|---|---|---|---|---|
| 2 | Mobile Access Inline Layer | All Mobile Access traffic | Any | Any | Mobile Access Inline Layer | Log |
| 2.1 | Mobile Access applications | All Mobile Access traffic | Any | Internal App OWA Business Mail | Accept | Log |
| 2.2 | Cleanup rule | Any | Any | Any | Drop | Log |
| 3 | Allow HTTPS | Any | Any | https | Accept | Log |
| 4 | Cleanup rule | Any | Any | Any | Drop | None |

Rule **2.1**, that allows access to Mobile Access applications, including Outlook Web Access (OWA) on HTTPS, is above rule **3**, which allows all HTTPS traffic.

If you put rule **3** to allow HTTPS above the Mobile Access rules, the user will not see the OWA Web application in the portal or in Capsule Workspace and will not be able to access it. To authorize a Mobile Access application, you must use a Mobile Access application in the **Services & Applications** column.

You *can* use HTTPS in the parent rule of the Mobile Access Inline Layer, but specify the Mobile Access application inside the Inline Layer. That way, the HTTPS traffic for OWA, for example, will match on the HTTPS rule, and will also match on the OWA App inside the Inline Layer.

### Native Applications

In this scenario with a Native application:

- The Native application is in an Inline Layer in the rule base.
- And the Native application configuration includes **Any** in the **Authorized Locations** tab.

Then the parent rule of the Inline Layer must include one of these in the Services & Applications column:

- **Any** service
- **HTTPS** service
- The Native Application

# Mobile Access Behavior in the Rule Base

- In a policy with Policy Layers, for the traffic to be approved, it needs to be accepted in all layers. It is only authorized when accepted in the last layer. The policy keeps going to the next layer until the Mobile Access traffic is matched with a **Drop** rule or it is accepted in all layers.
- In Inline Layers, like in multi-layered policies: Mobile Access is matched on the Inline Layer parent rule and then on the inner rule inside the Inline Layer. The matched application for Mobile Access is taken from the last rule matched with a Mobile Access application. If the matched rule inside the Inline Layer has no Mobile Access application, the policy looks for a Mobile Access application in the parent rule of the Inline Layer.

# Limitations for Mobile Access in the Unified Policy

- Mobile Access cannot work with Content Awareness or URL Filtering. Do not use Content Awareness or URL Filtering objects in rules with Mobile Access.
- These limitation apply for Access Roles in Mobile Access rules in the Unified Access Policy:
  - In the **Source** column - Access Roles can include **Networks**, **Users**, and **Remote Access Clients**.
  - In the **Destination** column - Access Roles can include **Networks** and **Users**.
- The Native Applications **Connect** button always shows in the Mobile Access Portal when SSL Network Extender is enabled.
- If users do not meet the defined Protection Level requirements for an application, the application does not show for them. This is true in the Mobile Access Portal and Capsule Workspace. (In the Legacy Mobile Access policy, the applications show but are disabled).
- If the Mobile Access Security Gateway was removed from the **RemoteAccess** VPN Community, the **VPN** column must contain **Any**.
- If you configure Unified Policy, you must include the authorized location (the range of IP addresses) for each application inside the encryption domain for remote access.

  **Note** - The range of IP addresses for an application must not overlap with the range for another application. Users with access to the first application have access to other applications within the same range.

# Mobile Access Applications

## Introduction to 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.

# File Shares

A file share is a collection of files, made available across the network by means of a protocol that enables actions on files, including opening, reading, writing, and deleting files across the network.

## Configuring File Shares

**To create a new File Share Application:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > File Share**.

   The **File Share Application** window opens.

### 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 lets you configure the file shares that users are authorized to access. These settings take effect whenever a user attempts access, no matter what interface is used, whether by manually typing a path in the portal, browsing using the file viewer, clicking a user-defined file favorite, or clicking the predefined file favorite path defined by the administrator in the **Link in Portal** page.

2. Fill in the fields on the page:

   - **Servers** are the machine(s) or DNS Name(s) on which the file server is hosted. Choose either a single **Host or DNS name**, or **Multiple hosts**.
   - **Allow access to any file share** gives the users access to all locations on the file server defined in **Servers**.
   - **Allow access to specific file shares** restricts user access to specific shares. For example `My_Share`. Use only the name of a share, such as `My_share`, `$$user`, or `My_share$`, without any slashes. Do not specify a sub-directory inside a share. The `$$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`, she will be allowed access to the share called `alice` that was defined on the server, such as `\\myserver\alice`.

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

## File Share Application - Link in Portal Page

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

1. Go to the **Link in Portal** page of the **File Share Application** object.
2. Fill in the fields on the page:

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

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

- **Tooltip (multi-language)** - Gives additional information. It can include `$$user`, which represents the user name of the currently logged-in user. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor 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**

## File Share Application - Protection Level Page

1. Go to the **Protection Level** page of the **File Share Application** object.
2. Fill in the fields on the page:

   **Security Requirements for Accessing this Application** allows you to:

   - Allow access to this application to any endpoint machine that complies with the security requirements of the Security Gateway
   - Make access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile

## Completing the Configuration of the File Share Application

1. Go to the **Policy** page of the Mobile Access tab.
2. In the **Policy** page, make rules to associate:

- *User groups*.
- *Applications* that the users in those user groups are allowed to access.
- *Install On* are the Mobile Access Security Gateways and Clusters that users in those user groups are allowed to connect to.

3. Click **Save** and then close SmartDashboard.
4. In SmartConsole, install the policy.

## Using the $$user Variable in File Shares

You can configure personalized user locations that use the login name of the currently logged in user. To do this, use the Mobile Access Applications 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`.

# 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

You can include Protection Levels in the definition of most Mobile Access application types. Each application can have a Protection Level associated with it. A single Protection Level can be assigned for all native applications.

When you define 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 Security 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. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree click **Additional Settings > Protection Levels** page from the navigation tree.

3. Click **New** to create a new Protection Level or double-click an existing Protection Level to modify it.

   The **Protection Levels** window opens, and shows the **General Properties** page.

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

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E). Or in SmartDashboard, **Mobile Access** tab, go to **Applications** > Application type.

2. Search for the Mobile Access application.

3. Double-click the application.

4. From the navigation tree, select **Additional Setting > Protection Level**.

5. To create a new Protection Level, select **Manage > New**.

6. 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, and shows the **General Properties** page.

**To configure the settings for a Protection Level:**

1. From the **General Properties** page in the **Protection Level** window, enter the **Name** for the Protection Level (for a new Protection Level only).

2. In the navigation tree, click **Authentication** 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 necessary, select **User must successfully authenticate via SMS**.

4. In the navigation tree, click **Endpoint Security** and select one or both of these 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 gives 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 policy.

# Web Applications

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

Mobile Access supports browsing to websites that use HTML and JavaScript.

Browsing to websites with VBScript, Java, or Flash elements that contain embedded links is supported using SSL Network Extender, by defining the application as a native application.

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

## Web Applications of a Specific Type

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

### iNotes

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

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

**Note** - To make iNotes work through the Mobile Access Portal, you must work with Mobile Access Applications.

These iNotes features are not supported:

- Working offline
- Notebooks with attachments.
- Color button in the Mail Composition window.
- Text-alignment buttons in the Mail Composition window.
- Decline, Propose new time and Delegate options in meeting notices.
- Online help- partial support is available.

### Outlook Web Access

Outlook Web Access (OWA) is a Web-based mail service, with the look, feel and functionality of Microsoft Outlook. Mobile Access supports Outlook Web Access versions 2000, 2003 SP1, 2007, 2010, 2013, and 2016.

## Configuring Mobile Applications

You can use SmartConsole to create and configure the settings for all the Mobile Access application objects. However, there are some Mobile Access settings that you can configure only from SmartDashboard.

**To create a new Mobile application in SmartDashboard:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartConsole opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Applications**.
3. Click the applicable application category.
4. Click **New**.

**To create a new Mobile application in SmartConsole:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New > Custom Application/Site > Mobile Application** and select the Mobile application type.

   The Mobile application window opens.

### Web Application - General Properties Page

Use the **General Properties** page to configure the basic settings for the Web Application.

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.

- **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.
  - **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

Use the **Authorized Locations** page to define the locations that can access the Web Application.

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.

- **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 pathscan include $$user, which is the name of the currently logged-in user.
- **Application paths are case sensitive** improves security. Use this setting for UNIX-based Web servers that are case sensitive.

- **Services** that are allowed are typically HTTP for cleartext access to the Web application, and HTTPS for SSL access.

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

- **Advanced** lets you select multiple services.

## Web Application - Link in Portal Page

Use the **Link in Portal** page to configure a link to the Web Application in the Mobile Access user portal.

- **Add a link to this Web application in the Mobile Access Portal** - 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.
- **Link text (multi-language)** - Shows in the Mobile Access Portal. Can include `$$user`, which represents the user name of the currently logged-in user. If more than one link is configured with the same (case insensitive) name, only one of them will be shown in the portal.
- **URL** - The link to the location of the application. Can include `$$user`, which represents the user name of the currently logged-in user. For example, a URL that is defined as `http://host/$$user` appears for user `aa` as `http://host/aa` and for user `bb` as `http://host/bb`.
- **Tooltip (multi-language)** - Gives additional information. It can include `$$user`, which represents the user name of the currently logged-in user. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor away from the link.

## Web Application - Protection Level Page

Use the **Protection Level** page to choose the protection level for Web applications, and configure how browser caching is configured.

**Security Requirements for Accessing this Application:**

- **This application relies on the security requirements of the gateway**

  Rely on the Security 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.

**Browser Caching on the Endpoint Machine** - Control caching of web application content in the remote user's browser.

- **Allow caching of all content** - Recommended setting for Hostname Translation, method of Link Translation. ActiveX and streaming media will use Hostname Translation.
- **Allow caching of these content types** - Select type of web application content to cache: images, scripts, HTML.
- **Prevent caching of all content** - Improves security for remote users who access a Web Application from a workstation that is not under their full control. Personal data is not stored on the workstation. **Be aware!** This setting prevents files that require an external application (for example, MS Office files) from opening. It can cause some applications to malfunction, if the application requires caching.

### Configuring Web Content Caching

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

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

### To let users open external files:

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

## Web Application - Link Translation Page

Use the **Link Translation** page to configure how the Web Application converts the internal URLs to valid links for the Internet.

- **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 Gateways** section.
- **Using the following method** - Select the Mobile Access Applications that this application uses:
  - **Path Translation** - Default for new installations.
  - **URL Translation** - Supported by the Mobile Access Security Gateway with no further configuration
  - **Hostname Translation** - Mobile Access Applications.

## 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 the "Mobile Access Applications" section.

## Completing the Configuration of the Web Application

To complete the configuration, add the Web application to a policy rule and install policy from SmartConsole.

For Unified Access Policy, see *"Mobile Access and the Unified Access Policy" on page 45*.

For legacy policy, see *"Getting Started with Mobile Access" on page 32*.

## 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.

## 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"`

# Web Application Features

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

## Reuse TCP Connections

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

**Best Practice** - We strongly recommend that you back up configuration files before you make changes.

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

In previous versions, if you chose one of these Application Type options, the TCP connections for the application are closed after each request. However, if you enable Reuse TCP Connections, the connections are reused. This leads to a boost in performance as the three-way handshake does not have to be renewed and the optimized authorization cache feature can be fully utilized.

By default, Reuse TCP Connections is enabled.

**To turn off Reuse TCP Connections:**

1. Change this line in the `$CVPNDIR/conf/http.conf` configuration file:

   from:

   ```
   CvpnReuseConnections On
   ```

   to:

   ```
   CvpnReuseConnections Off
   ```

2. Save the changes.
3. Run the `cvpnrestart` command to activate the settings.

If your Mobile Access Security Gateway is part of a cluster, make the same changes on each cluster member.

## Website Certificate Verification

Mobile Access lets you validate website security certificates, and either warn the user about problems, ignore any problems, or block websites with certificate problems.

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

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

You can configure Website Certificate Verification per Security Gateway and per application.

Website Certificate Verification is configured in Database Tool (GuiDBEdit Tool) (see sk13009).

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

1. In Database Tool (GuiDBEdit Tool), go to the **Network Objects > network_objects** > the Security Gateway object
2. In the bottom pane, go to the **Connectra_settings** section.
3. Search for:

   **certificate_verification_policy**
4. Enter **block**, **warn**, **monitor**, or **ignore** as the value.

   The default setting is monitor.

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

If the Mobile Access Security 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 Database Tool (GuiDBEdit Tool), go to the **Network Objects > network_objects** > the Web application object
2. In the bottom pane, search for **certificate_verification_policy**.
3. Type **block**, **warn**, or **ignore** as the value.
4. For the **use_gateway_settings** parameter:
   - Enter **true** to use the Security Gateway settings.
   - Enter **false** to use the setting configured for the application.
5. Save the changes in Database Tool (GuiDBEdit Tool) and close it.
6. Install policy on the Security Management Server.

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

## Saving a Trusted Certificate in .pem Format

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

**To save a trusted certificate in .pem format using Internet Explorer 7.0:**

1. Using your browser, **View** the certificate of a website that uses the Certificate Authority you want to add. Be sure to choose the Certificate Authority certificate: In the **Certification Path** tab, choose the CA and click View Certificate.
2. Select the **Details** tab and click **Copy to File**.

   The **Certificate Export Wizard** opens.
3. In the **Export File Format** page, select Base-64 encoded.
4. In the **File to Export** page, type the File name under which you want to save the certificate information with a .pem file extension.
5. Click **Finish**.

## Moving the CA Certificate to the Mobile Access Security Gateway

**To move the CA Certificate to the Mobile Access Security Gateway:**

1. Move the .pem file to your Mobile Access Security 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 Security 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 Security Gateway.
2. Run the following command: `rehash_ca_bundle`

   You do not need to restart Mobile Access services for the change to take effect.

# Link Translation

Link Translation is the process by which Mobile Access converts internal URLs to public URLs that are valid on the Internet. In this way internal resources become accessible through all internet browsers.

Mobile Access converts HTTP requests into secure HTTPS requests and changes the port to 443. To accomplish this, Mobile Access translates the source URL into an HTTPS URL that routes traffic to its destination through the Mobile Access Security Gateway. The translated URL is returned to the browser and is shown to users.

Mobile Access supports different methods of Link Translation:

- **Path Translation (PT)** - The default method that works with most web applications.
- **URL Translation (UT)** - The original link translation method, maintained for backward compatibility.
- **Hostname Translation (HT)** - This method is faster and supports a wider range of Web applications than PT. It requires additional configuration and a certificate.
- **Client-side Link Translation** - Works on the end user's browser through the Mobile Access browser plugin OR on a Wrapped Mobile application. It translates each request sent through Mobile Access on the client side.

## How Translated URLs Appear in a Browser

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

| Method | Translated `http://www.example.com/path` |
|---|---|
| UT | `https://ssl.example.com/Web/path,CVPNHost=www.example.com,CVPNProtocol=http` |
| HT | `https://c-ds1q-itfgppae7oq.ssl.example.com/path`<br>Note that the seemingly random character string, `c-ds1q-itfgppae7oq`, represents the destination URL. |
| PT | `https://ssl.example.com/PT/http://www.example.com/path` |
| Client-side | `https://ssl.example.com/PT/http://www.example.com/path` |

# SmartDashboard Configuration of Link Translation

You can configure Link Translation to meet the requirements of the application (a web application or a Citrix service) or of the Security Gateway through which the applications are accessed. For example, you can configure one Mobile Access application to work with URL Translation, while all other applications supplied by the Security Gateway use Path Translation.

- You can set the default Link Translation method for all applications of a Security Gateway - Only applications that have a different method configured will not use the default method.
- You can set the default Link Translation method for an application - This Web application uses the selected method, even if another method is default on the Security Gateways.
- You can configure which domains are translated.

## Configuring PT

Path Translation (PT) is selected by default for newly installed Security Gateways.

**To configure PT as default method for Security Gateways:**

1. In SmartConsole, right-click the Security Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Link Translation**.
3. Under **Supported Translation Methods**, make sure that **Path Translation (always supported)** is selected.
4. Under **Default Translation Method**, select **Path Translation**.
5. Click **OK**.

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

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The Web Application window opens.
4. Click **Additional Settings > Link Translation**.

   The **Link Translation** page of the Mobile Access application opens.
5. Select **Use the following method > Path Translation**.

6. Click **OK** and close the Web Application window
7. Install the policy.

## Configuring UT

URL Translation is supported by all versions of Security Gateways.

**To configure UT as default method for Security Gateways:**

1. In SmartConsole, right-click the Security Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Link Translation**.
3. Under **Supported Translation Methods**, make sure that **URL Translation (always supported)** is selected.
4. Under **Default Translation Method**, select **URL Translation**.
5. Click **OK**.

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

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The **Web Application** window opens.
4. Click **Additional Settings > Link Translation**.

   The **Link Translation** page of the Mobile Access application opens.
5. Click **URL Translation**.
6. Click **OK**.
7. Install the policy.

## Using 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.

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

**Important** - If the DNS server is not configured to resolve wildcard Mobile Access host names, users will be unable to connect to Mobile Access, because the portal changes to a sub-domain: `portal.ssl.example.com`.
If you use Hostname Translation as your method for link translation, users must enter an FQDN as the portal URL and not an IP address.

### Configuring HT

#### To configure the DNS server for HT:

1. Add a record to the DNS server, to resolve Mobile Access sub-domains to the Mobile Access IP address: `*.domain`

   For example, assume `ssl.example.com` is the Security Gateway. Configure the DNS to resolve `*.ssl.example.com` to the Security Gateway IP address. This wildcard includes all sub-domains of the parent domain, such as `a.ssl.example.com` and `b.ssl.example.com`.

2. Define the parent domain (`ssl.example.com`) as a separate DNS record, to resolve Mobile Access IP address.

   This lets users access the Mobile Access Portal directly, with its FQDN.

3. *"Server Certificates" on page 236*.

#### To configure HT as default method for Security Gateways:

1. In SmartConsole, right-click the Security Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.

2. From the navigation tree, click **Mobile Access > Portal Settings**.

   If this message appears, clear **Hostname Translation**, for now:

   ```
   Hostname Translation requires Portal URL to be defined in the
   following format: 'https://hostname/'
   ```

3. In **Main URL**, enter the portal URL of the Mobile Access Security Gateway.
4. From the navigation tree, click **Link Translation**.
5. Under **Supported Translation Methods**, click **Hostname Translation**.
6. Under **Default Translation Method**, select **Hostname Translation**.
7. Click **OK**.
8. Install the policy.

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

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The **Web Application** window opens.
4. Click **Additional Settings > Link Translation**.

   The **Link Translation** page of the Mobile Access application opens.
5. Select **Use the following method > Hostname Translation**.
6. Click **Advanced Hostname Translation Settings**.
7. Select the **HTTP Cookies Handling** mode:
   - **On the gateway** - Default. All HTTP cookies that are sent to clients by internal Web servers are stored on Mobile Access, and are not passed on to the client's browser.
   - **On the endpoint machine** - If the default setting causes the JavaScript (from the internal servers that run on the client browser) that handles HTTP cookies to fail, select this option. Mobile Access passes HTTP cookies to the browser.
8. Click **OK** and close the Web Application window.
9. Install the policy.

## Configuring Link Translation Domains in SmartDashboard

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.

Configure which domains use link translation in SmartDashboard > **Mobile Access** tab > **Additional Settings** > **Link Translation > Link Translation Domains**.

For Security Gateways R77.30, to enable this feature, you must install the R77.30 Add-on.

This option is not supported in Security Gateways lower than R77.30.

**To manually configure domains to translate:**

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

**Link Translation Domains**

The options are:

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

# Link Translation with Wrapped Applications

With *Client-Side Link Translation with wrapped applications*, Check Point Mobile App clients are responsible for link translation for specified, *wrapped applications*. These applications are *wrapped* in a security container that gives them secure access to network resources and prevents data leakage.

Wrapped applications are only available with mobile devices and do not show in the Mobile Access Portal.

To use Client-Side Link Translation with wrapped applications, see the App Wrapping Guide.

# Link Translation Issues

These Link Translation configuration tips apply to Web applications.

- For Web sites that use ActiveX and streaming media, configure Mobile Access Web applications to Allow caching of all content. This is configured in the **Protection Level** page of the Web application.
- Domain cookies created in JavaScript are not supported. For example, if you create a cookie with this JavaScript code:

  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, if 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`

  The maximum number of characters in each part of the host name (between https:// and the /path) is limited to 63 (see RFC 1034). Therefore, the entire internal host name, including the protocol and the port, Mobile Access Applications.

- Hostnames displayed in client browsers appear as a seemingly random character string, instead of the complete destination path.
- If you sign out from Outlook Web Access, Domino Web Access (iNotes), or Microsoft SharePoint, the Mobile Access session can become disconnected.

# Citrix Services

## Citrix Deployments Modes - Unticketed and Ticketed

### Unticketed Mode

In the recommended Unticketed Mode scenario:

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

### Ticketed Mode

In the Ticketed Mode scenario:

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

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

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

# Configuring Citrix Services

**To configure a new Citrix Service:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > Citrix Services**.

   The **Citrix Services** window opens.

## Before Configuring Citrix Services

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

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

**Note** - Make sure that the certificate is *"Server Certificates" on page 236*.

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

## Citrix Service ? Web Interface page

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

## Citrix Service ? Link in Portal Page

1. Go to the **Link In Portal** page of the **Citrix Service** object.
2. Fill in the fields on the page:
   - **Link text (multi-language)** - Shows 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** - The link to the location of the application, or to a sub-directory of the application.
- **Tooltip (multi-language)** - Gives additional information. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor away from the link.

## Citrix Service ? STA Servers Page

1. Go to the **STA servers** page of the **Citrix Service** object.
2. Get the Host from the current settings on the Web Interface (WI) server.
3. Get the STA ID from the Secure Ticketing Authority (STA) servers.

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

**To get the host name or IP address:**

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

**To get the STA ID:**

1. Login to the STA server.
2. From the Windows **Start** menu, select **Programs > Citrix > Citrix Secure Gateway > Secure Ticket Authority Configuration**.
3. Click **Next**.

The STA ID is shown in the **Enter the STA ID** field.

## Citrix Service - MetaFrame Servers Page

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

If you select **Restrict access to these servers only**:

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

## Citrix Service - XenApp Servers Page

Use the **XenApp Servers** page to configure access to the XenApp Servers.

**Note** - If you select **Restrict access to these servers only**,

1. Define the servers using an IP address or Fully Qualified Domain Name (FQDN).
2. Make sure that the definition matches the configuration made on the Metaframe server farm.

   If you do not, Mobile Access may not authorize the connection. (The XenApp server configuration affects one of the parameters in the ICA file that is received by the client).

## Citrix Service - Single Sign On Page

Single Sign On increases application security.

**To configure Single Sign On:**

1. Go to the **Single Sign On** page of the **File Share Application** object.
2. Select **Turn on single Sign On for this application**.

   Configure the sign on method for the application.

## Citrix Service - Protection Level Page

1. Go to the **Protection Level** page of the **Citrix Service** object.
2. Enter data in these fields:

   **Security Requirements for Accessing this Application** lets you:

   - Allow access to this application to any endpoint that complies with the security requirements of the Security Gateway,
   - OR make access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile.

   **Note** - The Citrix architecture requires ICA files and ActiveX executables to be temporarily cached by the client-side browser. As a result, Mobile Access's Protection Level settings do not apply to these files.

3. Get the Host and the STA ID of the Secure Ticketing Authority (STA) servers from the current settings on the Web Interface (WI) server.

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

**To get the hostname or IP address:**

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

**To get the STA ID:**

1. Login to the STA server.
2. From the Windows **Start** menu, select **Programs > Citrix > Citrix Secure Gateway > Secure Ticket Authority Configuration**.
3. Click **Next**.

   The STA ID is shown in the **Enter the STA ID** field.

### Completing the Configuration of the Citrix Service

To complete the configuration, add the Citrix Service to a policy rule and install policy from SmartConsole.

For Unified Access Policy, see *"Mobile Access and the Unified Access Policy" on page 45*.

For legacy policy, see *"Getting Started with Mobile Access" on page 32*.

# 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 Web Mail Services

**To configure a new Web Mail application:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > Mail Service**.

   The **Web mail service** window opens.

## 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)** - Shows 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)** - Gives additional information. The text appears automatically when the user holds the cursor over the link. It disappears when the user clicks a mouse button or moves the cursor away from the link.

## Web Mail Service - Single Sign-On Page

Configure the *"Single Sign On" on page 87* settings for the Web Mail Service.

1. Go to the **Single Sign On** page of the **Web mail service** object.
2. Select the sign on method for the application.

## 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** lets you:

- Allow access to this application to any endpoint machine that complies with the security requirements of the Security Gateway,
- Give access to the application conditional on the endpoint being compliant with the selected Endpoint Compliance Profile.

### Completing the Configuration of the Web Mail Service

To complete the configuration, add the Web Mail application to a policy rule and install policy from SmartConsole.

For Unified Access Policy, see *"Mobile Access and the Unified Access Policy" on page 45*.

For legacy policy, see *"Getting Started with Mobile Access" on page 32*.

### 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 Security Gateway. To enable search on contacts that are defined on an LDAP server, see sk34997.

# Native Applications

Native Applications are not clientless. They require the SSL Network Extender client on the endpoint machine. For more information, see the SSL Network Extender (SNX) Administration Guide.

# DNS Names

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

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

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

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

## DNS Names and Aliases

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

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

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

# Where DNS Name Objects are Used

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

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

# Defining the DNS Server used by Mobile Access

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

- In SmartDashboard:

  On the Mobile Access tab, go to the **Additional Settings > Network Accessories > Name Resolution** page.

- On the Mobile Access Security Gateway:

  For instructions, see the *R80.40 Gaia Administration Guide* - Chapter *Network Management* - Section *Hosts and DNS*.

# Configuring DNS Name Objects

**To create a new DNS Name object:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree click **Additional Settings > DNS Names**.
3. Click **New**.
4. Enter a **Name** for the DNS Name object.
5. Click **DNS Names**.
6. Click **Add**.
7. Type the DNS name.

8. Click **OK**.
9. Click **Save** and then close SmartDashboard.
10. In SmartConsole, install policy.

# 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 the "Mobile Access Applications" section.

# WebSockets

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

This feature is supported in R77.10 and above.

For WebSockets system requirements, see sk95311.

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

## Using WebSockets

**To use WebSockets support:**

Create a regular Web application to the WebSocket server.

- Make sure to include the port used for the WebSocket connection in the **Authorized Locations** of the Web application.
- The Web applications related to the WebSocket application must use **Path Translation** as their Link Translation method. It can be inherited from the Security Gateway setting or configured in the Web application.

# Monitoring WebSockets

**To monitor WebSocket connections:**

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Run:

   ```
   PingerAdmin report type ws
   ```

   Alternatively, to see all connections currently handled by the Pinger daemon (such as ActiveSync push), run:

   ```
   PingerAdmin report all
   ```

# Single Sign On

**Important** - In a Cluster, you must configure all the Cluster Members in the same way.

## Introduction to Single Sign On

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

## Supported SSO Authentication Protocol

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

- Basic Access - RFC enhancement. Not recommended because of security implications.
- Digest Access - RFC enhancement.
- Integrated Windows Authentication - RFC enhancement. Supports: NTLMv1, NTLMv2, and Kerberos.
- 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 opens:

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

### HTTP Based SSO Limitation

Single Sign On is not supported 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.

# Web Form Based SSO

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

The advantage of Web form based SSO authentication over HTTP authentication is that users are presented with the login page of the application itself, rather than a more obtrusive browser-specific page.

A typical Web form is shown below, for Outlook Web Access, together with a Mobile Access SSO popup that assists the user.

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

### Application Requirements for Easy Configuration

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

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

### Web Form Based SSO Limitations

Web form based SSO does not support:

- Password remediation forms.
- Forms that contain 'old/new/confirm' password fields. These fields are not recognized correctly, and wrong credentials might be recorded or forwarded.
- Forms that use Ajax requests instead of the usual 'ACTION' attribute for form submission.

### Configuring SSO Name Format

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

**Note** - This feature is for LDAP users who connect to the Mobile Access Portal. Internal users who connect to web applications though the portal with SSO authentication use a default of **$$user**.
For example, SSO can apply to both of these applications:

- Web application A that uses the format `domain\username`
- ActiveSync application B that uses the format `username@domain`

This feature is supported in R77.20 and higher. In R80.10 and higher you can configure it in SmartConsole.

**To configure the format of credentials required for an application:**

1. In SmartConsole, open a mobile application.
2. Select **Additional Settings** > **Single Sign-On**.
3. In the **Credential Formats** area, select an option.
4. Install Policy.

### Application and Client Support for SSO

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

| Mobile Access Application | Supports HTTP Based SSO | Supports Web Form Based SSO |
|---|---|---|
| Web applications | Yes | Yes |
| File shares | Yes | Not relevant |
| Citrix services | Yes | Yes |
| Web Mail | Simplified | No |
| Native applications | No | Not relevant |
| Mobile Mail | Yes | Not relevant |
| ActiveSync | Yes | Not relevant |

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 sk35080.

**Basic SSO configuration for a web application:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.
4. From the navigation tree click **Additional Settings > Single Sign On**.
5. Select **Turn on Single Sign On for this application**.
6. Configure the sign on method for the application. These are the default options:

   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.
7. Install the policy.

**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 analyzes the sign-in Web page of the application.

The default settings assume:

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

To configure Web Form SSO with default settings:

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

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

# SSO for Native Applications

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

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

### Configuring SSO for Native Applications

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

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

**Note** - When SSO is configured for a native application, it sends the end-user's password back to the client side.

Procedure:

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.
4. Select **Endpoint Applications** from the navigation tree of the object.
5. Select **Simple (Application is installed on the endpoint machine)** and enter information for these fields:
   - **Path and executable name** - Enter the path of the native application.
     For example for Remote Desktop Plus: `D:\rdp.exe`
   - **Parameters** - Enter this syntax for the username, password, and target remote host to connect to.
     For example: `/u:acme\$$user /p:$$password /v:192.0.2.2 /f`

     This setting defines how the Security Gateway sends the username and password of a locally logged-in user to the native application.
6. Install the policy.

### Upgrading the SSL Network Extender client to use SSO

Users must have an upgraded SSL Network Extender client on their computer to use SSO with native applications. To upgrade users' clients, make sure the **Client upgrade** setting is set to one of these:

- **Always upgrade** -Clients are upgraded automatically when users connect for the first time after the Security Gateway upgrade.
- **Ask user** -Users are prompted before installation starts. If you use this option, make sure to let users know that they must confirm the upgrade.

Upgraded SSL Network Extender clients can still connect to Security Gateways of earlier versions.

Procedure:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Additional Settings > VPN Clients**.
3. In **Advanced Settings for SSL Network Extender**, click **Edit**.

   The **SSL Network Extender - Advanced Settings** window opens.
4. In the **Deployment options** section, make sure that **Client upgrade upon connection** is configured for **Always upgrade** or **Ask user**.
5. Click **OK**.
6. Click **Save**
7. Close SmartDashboard.
8. Install the policy.

# Advanced Configuration of SSO

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

For configuration options that are specific to Web form SSO, see the "Single Sign On" section.

### 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.

1. Go to the **Single Sign On** page of the Mobile Access application.
2. For the **Advanced** options, click **Edit**.

These are the available single sign on methods.

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

### 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.

1. Go the **Single Sign On** page of the Mobile Access application.
2. In the **Login Settings** section, click **Edit**.

   The **Login Settings** window opens.
3. Fill in the fields according to the explanations below.

### Windows Domain

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

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

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

### User Notification

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

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

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

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

### Administrator Message

- **Show the following message together with the credentials prompt**

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

# Advanced Configuration of Web Form SSO

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

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

You can specify different criteria for:

- Sign In Success or Failure Detection
- Credential Handling

### Configuring Sign In Success or Failure Detection

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The Web Application window opens.
4. From the navigation tree, click **Additional Settings > Single Sign On**.
5. In the **Web Form** section, click **This application uses a Web form to accept credentials from users**.
6. Click **Edit**.
7. Click **Specify a criterion for success or failure** and then select one of these 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 this URL format:
     `<protocol>://<host>/[<path>][?< query>]`
8. Click **OK** and close the Web Application window.
9. Install the policy.

### Automatic 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.

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**.
3. Select **Automatically handle the credentials**.
4. Under **Sign in Web Form Detection Settings**, select:

   **Mobile Access regards the following URL as the sign in Web form:**

If the application presents a Web form that requires credentials, before the actual login form, so that Mobile Access is unable to automatically analyze the sign-in Web page, you can specify the URL of the actual login form.

Syntax:
`<protocol>://<host>/[<path>][?< query>]`

5. Under **Password Validation Settings**, select:

   **Mobile Access sends the following password:**

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

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

### Manual Credential Handling (Configuring HTTP Post Settings)

By default, Mobile Access looks for the user name and password fields at the application URL.

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

1. From the **Credentials Handling** window, select **Manually specify how to handle the credentials**.
2. Fill in the fields for **When the following sign in URL is requested**:
   - **post to the following URL**

     In this and the previous field, the URL must be absolute. Use the URL format

     `<protocol>://<host>/[<path>][?< query>]`
   - **the following POST data**, which must include:
     - `$USERNAME` resolves to the user name stored on Mobile Access.
     - `$PASSWORD` resolves to the password stored on Mobile Access.
     - `$DETAILS` resolves to the Windows domain stored on Mobile Access

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

# Kerberos Authentication Support

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

- Kerberos Authentication is supported for Web Applications (HTTP and HTTPS). Mobile Access can authorize against Kerberos servers on behalf of users.
- Microsoft IIS and other web servers employ Kerberos using the *Negotiate* method in HTTP authentication headers.
- Kerberos is sensitive to time differences between the Security Gateway and Domain Controller.

  Make sure clocks on the Mobile Access Security 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.
- By default, NTLM authentication is preferred as the authentication method over Kerberos authentication.

  To prefer Kerberos over NTLM, follow the instructions in sk106848.

**To use Kerberos with Mobile Access:**

- If Microsoft Active Directory is configured, the Security Gateway automatically updates with the relevant settings from the AD Account Unit and Kerberos enabled.

  You can review the Kerberos settings in the `$CVPNDIR/var/krb5.auto.conf` file.

  **Warning** - Do not edit the `krb5.auto.conf` file manually.

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

  The template is used to create the `krb5.auto.conf` file.

  To edit `krb5.auto.conf.template` file:

  1. Edit the `$CVPNDIR/var/krb5.auto.conf.template` file and add your changes.

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

     **Important** - Do **not** change the place holder names.

2. On the Security Gateway, run:

   ```
   cvpnd_admin policy
   ```

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

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

   Example of how it looks in the file `krb5.auto.conf`:

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

- If Microsoft Active Directory is not yet configured for Mobile Access, but you want to use it:
  1. Use the Mobile Access wizard to configure your AD.
  2. Edit the SmartDashboard Network Objects for the AD server and for the Single Sign On.
- If you do not want to use Microsoft Active Directory, manually configure Kerberos for your Single Sign On.

# Configuring Microsoft Active Directory for Mobile Access

These steps assume you defined the Microsoft AD server as a Check Point LDAP Account Unit object. If that object does not exist, create one: **Objects > New > More > Server > LDAP Account Unit**.

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

1. In the SmartConsole, go to **Objects > Servers > LDAP Account Units**.
2. Right-click the LDAP AD server and select **Edit**.

   In the **General** tab of the **LDAP Account Unit Properties** window, the value of **Profile** is **Microsoft_AD**.
3. Make sure the value of **Domain** is correct for the AD Domain.
4. Click **OK**.
5. Publish the SmartConsole session.

**To configure Microsoft Active Directory server priorities:**

1. Open the object for the Security Gateway with Mobile Access enabled.

   If there is more than one, do these steps for each.
2. Open **Other** > **User Directory**.

   By default, the Security Gateways use all Domain Controllers of the AD. If there is a connectivity issues (no or poor connectivity) from a Security Gateway to a Domain Controller, adjust the priorities.
3. Make sure that **Selected Account Units List** is selected.

   When this is selected, the **Selected AUs** list is available. If the list is empty, click **Add** to add an **LDAP Account Unit** defined for **Microsoft_AD**.
4. Select the Microsoft AD server.

   The **Servers priorities for selected AU** is available.
5. Clear **Use default priorities**.
6. Select a host of the AD server.

   The **Priority** field is available.
7. Set the priority of the host with connectivity issues to be lower than a different host.

   For example: Priority **1** is highest. Priority **5** is lower.
8. Click **Set**.
9. Click **OK**.

# Manual Configuration for Kerberos

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

1. Create the `$CVPNDIR/var/krb5.manual.conf` file.
2. Populate the `krb5.manual.conf` file with values that specify your domain addresses and domain controllers.

   Use this format:

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

   In the file:

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

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

**Important** - If you specify multiple domain addresses (realms) and domain controllers in the `krb5.manual.conf` file, you must also add them to the Mobile Access configuration in the `$CVPNDIR/conf/cvpnd.C` file.

To add them, use these `cvpnd_settings` commands:

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

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

1. Test the manual configuration:
   a. Set `KRB5_CONFIG` as an environment variable in the shell to point to the relevant configuration file:
      - In the Expert mode (Bash shell), run:

        ```
        export KRB5_CONFIG=$CVPNDIR/var/krb5.manual.conf
        ```

      - In the Tcsh or Csh shell, run:

        ```
        setenv KRB5_CONFIG $CVPNDIR/var/krb5.manual.conf
        ```

   b. From the Mobile Access Security Gateway command line, run in the Expert mode (Tcsh, or Csh):

      ```
      kinit your-ad-username
      ```

      - If there are several realms, the `kinit` syntax applies to the default realm.
      - For other realms, use the syntax:

        ```
        kinit your-ad-username@YOUR.OTHER.AD.NAME
        ```

      You should get a prompt similar to:

      ```
      Password for your-ad-username@YOUR.DOMAIN:
      ```

   c. Enter the password.
   d. Run:

      ```
      klist
      ```

      The `Ticket cache` list shows one ticket.

   e. Delete the list by running:

      ```
      kdestroy.
      ```

2. Open `$CVPNDIR/conf/cvpnd.C` for editing.
3. Change the value of the `kerberosConfigMode` attribute from `auto` to `manual`.

   Alternatively, run:

   ```
   cvpnd_settings $CVPNDIR/conf/cvpnd.C set kerberosConfigMode
   manual
   ```

   **Note** - If you assign the value `none` to `kerberosConfigMode`, it disables Kerberos SSO.

4. Run:

   ```
   cvpnrestart
   ```

# Kerberos Constrained Delegation

Kerberos constrained delegation is a Single Sign-On method that uses Kerberos authentication for users to access internal resources without the need to enter a password.

It is supported for the Mobile Access Portal and Capsule Workspace.

### To enable Kerberos constrained delegation:

1. On the Mobile Access Security Gateway, run:

   ```
   cvpnd_settings $CVPNDIR/conf/cvpnd_internal_settings.C set
   EnableKCD true
   ```

2. Run:

   ```
   cvpnrestart
   ```

3. In a cluster environment, repeat the steps on all cluster members.

### Configuring Kerberos Constrained Delegation

Before you begin, make sure:

- That your site supports Kerberos authentication.
- The Mobile Access Security Gateway is configured to support Kerberos. .
- The date and time on the Security Gateway and Active Directory server are the same.
- You must use FQDN and not an IP address with your internal server name. Make sure that the FQDN resolves both on the Security Gateway and on the Kerberos server.

The configuration includes:

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

### Configuring a Delegate User on the AD Server

A delegate user can have specified permissions without being part of a higher privileged group.

For Kerberos Constrained Delegation, the delegate user can allow access to other users for specified services.

1. Add a new user to the AD server.
2. Open the command prompt on the AD server and run the command:

   `setspn -A HTTP/<user name> <domain name>\<user name>`

   - `<user name>` - The user name for the user that was created.
   - `<domain name>` - The domain name that the created user belongs to.
3. From the **Users and Computers** tree, right-click the user to open the **User Properties** of the new user.
4. Click the **Delegation** tab.
5. Select: **Trust this user for delegation to specified services only**.
6. Select: **Use any authentication protocol**.
7. In the **Services to which this account can present delegated credentials** table, click **Add** to add http on the server that the user is allowed to access.
8. Click **OK**.

### Configuring Kerberos Constrained Delegation Support

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

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application for which you want to configure Kerberos Constrained Delegation.

   The Web Application window opens.
4. From the navigation tree click **Additional Settings > Single Sign On**.
5. Configure these settings:
   - Select **Turn on Single Sign On for this application**
   - Select **Advanced**
6. Click **Edit**.
7. In the **Advanced** window, select **This application reuses the portal credentials. Users are not prompted**.
8. Click **OK** and close the Web Application window.
9. Install the policy.

**Troubleshooting issues with Kerberos Constrained Delegation:**

1. Connect to the command line on the Mobile Access Security Gateway.
2. Make sure that the value of **EnableKCD** in `$CVPNDIR/conf/cvpnd_internal_settings.C` is **true**.
3. Run the `cvpnrestart` command.
4. See if there is a **Kerberos Constrained Delegation failure** entry in the Mobile Access logs in SmartLog.
5. Make sure that the account unit credentials have delegate privileges.
6. Make sure that the date and time of the Security Gateway and Active Directory server are synchronized.
7. Make sure that the DNS server is configured correctly and the Security Gateway can resolve the web application host name and the Active Directory server.

# Certificate Attribute Forwarding

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

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

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

| To: | Parameter=Value in the `$CVPNDIR/conf/cvpnd.C` |
|---|---|
| Enable | `:EnableCertHeadersForwarding (true)` |
| Disable | `:EnableCertHeadersForwarding (false)` |

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

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

| To forward: | Parameter=value in the `$CVPNDIR/conf/cvpnd.C` |
|---|---|
| Complete certificate, encoded in base 64 | "*<header_name>*: *<Certficate in Base64>*" |

| To forward: | Parameter=value in the `$CVPNDIR/conf/cvpnd.C` |
|---|---|
| Certificate Issuer DN | "*<header_name>* : *<DN of Certficate Issuer>*" |
| Serial number of the certificate | "*<header_name>* : *<Certficate Serial>*" |
| Subject DN | "*<header_name>* : *<DN of Certficate Subject>*" |
| Alternative subject DN | "*<header_name>* : *<DN of Certficate Alternative Subject>*" |
| Valid start date, before which the certificate cannot be used | "*<header_name>* : *<Certficate Validity Start Date>*" |
| Certificate expiration date | "*<header_name>* : *<Certficate Validity End Date>*" |

**Example:**

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

```
:EnableCertHeadersForwarding (true)
:CertHeaders (
    : ("X-Cert-IssuerDN : <DN of the Certificate Issuer>"
)
```

# Exchange Mail Applications for Smartphones and Tablets

## Introduction to Exchange Mail Applications

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

## Mobile Mail Applications

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

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

### Configuring Mobile Mail Applications

**To create and configure a new Mobile Mail application:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > Business Mail**.

   The **Mobile Mail Application** window opens.
3. In the **General Properties** page:
   - Enter a **Name** for the application in SmartDashboard
   - Enter the name of the **Exchange Server** that communicates with the Security Gateway and the **Port**. For example, **ad.example.com**
4. In the **Exchange Access** page, in the **Define access settings** area:
   - **Use encryption (https)** - By default, traffic to the Exchange server works with HTTPS.

- **Use non-default path** - If the Exchange Web Services path on the Exchange server to the application is not the default, enter the path here.

  The default path is `EWS/Exchange.asmx` and the URL is `https://<IP address of the Exchange Server>/EWS/Exchange.asmx`

- **Use specific domain** - If you want users to authenticate to a specified domain on the Exchange server, enter it here.

5. In the **Exchange Access** page, in the **Proxy Settings** area, if there is a proxy server between the Exchange Server and the Security Gateway, configure these settings:

   - **Use gateway proxy settings** - By default the proxy settings configured for the Security Gateway are used.
   - **Do not use proxy server** - Select if no proxy server is required.
   - **Use specific proxy server** - Configure a proxy server that the Security Gateway communicates with to reach the Exchange Server.

   a. Select the **Host** and **Service**.

   b. If credentials are required to access the proxy server, select **Use credentials for accessing the proxy server** and enter the **Username** and **Password**.

6. In the **Display Link** page:

   - **Title** - The name of the application that users will see on their mobile devices.
   - **Description** - The description of the application that users will see on their mobile devices.

7. In the **Single Sign On** page, select the source of the credentials used for Single Sign-On for this application:

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

8. In the **Periodic Test** page, select which tests are run regularly on the Security Gateways to make sure they can connect to the Exchange server. If there is a connectivity problem, a System Alert log generated.

- **Run periodic test from gateways that have access to this application** - A test makes sure there is connectivity between the Security Gateway and Exchange server. The test runs at the interval that you enter.
- **Perform extensive test using the following account** - Periodically run a test to make sure that a user can authenticate to the Exchange server. To run this test you must enter a valid **Username** and **Password**.

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

9. Click **OK**.
10. Install the policy.

# ActiveSync Applications

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

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

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

## Configuring ActiveSync Applications

**To create a new ActiveSync application:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New Custom Application/Site > Mobile Application > ActiveSync Application**.

   The ActiveSync Application window opens.

**To configure an ActiveSync application:**

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.

   The **ActiveSync Application** window opens.
4. In the **General Properties** page:

- Enter a **Name** for the application in SmartDashboard
- Enter the name of the **Exchange Server** that will communicate with the Security Gateway and the **Port**. For example, **ad. example.com**

5. In the **Exchange Access** page, in the **Define access settings** area:
   - **Use encryption (https)** - By default, traffic to the Exchange server works with HTTPS.
   - **Use non-default path** - If the ActiveSync path on the Exchange server to the application is not the default, enter the path here.
   - **Use specific domain** - If you want users to authenticate to a specified domain on the Exchange server, enter it here.
6. In the **Exchange Access** page, in the **Proxy Settings** area, if there is a proxy server between the Exchange Server and the Security Gateway, configure the settings here.
   - **Use gateway proxy settings** - By default the proxy settings configured for the Security Gateway are used.
   - **Do not use proxy server** - Select if no proxy server is required.
   - **Use specific proxy server** - Configure a proxy server that the Security Gateway communicates with to reach the Exchange Server.

   a. Select the **Host** and **Service**.

   b. If credentials are required to access the proxy server, select **Use credentials for accessing the proxy server** and enter the **Username** and **Password**.
7. In the **Display Link** page:
   - **Title** - The name of the application that users will see on their mobile devices.
   - **Description** - The description of the application that users will see on their mobile devices.
8. In the **Periodic Test** page, select which tests are run regularly on the Security Gateways to make sure they can connect to the Exchange server. If there is a connectivity problem, a System Alert log generated.
   - **Run periodic test from gateways that have access to this application** - A test makes sure there is connectivity between the Security Gateway and Exchange server. The test runs at the interval that you enter.
   - **Perform extensive test using the following account** - Periodically run a test to make sure that a user can authenticate to the Exchange server. To run this test you must enter a valid **Username** and **Password**.

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

10. Install the policy.

# Configuring a TLS/SSL Version for an Application

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

Configure the feature for each application in Database Tool (GuiDBEdit Tool) (see sk13009).

**To configure an SSL version for an application:**

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with Database Tool (GuiDBEdit Tool) to the Management Server.
3. Go to **Other** > **network_applications** > **APPLICATION NAME** > **internal_resource_ssl_version**.
4. Select a version. The options are:
   - auto (default) - Uses the version that the organizational server recommends
   - SSLv3 (SSL 3.0)
   - TLSv1 (TLS 1.0)
   - TLSv1.1 (TLS 1.1)
   - TLSv1.2 (TLS 1.2)
5. Save the changes and close Database Tool (GuiDBEdit Tool).
6. Connect with SmartConsole to the Management Server.
7. Install policy.

# Policy Requirements for ActiveSync Applications

- To access ActiveSync, users must belong to a user group that is allowed to access ActiveSync applications.
- Each user must have an email address defined the **Email Address** field in the properties of an internal user object, or on an LDAP server (for LDAP users).

- If users are internal, their Check Point client passwords must be the same as their Exchange passwords, otherwise ActiveSync will not work.

# Mobile Access for Smartphones and Tablets

## Overview of Mobile Access for Smartphones and Tablets

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

- For email, calendar, and contact access, configure Mobile Mail or ActiveSync applications.

  This can be done automatically in the Mobile Access Wizard.

- Configure Web applications, if necessary.
- Make sure users have the information and credentials required to authenticate to the Security Gateway.

  For client certificates, use the Certificate Creation and Distribution Wizard (see the "Creating Client Certificates" section).

- Make sure users' Mobile Settings meet your organization's needs (see the "Managing Mobile Settings" section).
- Tell users which App to install.
- Make sure smartphone and tablet users are included in your Mobile Access Policy.

## Certificate Authentication for Handheld Devices

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

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

# Managing Client Certificates

Check Point Mobile Apps for mobile devices can use certificate-only authentication or two-factor authentication with client certificates and username/password. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.

Manage client certificates in **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**..

The page has two panes.

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

# Creating Client Certificates

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

**To create and distribute certificates with the client certificate wizard**

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. In the **Client Certificates** pane, click **New**.

   The **Certificate Creation and Distribution** wizard opens.
3. In the **Certificate Distribution** page, select how to distribute the enrollment keys to users. You can select one or both options.

a. **Send an email containing the enrollment keys using the selected email template** -Each user gets an email, based on the template you choose, that contains an enrollment key.

- **Template** - Select the email template that is used.
- **Site** - Select the Security Gateway, to which users connect.
- **Mail Server** - Select the mail server that sends the emails.

You can click **Edit** to view and change its details.

b. **Generate a file that contains all of the enrollment keys** - Generate a file for your records that contains a list of all users and their enrollment keys.

4. **Optional:** To change the expiration date of the enrollment key, edit the number of days in **Users must enroll within x days**.
5. **Optional:** Add a comment that will show next to the certificate in the certificate list on the **Client Certificates** page.
6. Click **Next**.

   The **Users** page opens.
7. Click **Add** to add the users or groups that require certificates.
   - Type text in the search field to search for a user or group.
   - Select a type of group to narrow your search.
8. When all included users or groups show in the list, click **Generate** to create the certificates and send the emails.
9. If more than 10 certificates are being generated, click **Yes** to confirm that you want to continue.

   A progress window shows. If errors occur, an error report opens.
10. Click **Finish**.
11. Click **Save**.
12. In SmartConsole, install the Policy.

# Revoking Certificates

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

**To revoke one or more certificates**

1. Select the certificate or certificates from the **Client Certificate** list.
2. Click **Revoke**.
3. Click **OK**.

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

# Creating Templates for Certificate Distribution

**To create or edit an email template**

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. To create a new template: In the **Email Templates for Certificate Distribution** pane, select **New**.

   To edit a template: In the **Email Templates for Certificate Distribution** pane, double-click a template.

   The **Email Template** opens.
3. Enter a **Name** for the template.
4. **Optional:** Enter a **Comment**. Comments show in the Mail Template list on the **Client Certificates** page.
5. **Optional:** Click **Languages** to change the language of the email.
6. Enter a **Subject** for the email. Click **Insert Field** to add a predefined field, such as a Username.
7. In the message body add and format text. Click **Insert Field** to add a predefined field, such as Username, Registration Key, or Expiration Date.
8. Click inside the E-mail Template body.
9. Click **Insert Link** and select the type of link to add (link or QR code).

- **Site and Certificate Creation**

  For users who already have a Check Point app installed.

  When users scan the QR code or go to the link, it creates the site and registers the certificate.

  Select the client type that will connect to the site- Select one client type that users will have installed:

  - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
  - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.

- **Download Application**

  Direct users to download a Check Point App for their mobile devices.

  Select the client device operating system:

  - **iOS**
  - **Android**

  Select the client type that will connect to the site- Select one client type that users will have installed:

  - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
  - **Capsule Connect/VPN** - A full Layer 3 tunnel app that gives users network access to all mobile applications.

- **Custom URL**

  Lets you configure your own URL.

**For each link type, you can select which elements are added to the mail template**

- **Link URL** - Enter the full link address.
- **QR Code** - When enabled, users scan the code with their mobile devices.
- **HTML Link** - When enabled, users tap the link on their mobile devices.

  You can select both **QR Code** and **HTML Link** to include both in the email.
- **Display Text** - Enter the text for the link title.

10. Click **OK**.
11. **Optional:** Click **Preview in Browser** to see a preview of how the email will look.
12. Click **OK**.
13. Publish the changes

# Cloning a Template

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

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

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

# Remote Wipe

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

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

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

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

Remote Wipe send logs:

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

This feature is supported in R77.10 and above.

**To configure Remote Wipe**

1. Run the command on the Security Gateway.

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

- To enable or disable Remote Wipe:

  ```
  [Expert@HostName:0]# cvpnd_settings $CVPNDIR/conf/cvpnd.C
  set RemoteWipeEnabled {true|false}
  ```

  Remote Wipe is enabled by default.

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

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

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

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

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

2. Run:

   ```
   [Expert@HostName:0]# cvpnrestart
   ```

   You must restart the cvpn service to apply the changes.

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

**To trigger Remote Wipe on a device**

1. Make sure that the `cvpnd.C` file is configured for Remote Wipe and, if you want, for Push Notifications.

   If you change the file, run: `[Expert@HostName:0]# cvpnrestart`

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

**To see Remote Wipe logs**

1. Open SmartLog.
2. Query for:

```
"Remote Wipe" AND blade:"Mobile Access" action:"Failed Log In".
```

You can filter these results for user DN, device ID, or certificate serial number.

# Managing Mobile Settings

For Capsule Workspace, many settings that affect the user experience on mobile devices come from the **Mobile Profile**.

Each Mobile Access user group has an assigned Mobile Profile. By default, all users get the Default Profile.

The settings in the Mobile Profile include:

- Passcode Settings
- Mail, Calendar, and Contacts availability
- Settings for offline content
- Where contacts come from

Manage the Mobile Profiles in **Mobile Access** tab > **Capsule Workspace Settings**.

- In the **Mobile Profiles** pane:
  - See all Mobile Profiles.
  - Create, edit, delete, clone, and rename Mobile Profiles.
- In the **Mobile Profile Policy** pane:
  - Create rules to assign Mobile Profiles to user groups.
  - Search for a user or group within the policy rules.

## Creating and Editing Mobile Profiles

**To create or edit a Mobile Profile**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Capsule Workspace**.
3. **Optional:** Create a new Mobile Profile, click **New**.
4. In the **Mobile Profiles** pane select the profile and click **Edit**.

5. Change settings. See the *Capsule Workspace Settings in the Mobile Profile* section below.
6. Click **Save** and then close SmartDashboard.
7. In SmartConsole, install the policy.

# Capsule Workspace Settings in the Mobile Profile

**Instructions**

1. In the **Access Settings** area, configure:
   - **Session timeout** - After users authenticate with the authentication method configured in **Gateway Properties** > **Mobile Access** > **Authentication**, configure how long they stay authenticated to the Security Gateway.
   - **Activate Passcode lock** - Select to protect the Business Secure Container area of the mobile device with a passcode.
     - **Passcode profile** - Select a passcode profile to use. The profile includes the passcode complexity, length, expiration, and number of failed attempts allowed.
     - **Allow storing user credentials on the device for single-sign on** - If username and password authentication is used, store the authentication credentials on the device. Then users are only prompted for their passcode not also for their username and password.
   - **Report jail-broken devices** - Create a log if a jail-broken device connects to the Security Gateway.
     - **Block access from jail-broken devices** - Block devices that are jail-broken from connecting to the Security Gateway.
   - **Track user's GPS location** (upon user's approval) - Tracks devices connecting to the Security Gateway.
2. In the **Allowed Items** area, select which Exchange features are available on devices:
   - **Mail**
   - **Calendar**
   - **Contacts**
   - **Notes** (iOS only)
3. In the **Offline Content** area, configure what data is saved and for how long when the Check Point App cannot reach the Security Gateway.

- **Mail from the last x days** - Select the length of time from which emails are saved.
  - **Cache Mail** - Select which parts of the email are saved in the offline cache.
- **Calendar from the last x months and the following x months** - Select which parts of the calendar are saved: the length of time in the past and length of time in the future.
  - **Cache Calendar** - Select which parts of the calendar entry are saved in the offline cache.
- **Synchronize contacts** - Synchronize contacts so they are available offline.

4. In the **Push Notifications** area, select if you allow push notifications on devices and which notification templates to use.

   See the *Push Notifications* section below for details.

   To use this, push notifications must be enabled for Capsule Workspace on the Security Gateway that users connect to.

5. In the **Mail** area, select **Allow copy paste of mail content** if you allow contents of emails to be pasted into other apps.
6. In the **Calendar** area, select **Allow business calendar to sync to the device's native calendar** if you want to sync both calendars on the device. Events from Capsule Workspace will show in the device's calendar, outside of Capsule Workspace.
7. In the **Contacts** area, select which additional contacts to show on the device:
   - **Global Address List**
   - **Local Phone**
8. In the **Check Point Capsule Docs** area, select the Capsule Docs information that is stored in Capsule Workspace:
   - **Allow caching Check Point Capsule Docs credentials** - The credentials are required to open Capsule Docs protected documents are cached on the device. If they are not cached, users must enter their credentials each time they open a document for the first time.
   - **Allow caching Check Point Capsule Docs keys** - The Capsule Docs keys are cached on the device. If they are cached users can open a previously opened document with no need to enter credentials.

# Managing Passcode Profiles

A passcode lock protects Capsule Workspace in mobile devices. In each Mobile Profile, configure which Passcode Profile it uses. The profile includes the passcode requirements, expiration, and number of failed attempts allowed. The default passcode profiles are Normal, Permissive, and Restrictive. You can edit the default profiles and create new profiles.

### To manage Passcode Profiles

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Additional Settings > Passcode Profile**.
3. To create a new Passcode Profile, click **New**.
4. Configure the settings for the profile.
5. Click **Save**
6. Close SmartDashboard.
7. Publish the SmartConsole session.

### Passcode Profile Settings

A Passcode Profile includes these settings:

- **Passcode Requirements** - The complexity requirements. When you configure this, remember that users usually have a small on-screen keyboard.
  - **Simple Passcode (4 digits)** - Users create a simple password of 4 numbers.
  - **Custom passcode strength** - Select from the requirements below.
    - **Minimum passcode length** - Enter the minimum number of characters.
    - **Require alphanumeric characters** - Show an alphanumeric keyboard and require at least one character to be a letter.
    - **Minimum complex characters** - Enter the number of characters that must be a special character.
- **Force passcode expiration** - Enter the number of days after which user's passcodes expires and must be replaced.
- **Allow grace period for entering passcode** - Select to let users access the Business Secure Container for a specified period of time without re- entering their passcode. Enter the quantity of time in minutes.

- **Exit after a few failures in passcode verification** - Select to lock users out after a specified number of failed attempts. After the failed attempts, users must re-authenticate. If the authentication method includes username and password, users must enter them. If the authentication is certificate-only, users need a new certificate.
- **Enforce passcode history** - When selected, users cannot use a passcode that is the same as earlier passcodes. Select the number of earlier passcodes that users cannot use.

# Push Notifications

This feature sends push notifications for incoming emails and meeting requests on handheld devices, while the Mobile Mail app is in the background. The app icon shows the number of new, unhandled notifications. One user can get notifications for multiple devices.

Push notifications are disabled by default, but enabled when you run the Mobile Access First Time Wizard.

To use push notifications, the Security Gateway must have connectivity to these URLs on ports 443 and 80:

- https://push.checkpoint.com (209.87.211.173 and 217.68.8.71)
- http://SVRSecure-G3-crl.verisign.com/SVRSecureG3.crl
- http://crl.verisign.com/pca3-g5.crl

**Notes:**

- Users must enable notifications for the Mobile Mail app on iOS devices
- Push notifications can increase Exchange server CPU usage if many users are connected
- The Exchange server must have access to the Mobile Access Portal.
- If you change the URL or IP address of the Mobile Access Portal after you enable push notifications, you must update the Push Portal attributes with Database Tool (GuiDBEdit Tool):
  1. In Database Tool (GuiDBEdit Tool) (see sk13009), go to the **Portals** section of your Security Gateway > **portal_name** > **ExchangeRegistration**.
  2. Change **main_url** and **ip_address** to match the URL of the Mobile Access Portal.
  3. Save the changes and close Database Tool (GuiDBEdit Tool).
  4. In SmartDashboard, install policy on the Security Gateway.

# Configuring Push Notifications

**To enable push notifications**

Enable push notifications from the Mobile Access Wizard or from the Security Gateway Properties of each Security Gateway.

- From the Mobile Access Wizard:
  - If you enable Mobile Mail in the Mobile Access Wizard, push notifications are automatically enabled for the Security Gateway.
  - If you enable Mobile Mail from the Mobile Access tab, push notifications are NOT enabled.
- From the Security Gateway Properties:
  1. Open a Security Gateway object that has Mobile Access enabled.
  2. Select **Mobile Access** > **Capsule Workspace** from the tree.
  3. Select **Enable Push Notifications**.
  4. Click **OK**.

# Customizing Push Notifications

Customize push notifications from the mobile profile in the **Mobile Access** tab > **Capsule Workspace Settings**.

You can customize templates for Mail and Meeting notifications.

**To see the default notifications or change the notifications**

1. From SmartDashboard > **Mobile Access** tab > **Capsule Workspace Settings**, open a **Mobile Profile**.
2. Under **Push Notifications**, click **Manage**.

# Exchange Server and Security Gateway Communication

Make sure that the Exchange server can access the Mobile Access Portal.

On R77.20 and higher Security Gateways, all confidential information between the Exchange server and the Security Gateway uses encrypted SSL tunnels. Non-confidential information can use unencrypted HTTP connections.

You can configure all push notification communication to use SSL tunnels.

By default, Kerberos authentication is not enabled for Push Notification registration to the Exchange server. To enable it, follow the instructions in sk110629.

**To force all push notification communication to go through SSL tunnels**

1. Install a trusted server certificate on the Mobile Access Security Gateway. See sk98203.
2. Close all SmartConsole windows connected to the Management Server.
3. Connect with Database Tool (GuiDBEdit Tool) (sk13009) to the Management Server.
4. Search for the field **main_url** (Ctrl +F).
5. Press F3 to see next **main_url** until you find **main_url** that contains the value **ExchangeRegistration**.
6. Double-click the **ExchangeRegistration main_url** field and edit the value to be **https://** and not **http://**.
7. Save the changes and close Database Tool (GuiDBEdit Tool).
8. Connect with SmartConsole to the Management Server.
9. Open the Mobile Access Security Gateway object.
10. Click **OK**.
11. Install policy.

On Security Gateways R77.10, if the certificate on the Security Gateway is not trusted, import the certificate to the Exchange Server. This is not necessary on Security Gateways R77.20 and higher. For details about how to get the Security Gateway certificate, see sk98203.

**To import a certificate to the Exchange server**

1. Download the certificate to the Exchange server.
2. Double-click the certificate file, and follow the Windows certificate installation wizard steps.
3. Run the **Microsoft Management Console**.
4. In the window that opens, click **File > Add/Remove Snap-in**.

   **Add or Remove Snap-ins** window opens.
5. Select **Certificates** from the Available snap-ins, and click **Add**.
6. Select **My user account**.
7. Click **Finish**.
8. Select **Certificates** and click **Add** again.
9. Select **Computer account**.
10. Click **Next**.

11. Click **Finish**.
12. Click **OK**.

    The certificate is stored in **Local computer** and in **Current user** stores.

# Push Notification Status Utility

Use the *Push Notification Status Utility* to understand if your environment is configured correctly for push notifications.

### Intructions

Run the `$CVPNDIR/bin/PushReport` command to generate a report that contains this data:

1. **License** - Shows if the license is valid or if you have an evaluation license.
2. **Configuration** - Shows if push notifications are configured and enabled in the database.
3. **Connectivity** - Shows if you have a connection to the Check Point Cloud and CRLs list.
4. **Callback URL** - Shows the configured callback URL. If it is an https URL, the utility shows that a certificate is needed.

### Output Example

```
[admin@gw-105 bin]# PushReport
This is your configuration status:
==================================
Topic               Status              Description
-------------------------------------------------------------
-------------
License             OK                  You are not using an
evaluation license
Configuration       OK                  Push is enabled in
configuation
Connectivity        OK                  You have connectivity to
cloud
Callback URL        OK                  Your callback push url
is: http://198.51.100.2/ExchangeRegistration. Make sure you have
internal connectivity to this URL.
```

## Monitoring Push Notification Usage

Use the *"fwpush" on page 273* commands to monitor, debug, and troubleshoot push notification activity.

**Note** - Users must first install the latest version of the Capsule Workspace app from the app store and connect to the site created on the Security Gateway.

To see failed batches, expired push notifications, and delayed push notifications, see:
`$FWDIR/log/pushd_failed_posts`

**Legal disclaimer on product functionality**

Check Point uses Apple and Google services to deliver push notifications to iOS and Android devices. This is consistent with industry practice and similar to other applications vendors. Accordingly, Check Point assumes no liability in the event a notification is not sent or is not successfully pushed.

Information which is sent as a push notification passes through Check Point's push service and the Apple or Google push service (according to the user's device). Check Point does not keep, filter, or read any information that passes through. Check Point may review basic information to determine if a push notification reached its destination.

Check Point provides configuration options for the information sent as a push notification. The administrator can choose whether to set the subject, the sender, or the importance of any email, and can send the meeting location for meeting invitations.

Check Point will not be held liable for any loss of information that may result during the push notification process.

# ESOD Bypass for Mobile Apps

Hand-held devices cannot run Endpoint Security on Demand (ESOD) components. By default, ESOD is disabled for smartphones and tablets.

If your organization has ESOD enabled, mobile apps cannot access ESOD enforced applications.

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

**To change the ESOD setting on the Security Gateway**

1. On the Security Gateway run:

   ```
   cvpnd_settings $CVPNDIR/conf/cvpnd.C set
   MobileAppBypassESODforApps "true"
   ```

   or

```
cvpnd_settings $CVPNDIR/conf/cvpnd.C set
MobileAppBypassESODforApps "false"
```

- **true** - Bypasses ESOD for mobile apps (default).
- **false** - Does not bypass ESOD.

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

# MDM Cooperative Enforcement

Support for Mobile Device Management (MDM) through third-party vendors enforces a unified security policy for devices that access internal resources. Only managed devices that comply with the organizational security policy can successfully connect and access your business resources.

This feature is supported in R77.10 and above.

Check Point Apps establish a secure VPN connection to the corporate network through a Check Point Security Gateway. The Security Gateway queries the policy of the MDM server. The MDM server verifies the compliance level of employees' mobile devices when the VPN connection is established. The Security Gateway uses the MDM results to allow or block access, according to the device security and the user's permissions.

This feature is supported by Check Point Capsule Connect and Capsule Workspace clients.

For the most updated vendor information see sk98201.

To configure MDM Cooperative Enforcement with iOS 7, see sk98447.

**Overview of the MDM Enforcement workflow**

1. Before you start you must have:
   - An MDM account set up with required vendor license, if necessary
   - Necessary licenses for Capsule Connect or Capsule Workspace
   - Users with supported iOS or Android devices
2. Configure MDM on the Mobile Access Security Gateway. Edit the global options and vendor options.
3. For iOS 7 only: Configure settings and policy for your MDM vendor. See sk98447.
4. Make sure that the MDM functionality works - from a mobile device or Security Gateway console.

# Configuring MDM on the Security Gateway

Enable MDM Enforcement in a configuration file on the Security Gateway. Then define global options and vendor-specific options.

**To configure Mobile Device Management on a Security Gateway**

1. Connect to the command line ine the Security Gateway.
2. Log in to the Expert mode mode.
3. Edit the `$FWDIR/conf/mdm.conf` file.
4. Edit the global options.

   **Description**

   MDM is disabled by default. You must change the value of the `enabled` parameter to `1`.

| mdm.conf Options | Description |
|---|---|
| `enabled` | `0` - MDM disabled<br>`1` - MDM enabled |
| `monitor_only` | `0` - Full enforcement: non-compliant mobile devices cannot log in.<br>`1` - Monitor only: non-compliant devices can log in and attempts are logged. |
| `fail_open` | Defines behavior for cases of uncertainty, when an error occurs while checking MDM status.<br>`0` - Drop VPN connections when an error occurs while checking MDM compliance status.<br>`1` - Allow VPN connections when an error occurs while checking MDM compliance status. |
| `session_timeout_in_sec` | Maximum seconds allowed to determine device compliance status between the Security Gateway and the MDM cloud service.<br>Starts at device login. If passed, the action of `fail_open` starts.<br>Recommended: keep default. |

| mdm.conf Options | Description |
|---|---|
| `active_ vendor` | Name of active third-party vendor, to test MDM compliance.<br>You can configure multiple MDM vendors, but only one can be active.<br>See the *Advanced Vendor Support* section below. |
| `password_ is_ obscured` | `0` - `password` parameters in **mdm.conf** show in clear text.<br>`1` - `password` parameters in **mdm.conf** show strings.<br>Recommended: keep default (1).<br>If the global property **password_is_obscured** is enabled, you cn obscure all parameters named `password` in the **Vendor Configuration** blocks.<br><br>**To get an obscured password string from your password:**<br>a. Run in the Expert mode:<br>`# obfuscate_password <Your Expert mode Password>`<br>The output is a string. For example:<br>`33542b323a3528343640`<br>b. Copy the string to the **mdm.conf file**, as the `password` value.<br>c. Save the file.<br>d. Install policy. |
| `verify_ ssl_cert` | `0` - SSL certificates not verified when Security Gateway accesses MDM cloud services.<br>`1` - SSL certificates verified. Prevents some DNS poisoning, spoofing, man-in-the-middle attacks against Security Gateway.<br>Recommended: keep default (1). If the MDM server is in a cloud, this parameter must be `1`.<br>If you change it, the devices will be vulnerable to MITM attacks. (This risk is lower if the MDM server is local.) |
| `ssl_ca_ bundle_ path` | Local path on Security Gateway of known CA certificate files.<br>You can add more certificates to those that come with installation.<br>Recommended: keep default. |
| `ssl_ cipher_ list` | Allowed ciphers for HTTPS between Security Gateway and MDM cloud services.<br>Recommended: keep default. |

| mdm.conf Options | Description |
|---|---|
| `ssl_use_tls_v1` | To use TLSv1 or SSL for HTTPS between Security Gateway and MDM cloud services.<br>Recommended: keep default. |

5. Edit the vendor options.

   **Description**

   You can add more, if you have an understanding of the vendor's API and expertise with PHP programming.

   See the *Advanced Vendor Support* section below.

   For the most updated vendor information see sk98201.

6. Save the `$FWDIR/conf/mdm.conf` file.
7. Install policy.
8. Test the configuration.

## Advanced Vendor Support

You can add more vendors. This requires PHP programming skills and an understanding of the third-party MDM vendor's cloud API.

**Instructions**

In these steps, we use "BestMDM" as the name of a fictional MDM vendor.

BestMDM's API requires an XML request to be sent to their URL that includes credentials and the ID of the device.

It returns an XML response with the device status and reason.

**Example Request:**

```
<request>
      <username>api_username</username>
      <password>api_password</password>
      <device>device_id</device>
</request >
```

**Example Response:**

```
      <response>
            <status>compliance_status_code</status>
            <reason>reason</reason>
      </response >
```

**Example URL:**

```
https://bestmdm.com/api
```

We use these examples in the steps below.

**To add support for a new third-party vendor:**

1. Edit the `$CVPNDIR/phpincs/MDMVendors.php` file.
2. Search for the text: **to add another vendor**
3. Remove the comment for a **case** branch.
4. Enter your MDM vendor name.

   For example:

   ```
   case "BestMDM":
         BestMDM($mdm_data);
         break;
   ```

5. At the end of the file, add a new PHP function. It must access the vendor's cloud API, and return a status and reason array.

   For example:

```
function BestMDM($mdm_data) {
      // Build the request XML
      $request_xml = new
      SimpleXMLElement
("<request><username/><password/><device/></request>");
      // Fill its fields with data from $mdm_data.
      // Note that "username", "password" and "device_id"
always in $mdm_data.
      $request_xml ->username = $mdm_data["username"];
      $request_xml->password = $mdm_data["password"];
      $request_xml->device = $mdm_data["device_id"];
      // Make POST request using the supplied class
URLRequest
      // (The class URLRequest is defined in the same .php
file).
      $url = "https://bestmdm.com/api";
      $conn = new URLRequest(); // open HTTP/HTTPS request
session
      $resp_data = $conn->Request( $url, $post_body = $xml-
>asXML() );
      // Handle possible network error.
      If ($resp_data === FALSE)
            return array("status"=>MDM_ERROR, "reason"=>
$conn->get_error_message());
      // Now $resp_data is raw string returned by the cloud
API. Parse it as XML:
      $resp_xml = new SimpleXMLElement($resp_data);
      // Check the status codes returned by the vendor's
API.
      $status = MDM_ERROR;
      switch ($resp_xml->status) {
            case "not_managed":
                  return array("status"=>MDM_NOT_MANAGED,
"reason"=>"");
            case "compliant":
                  return array("status"=>MDM_COMPLIANT,
"reason"=>"");
            case "not_compliant":
                  return array("status"=>MDM_NOT_COMPLIANT,
"reason"=>$resp_xml->reason);
            default:
                  return array("status"=>MDM_ERROR,
"reason"=>"unknown status");
```

```
      } // end switch
} // end BestMDM compliance protocol handler
```

**Status Codes**:

- MDM_ERROR - Error occurred while accessing the MDM vendor's Cloud API.
- MDM_NOT_MANAGED - The device is not registered in the vendor's database.
- MDM_NOT_COMPLIANT - The device is known to the vendor as "not compliant with its policy".
- MDM_COMPLIANT - The device is known to the vendor as "compliant with its policy".

6. Define `$mdm_data` as an array of data from mdm.conf and the device ID.

```
Array(
"device_id"=><MAC address of device, or other ID known by
the vendor>,
"username"=><username to access the API of the MDM vendor>,
"password"=><password to access the API of the MDM vendor>
)
```

**Important Notes:**

- Global parameters and vendor parameters are merged in one list.
- If a vendor parameter is the same name as a global parameter, the vendor parameter overrides the global parameter.
- If **$mdm_data** includes a `password` parameter, and `password_is_obscured=1`, the password is decrypted automatically. The function gets the clear text password.

**Example of $mdm_data:**

| With mdm.conf: | $mdm_data value: |
|---|---|
| ( :enabled (1) :monitor_only (0) :fail_open (0) :active_vendor (BestVendor) :BestVendor ( :username (MyUser) :auth_key (12345) ) ) | Array( "enabled"=>1, "monitor_only"=>0, "fail_open"=>0, "active_vendor"=>"BestVendor", "username"=>"MyUser", "auth_key"=>"12345", "device_ id"=>"12:34:56:78:9A:BC:DE:F0" ) |

7. Save the `$CVPNDIR/phpincs/MDMVendors.php` file.
8. Edit the `$FWDIR/conf/mdm.conf` file.
9. Add a section after the last block for the new vendor.

   For example:

```
:BestMDM (
      :username (MyUserName)
      :password (123456)
)
```

10. Change the value of **active_vendor** to be the name of the new vendor.

    For example: `:active_vendor (BestMDM)`
11. Save the `$FWDIR/conf/mdm.conf` file.
12. Install policy.

# Testing MDM

**To make sure that MDM functionality is configured correctly**

1. On a mobile device, launch the Check Point Mobile app.
2. Connect to the Security Gateway.
3. Look for Mobile Access login logs in SmartLog.

   The **Compliance Check**, **Information**, and **Reason** values in the details of the device login, show data about MDM compliance status and requirements.

# Advanced Testing

You can make sure the MDM configuration works without a device in hand, but it requires expert knowledge. You log in to a test web page and enter the WiFi MAC address of a real device. For security, the MDM test page is disabled by default.

**To enable the test page**

1. Connect to the command line on the Security Gateway and log in the Expert mode.
2. Back up the `$CVPNDIR/conf/includes/Login.location.conf` file.
3. Edit the `$CVPNDIR/conf/includes/Login.location.conf` file.
4. Search for **test your integration**, and carefully follow the instructions there.
5. After you make required changes, save the file and run:

   ```
   [Expert@HostName:0]# cvpnrestart
   ```

6. Open the Mobile Access Portal with the `/Login/MDMProxy` path.

   For example: `https://<Security Gateway Hostname>/sslvpn/Login/MDMProxy`

7. Enter the device MAC address.
8. Click **Submit**.

   If there are issues for that device to access the third-party MDM vendor, the page shows diagnostics.

9. Revert `Login.location.conf` to the backup file.
10. Run:

    ```
    [Expert@HostName:0]# cvpnrestart
    ```

To prevent security risks, always revert and close the test page.

**Example Diagnostics**

- Parameters for the MDM vendor's cloud service (such as `Username` or `Password`) are not configured correctly in `$FWDIR/conf/mdm.conf`.
- There is a network problem accessing MDM vendor's cloud service.
- There is a problem with SSL certificates, which prevents the Security Gateway from accessing the MDM vendor's cloud service.

# System Specific Configuration

This section describes system specific configuration required for iPhones, iPads, and Android devices. In some instances, end-user configuration is also required.

## iPhone and iPad Configuration

### Connecting iPhone/iPad Clients to ActiveSync Applications

When you allow access to an ActiveSync application, users see the **ActiveSync Setup** item and can install the ActiveSync profile. This gives users access to their corporate email.

**Note** - If your ActiveSync application requires a client certificate to connect, the ActiveSync profile will work only if a client certificate is also required for Capsule Workspace.

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

**To connect to corporate email:**

1. Sign in to the Mobile Access site.
2. Tap **Mail Setup**.
3. Do the on-screen instructions.

### Getting Logs from iPhones or iPads

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

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

**To configure logs:**

1. Tap the **i** icon.

   Before login, this is on the top right. After login, this is on the bottom right.

2. Tap **Report a Problem** on the navigation bar.

   If you do not have an email account configured on the iPhone, a message shows that one must be configured. After this is done, you must open Check Point Mobile Access again.

   When an email account is configured, the email page opens. The logs are attached.

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

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

### Disabling Client SSO

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

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

**To disable SSO on a client:**

1. Tap **Settings**.
2. Scroll down to the **Check Point Mobile** icon and tap it.
3. In the **Mobile** global settings, tap the **Single Sign On** > **Enabled** switch.

# Android Configurations

### Browsing to Servers with Untrusted Server Certificates

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

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

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

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

### Session Timeout for Android Devices

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

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

### Getting Logs from Android Clients

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

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

**To send logs:**

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

# Instructions for End Users

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

## iPhone/iPad End User Configuration

Do these procedures on your iPhone/iPad so you can work with Mobile Access.

Before you start, make sure that your administrator gives you:

- The name of the site you will connect to.
- The required Registration key (also called Activation key).
- **Important** - Do only the procedures that your network administrator has instructed you to do.

**To connect to the corporate site:**

1. Get Check Point Capsule Workspace from the App Store.
2. When prompted, enter the:
   - Site Name
   - Registration key

**To connect to corporate email:**

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

**To configure logs:**

1. Tap **Information**.

   Before login, this is on the top right. After login, this is on the bottom right.

2. Tap **Report a Problem** on the navigation bar.

   If you do not have an email account configured on the iPhone, a message shows that one must be configured. After this is done, you must open Check Point Mobile Access again.

   When an email account is configured, the email page opens. The logs are attached.

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

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

**To disable SSO on a client:**

1. Tap **Settings**.
2. Scroll down to the **Capsule Workspace** icon and tap it.
3. In the **Mobile** global settings, tap the **Single Sign On** > **Enabled** switch.

# Android End User Configuration

**To disable the server certificate validation for Web applications**

1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap **Settings**.
4. Enable **Allow connection to untrusted servers**.

**To disable the server certificate validation for Web applications**

1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap **Settings**.
4. Enable **Allow connection to untrusted servers**.

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

Before you start, make sure that your administrator gives you:

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

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

**To connect to the corporate site**

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

**To send logs**

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

**To transfer the client certificate to the 3rd party mail client**

1. Launch the Check Point Mobile app.
2. Log in to the site.
3. Press the menu button and tap **Settings**.
4. From the **Export Certificate** option, tap **Export**. The Export Certificate window opens.

   If the Export Certificate option is disabled, contact the system administrator.
5. Select the certificate format appropriate for your mail client: P12 or PFX.

6. Select the location to save the certificate.
   The default path is /sdcard (for devices that have an SD card) or an external resource folder (for devices that do not have an SD card).
7. Tap **OK** to save the certificate to the selected location.

   A window shows: Export succeeded. Certificate password is: _____
8. You can copy the password to the clipboard. You will need the password when you import the certificate to the third party mail app.

# Advanced Security Gateway Configuration for Handheld Devices

You can customize client authentication, device requirements, certificate details, and ActiveSync behavior. Use the CLI commands explained here to change the configuration file: `$CVPNDIR/conf/cvpnd.C`

**Note** - Disable Link Translation Domain on Mobile Access Security Gateways before you connect to them with the Android client. To apply changes:

Restart the Mobile Access services: `cvpnrestart`

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

### To set Mobile Access attributes:

```
cvpnd_settings set <attribute_name> "<value>"
```

### To get the current value of an attribute:

```
cvpnd_settings get <attribute_name>
```

### Attributes

| Attribute | Description |
|---|---|
| ActiveSyncAllowed (true) | If access to ActiveSync applications is allowed. |
| ActiveSyncExchangeServerAuthentication Method (basic) | Method of forwarding authentication from the Mobile Access Security Gateway to the internal Exchange server.<br>Valid values: `basic`, `digest`, `ntlm` |

| Attribute | Description |
|---|---|
| MobileAppAllowActiveSyncProfileConfig (true) | Make the automatic ActiveSync Profile configuration for iPhones and iPads available to users.<br>If true, only users with authorization to access ActiveSync applications see this feature.<br>If false, no user sees this feature. |
| MobileAppMinRequiredClientOSVersion (3.1) | Minimum operating system version for iPhones and iPads. If a client fails this requirement, user sees<br>`Your OS version must be upgraded` |
| MobileAppAndroidMinRequiredClient OSVersion (2.1) | Minimum operating system version for Android. If a client fails this requirement, user sees<br>`Your OS version must be upgraded` |
| MobileAppMinRecommendedClient OSVersion (3.1) | Recommended operating system version for iPhones and iPads. If a client fails this recommendation, user sees a message but usage continues.<br>Note: value must be equal to or greater than **Required** value, or Mobile Access will not start. |
| MobileAppAndroidMinRecommendedClient OSVersion (2.1) | Recommended operating system version for Android. If a client fails this recommendation, user sees a message but usage continues.<br>Note: value must be equal to or greater than **Required** value, or Mobile Access will not start. |
| MobileAppMinRequiredClientAppVersion (1.3) | Minimum App version required for iPhones and iPads.<br>If a client fails this requirement, user sees<br>`Application Update Required` |

| Attribute | Description |
|---|---|
| MobileAppAndroidMinRequiredClient AppVersion (1.0) | Minimum App version required for Android.<br>If a client fails this requirement, user sees<br>`Application Update Required` |
| MobileAppMinRecommendedClient AppVersion (1.3) | Recommended App version for iPhones and iPads.<br>If a client fails this recommendation, user sees a message but usage continues.<br>Note: value must be equal to or greater than **Required** value, or Mobile Access will not start. |
| MobileAppAndroidMinRecommendedClient AppVersion (1.0) | Recommended App version for Android.<br>If a client fails this recommendation, user sees a message but usage continues.<br>Note: value must be equal to or greater than **Required** value, or Mobile Access will not start. |
| MobileAppMinClientOSVersionForProfile Config (3.1) | Minimum operating system version for iPhone and iPad to configure ActiveSync with the app.<br>If you want data encryption, change this value from the default to `4.0`. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption. |
| MobileAppAndroidMinClientOSVersionFor ProfileConfig (2.1) | Minimum operating system version for Android to configure ActiveSync with the app.<br>If you want data encryption, change this value from the default to `3.0`. Make sure the ActiveSync policy (configured on the Exchange server) enforces data encryption. |

| Attribute | Description |
|---|---|
| MobileAppBypassESODforApps (false) | When true, mobile apps are allowed access to Mobile Access applications whose protection level requires Endpoint Security on Demand compliance.<br>Mobile apps can always access the Mobile Access Portal. |
| MobileAppAllowClientCertExport (false) | When true, allows mobile app clients to export their client certificates to other apps and devices. See Using 3rd Party Android Mail Clients. |

# User Authentication in Mobile Access

## 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 or more of these authentication schemes:

- **Username and password** - Users enter a user name and password.
- **Client Certificates** - Digital Certificates are issued by the Internal Certificate Authority or by a third party OPSEC certified Certificate Authority.
- **RADIUS Server** - Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme. The Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users. The RADIUS protocol uses UDP for communications with the Security Gateway. RADIUS Servers and RADIUS Server Group objects are defined in SmartDashboard.

  For more about configuring a Security Gateway to use a RADIUS server, see the *R80.40 Security Management Administration Guide*.
- **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 or software that is synchronized with the central server and displays the current password. The Security Gateway forwards authentication requests by remote users to the RSA Authentication Manager.

  For more about configuring a Security Gateway to use SecurID, see the *R80.40 Security Management Administration Guide*.
- **DynamicID One Time Password** - DynamicID One Time Password can be required as a secondary or later authentication method (not the first). When this is configured, users who successfully complete the first-phase or phases of authentication are challenged to enter an additional credential: a DynamicID One Time Password (OTP). The OTP is sent by email or text message to a mobile phone, or other mobile communication device.
- **Defined on user record (Legacy Authentication)** - The authentication method for each user is defined on the user record. For internal users, it is in the **Authentication** page of the User Properties. For LDAP users, it is on the user record in LDAP.

A user who tries to authenticate with an authentication scheme that is not configured for the Mobile Access Security Gateway will not be allowed to access resources through the Security Gateway.

**Note** - Legacy Mobile Access Policy (configured in SmartDashboard) does not support users configured on an LDAPS server.

# Configuring Authentication for Security Gateways R77.30 and lower

Permitted authentication schemes must be configured for each Security Gateway.

On the Security Gateway, configure authentication in the **Gateway Properties** window of a Security 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.

The default authentication scheme is **Username and Password**.

In the **Mobile Access** tab in SmartDashboard, select **Authentication** to show an overview of the Mobile Access Security Gateways and their authentication schemes.

On this page you can also configure settings for Two- Factor Authentication with a DynamicID One Time Password. Configure settings for the Security Gateway or global settings that are used for all Security Gateways that do not have their own DynamicID settings.

# Requiring Certificates for Mobile Devices on Security Gateways R77.30 and lower

**To require client certificates for mobile devices:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Authentication**.
3. Make sure that the Authentication Method is one of these options:
   - **Username and password**
   - **RADIUS**
   - **SecurID**
4. From the **Certificate Authentication for mobile devices** section, click **Require client certificate when using ActiveSync applications or Mobile Mail**.

5. Click **OK**.
6. Install the policy.

# Image-Based RADIUS Authentication

Use Image-based RADIUS as a secondary authentication factor to authenticate to the Mobile Access Portal. It allows Mobile Access to integrate with third-party authentication services.

The images in this authentication factor are patterns of random numbers in a grid. During authentication, the user selects the numbers in the positions that correspond to a pre-selected pattern.

## Configuring Image-Based RADIUS

To use image-based RADIUS as an authentication factor in Mobile Access, you have to configure RADIUS authentication with SmartConsole.

**To configure Mobile Access authentication factors in SmartConsole:**

1. In SmartConsole, from the **Gateways & Servers** tab, double-click the Security Gateway.

   The Check Point Security Gateway window shows.
2. From the menu, click **Mobile Access > Authentication**.
3. In the **Multiple Authentication Client Settings** table, add a new login option.
   a. Click **Add > New**.

      The **Multiple Login Options** window shows.
   b. In the **Authentication Methods** table, click **Add** to create **Authentication Factors**.
   c. When the **Authentication Factor** window opens, click **RADIUS**.
   d. Under **Customize Display**, add an appropriate description to the **Headline**.

      **Note** - When you return to the **Authentication Methods** table, make sure RADIUS authentication is not the first factor.

## Enabling Image-Based RADIUS on Security Gateways

To enable Image-based RADIUS, edit the configuration file, `$CVPNDIR/conf/cvpnd.C` on each Mobile Access Security Gateway that uses Image-based RADIUS as an authentication factor.

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

```
:isImageBasedRadiusEnabled (false)
:ImageBasedRadiusRealmNames (
)
:ImageBasedRadiusURL ("")
```

| Fields | Description | Example |
|---|---|---|
| `:isImageBasedRadiusEnabled (true)`<br>`:isImageBasedRadiusEnabled (false)` | Enter **true** to enable.<br>Enter **false** to disable.<br>If set to true, the Security Gateway treats every RADIUS authentication factor found in `:ImageBasedRadiusRealmNames` as an Image-based RADIUS authentication factor. | |
| `:ImageBasedRadiusRealmNames` | List that has authentication realm names that are configured in SmartConsole, that contain Image-based RADIUS authentication as a secondary factor.<br>If empty, all the authentication realms with RADIUS as a secondary authentication factor, are treated as an Image-based RADIUS authentication factor. | `(: ("`*realm name as configured*`")`<br>`: (`*"another realm with Image-based RADIUS"*`))` |
| `:ImageBasedRadiusURL` | The URL from the third-party authentication service to get the user grid.<br>Use `$$username` as a placeholder for the username. | `("https://<`*authentication_provider_url*`>?<`*query_string*`>&username=$$username")` |

# Authentication on a RADIUS Server over MS-CHAPv2 with UPN

**To enable authentication of Remote Access VPN Clients on a RADIUS server over Microsoft Challenge-Handshake Authentication Protocol (MS-CHAPv2) with UPN (<username>@<domain>):**

**Note** - This feature is available starting from R80.40 Jumbo Hotfix Accumulator Take 190.

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Get the current value:

   ```
   ckp_regedit -p SOFTWARE/Checkpoint/VPN1 | grep --color RADIUS_MSCHAPV2_UPN
   ```

4. To enable this feature:

   ```
   ckp_regedit -a SOFTWARE/Checkpoint/VPN1 RADIUS_MSCHAPV2_UPN -n 1
   ```

   This command applies immediately and does **not** require a restart.

   To disable this feature:

   ```
   ckp_regedit -a SOFTWARE/Checkpoint/VPN1 RADIUS_MSCHAPV2_UPN -n 0
   ```

# Google reCAPTCHA Challenge

The reCAPTCHA service uses an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities. It prevents malicious logins and at the same time allows authenticated users to pass through easily.

Configure your Security Gateway with Google reCAPTCHA v2 to challenge a user upon multiple, incorrect login attempts. reCAPTCHA appears as a challenge when a user reaches the maximum number of failed attempts.

The reCAPTCHA challenge is compatible with ClusterXL and VSX.

The reCAPTCHA challenge is not supported in the Capsule Workspace.

For supported browsers, see the Google documentation.

# Registering Mobile Access for reCAPTCHA on Google

To use Mobile Access with reCAPTCHA, you have to register the Mobile Access Portal FQDN with reCAPTCHA.

Go to the Google reCAPTCHA site for instructions.

# Adding reCAPTCHA to the Mobile Access Portal

You have to configure the Security Gateway manually to add reCAPTCHA. To enable reCAPTCHA, the Security Gateway needs:

- Internet connectivity
- A DNS configured
- Portal URL configuration with an FQDN and not an IP addres

  If you browse to the Portal with an IP address rather than an FQDN, you are redirected to the FQDN link.

  **Note** - In a cluster environment, each Security Gateway has to be configured identically.

To configure the Security Gateway manually, edit the `$CVPNDIR/conf/cvpnd.C` file.

**Important** - After every change in the `cvpnd.C` file, you must restart the CVPN services with the `cvpnrestart` command.

This shows:

```
:isCaptchaEnabled (false)
:isCaptchaEnabledForRelogin (false)
:captchaFailOpen (false)
:captchaPenaltyTimeInSeconds (1800)
:captchaFailedAttemptsThreshold (2)
:reCaptchaSiteKey ()
:reCaptchaSecret ()
:isCaptchaSettingsVerifierEnabled (false)
```

| Fields | Description |
|---|---|
| `:isCaptchaEnabled (true)`<br>`:isCaptchaEnabled (false)` | Enter **true** to enable.<br>Enter **false** to disable. |
| `:IsCaptchaEnabledForRelogin(true)`<br>`:IsCaptchaEnabledForRelogin(false)` | Determines if reCAPTCHA shows on a re-login flow.<br>Enter **true** to enable.<br>Enter **false** to disable. |

| Fields | Description |
|---|---|
| `:captchaFailOpen(true)`<br>`:captchaFailOpen(false)` | Entrance to the Portal.<br>Enter **true** to enable.<br>Enter **false** to disable.<br>This determines when to block users:<br>■ No connectivity from the Security Gateway to Google<br>■ Invalid or missing a secret key<br>■ Invalid or missing a validation response from Google<br>■ Portal URL is not configured with an FQDN<br>**False** - User is not allowed access to the Portal. See the login log for more information.<br>**True** - User is allowed access to the Portal. A warning that the reCAPTCHA challenge was not verified shows. See the login log for more information. |
| `:captchaPenaltyTimeInSeconds (1800)` | The amount of time in seconds that the user in penalty is challenged with reCAPTCHA on each login until the user succeeds to log in. The default is 1800 seconds. |
| `:captchaFailedAttemptsThreshold (2)` | This is the number of times a user tries to log in unsuccessfully before reCAPTCHA shows.<br>The default is two failed login attempts within the pre-determined time frame. Failures within that time frame are counted. If the time frame passes, the failure counter is set to zero again.<br>If the field is set to zero, there is a reCAPTCHA challenge on every login attempt. |
| `:reCaptchaSiteKey ()` | The site key from Google. |
| `:reCaptchaSecret ()` | The secret from Google. |

| Fields | Description |
|---|---|
| `:isCaptchaSettingsVerifierEnabled (true)`<br>`:isCaptchaSettingsVerifierEnabled (false)` | A utility page that checks the reCAPTCHA configuration and the connectivity from the Security Gateway.<br>Enter **true** to enable the page.<br>Enter **false** to disable the page.<br>To see this page, go to:<br>`https://<Portal URL >/Login/verifyCaptchaSettings` |

**Best Practice** - If you enable and configure reCAPTCHA, make sure the Capsule Workspace uses certificate authentication. reCAPTCHA is not supported in the Capsule Workspace.

When you are challenged with reCAPTCHA, some Java scripts are downloaded to your browser.

# Multiple Login Options for Security Gateways R77.30 and lower

On Security Gateways R80.10 and higher, you can configure multiple login options for Mobile Access and IPsec VPN.

The options can be different for each Security Gateway and each supported Software Blade, and for some client types. Users select one of the available options to log in with a supported client.

By default, all clients connect with the method for R77.30 and lower. When you create new login options, newer clients can see them in addition to the option of R77.30 and lower, but older clients cannot.

To see which clients support the new multiple login options, see sk111583.

Each configured login option is a global object that can be used with multiple Security Gateways and the Mobile Access and IPsec VPN Software Blades.

## Compatibility with Older Clients

Older clients connect with the same login options available on Security Gateways R77.30 and lower. If you upgrade all or most clients to versions that support multiple login options, you can block older clients from connecting. After you do this, only clients that support multiple login options can connect to the Security Gateway.

By default, **Allow older clients to connect to this gateway** is selected in **Mobile Access** > **Authentication**. If you clear the option, older clients are blocked.

You can choose if newer clients that support multiple login options can connect with the authentication settings defined for older clients.

## Configuring the Authentication Method for Newer Clients

**To block newer clients from using the authentication method defined for older clients:**

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. In the **Compatibility with Older Clients section**, click **Settings**.

   The **Single Authentication Clients Settings** window opens.
3. Clear **Allow newer clients that support Multiple Login Options to use this authentication method**.
4. Click **OK**.
5. Install policy.

**To let newer clients connect to the Security Gateway with the authentication settings defined for older clients:**

Select **Allow newer clients that support Multiple Login options to use this authentication method**.

## Configuring Authentication Settings for Older Clients

**To let older clients connect to the Security Gateways R80.10 and higher:**

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. Select **Allow older clients to connect to this gateway**.

   If this is not selected, older clients cannot connect to the Security Gateway.

**To change the authentication method for older clients:**

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. In the **Compatibility with Older Clients** section, click **Settings**.

   The **Single Authentication Clients Settings** window opens.
3. Change the **Display Name** to change the way the authentication method is shown in SmartConsole.
4. Select an **Authentication method**.

5. Click **Customize** to change the description of fields that are shown to users in the **login** window. See the "Customize Display Settings" section.
6. To require DynamicID with the selected authentication method, select **Enable DynamicID**. After you select this, you must configure the DynamicID settings for the Security Gateway from **Authentication** > **DynamicID Settings** > **Edit**.
7. Define the settings for **Capsule Workspace**:
   - Select **Require client certificate** to require **Capsule Workspace** to always use client certificates.
   - Select Allow DynamicID to require DynamicID in addition to the selected authentication method. After you select this, you must configure the DynamicID settings for the Security Gateway from **Authentication** > **DynamicID Settings** > **Edit**.
8. Click **OK**.
9. Click **OK**.
10. Install policy on the Security Gateway.

**To configure global DynamicID settings that all Security Gateways use:**

1. For each Security Gateway, in **Gateway Properties** > **Mobile Access** > **Authentication** > **DynamicID Settings**, select **Use Global Settings**.
2. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
3. Configure the global settings in **Mobile Access** tab > **Authentication** > **Two-Factor Authentication with DynamicID**.
4. Close SmartDashboard
5. In SmartConsole, install policy on the Security Gateway.

# Configuring Multiple Log-in Options

You can configure login options from:

- **Gateway Properties** > **Mobile Access** > **Authentication**
- **Gateway Properties** > **VPN Clients** > **Authentication**
- SmartDashboard > **Mobile Access** tab > **Authentication**

The login options selected for Mobile Access clients, such as the Mobile Access Portal and Capsule Workspace, show in the **Mobile Access** > **Authentication** page in the **Multiple Authentication Client Settings** table.

The login options selected for VPN clients, such as Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote, show in the **VPN Clients** > **Authentication** page in the **Multiple Authentication Client Settings** table.

**To configure multiple login options for Mobile Access Clients:**

1. From the **Gateway Properties** tree of a Security Gateway, select **Mobile Access** > **Authentication**.
2. In the **Multiple Authentication Clients Settings** table, see a list of configured login options.

   The default login options are:

   - Personal_Certificate - Require a user certificate.
   - Username_Password - Require a username and password.
   - Cert_Username_Password - Require a username and password and a user certificate.
3. Click **Add** to create a new option or **Edit** to change an option. Each configured login option is a global object that can be used with multiple Security Gateways and Software Blades.
4. For each login option select one or more **Authentication Factors** and relevant **Authentication Settings**.

   For example, if you select **SecurID**, select the SecurID **Server** and **Token Card Type**. If you select **Personal Certificate**, select which certificate field the Security Gateway uses to fetch the username. See the "Certificate Parsing" section.
5. Select **Customize Display** to configure what users see when they log in with this option. See the "Customize Display Settings" section.
6. Click **OK**.
7. Use the **Up** and **Down** arrows to set the order of the login options.
   - If you include **Personal Certificates**, it must be first.
   - If you include **DynamicID**, it cannot be first.
8. On each **Login Option** > **Usage in Gateway**, select if the login option is available from:
   - The **Mobile Access Portal**
   - **Capsule Workspace**
9. Click **OK**.

## Selecting a Client for a Login Option

For login options created from the **Mobile Access** > **Authentication** page, you can select if the login option is available for the Mobile Access Portal, Capsule Workspace, or both.

The login option will only be visible for the clients that you select.

## Customize Display Settings

Enter descriptive values to make sure that users understand what information to input. These fields must all be the same language but they do not need to be in English.

- **Headline** - The title of the login option, for example, **Log in with a Certificate** or **Log in with your SecurID Pinpad**.
- **Username label** - A description of the username that users must enter, for example, **Email address** or **AD username**.
- **Password label** - A description of the password that users must enter, for example, **AD password**.

## Certificate Parsing

When you select **Personal Certificate** as a Login option, you can also configure what information the Security Gateway sends to the LDAP server to parse the certificate. The default is the DN. You can configure the settings to use the user's email address or a serial number instead.

**To change the certificate parsing:**

1. In the **Multiple Authentication Clients Settings** table on the **Authentication** page, select a **Personal_Certificate** entry and click **Edit**.

   The **Authentication Factor** window opens.
2. In the **Authentication Settings area** in the **Fetch Username from** field, select the information that the Security Gateway uses to parse the certificate.
3. Click **OK**.
4. Install policy.

## Deleting Login Options

**To permanently delete a Login option:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

2. In SmartDashboard go to the **Mobile Access** tab > **Authentication** page.
3. From the list of login options, select an option and click **Delete**.

### Viewing all Authentication Settings

**To see all Security Gateways and their authentication settings:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.
2. In SmartDashboard go to the **Mobile Access** tab.
3. From the tree, select **Gateways**.
4. Click a Security Gateway to see its authentication settings.

# Multi-Factor Authentication with DynamicID

Multi-factor authentication is a system where two or more different methods are used to authenticate users. Using more than one factor delivers a higher level of authentication assurance. DynamicID is one option for multi-factor authentication.

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.

On Security Gateways R80.10 and higher, DynamicID is supported for all Mobile Access and IPsec VPN clients.

## How DynamicID Works

When logging in to the Mobile Access Portal, users see an additional authentication challenge such as:

**Please type the verification code sent to your phone**.

Users enter the one time password that is sent to the configured phone number or email address and they are then admitted to the Mobile Access Portal.

On the User Portal sign in screen, the **I didn't get the verification code** link shows. If the user does not receive an SMS or email with the verification code within a short period of time, the user can click that button to receive options for resending the verification code.

Administrators can allow users to select a phone number or email address from a list. Only some of the phone number digits are revealed. Users can then select the correct phone number or email address from the list and click **Send** to resend the verification code. By default, users can request to resend the message three times before they are locked out of the Portal.

### Match Word

The Match Word feature ensures that users can identify the correct DynamicID verification code in situations when they may receive multiple messages. Users are provided with a match word on the Login page that will also appear in the correct message. If users receive multiple SMS messages, they can identify the correct one, as it will contain the same match word.

## The SMS Service Provider

In Security Gateways R77.30 and lower, proxy settings for the SMS service provider were configured in **Gateway Properties** > **Mobile Access** > **HTTP Proxy**.

In Security Gateways R80.10 and higher, this is configured in **Gateway Properties** > **Network Management** > **Proxy**.

**To access the SMS service provider, configure the proxy settings on the Security Gateway:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.

2. From the navigation tree, click **Network Management** > **Proxy**.

3. Define the Proxy settings.

   If no proxy is defined on this page, no proxy is used for the SMS provider.

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.

## DynamicID Authentication Granularity

You can make multi-factor authentication with DynamicID a requirement to log in to the Security Gateway. Alternatively, you can make DynamicID a requirement to access specified applications. This flexibility gives you different security clearance levels.

To make multi-factor authentication with DynamicID a requirement to access specified applications, configure a Protection Level to require multi-factor authentication, and associate the Protection Level with Mobile Access applications (see the "Two-Factor Authentication per Application" section).

In an environment with multiple Mobile Access Security Gateways, make multi-factor authentication a requirement for a specified Security Gateway, configure multi-factor authentication for that Security Gateway.

On Security Gateways R80.10 and higher, DynamicID authentication can be part of a login option that is required for the Mobile Access Portal or Capsule Workspace, or both.

# Basic DynamicID Configuration for SMS or Email

The workflow for basic configuration of two-factor authentication via DynamicID is:

1. **Obtain the SMS provider credentials and/or email settings.**

   Get these required SMS service provider settings from your SMS provider.

   - A URL in the format specified by the SMS provider or a valid email address.
   - Account credentials:
     - User name
     - Password
     - API ID (optional and may be left empty)

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

2. **Configure the Phone Directory**

   The default phone number and email search method is that the Security 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 Security 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 Security Gateway. For a Mobile Access cluster, configure the directory on each cluster member.

   **To configure a list of phone numbers on a Security Gateway:**

   a. Connect to the command line on the Mobile Access Security Gateway using a secure console connection.

b. Log in to the Expert mode.

c. Back up the `$CPDIR/conf/dynamic_id_users_info.lst` file.

**Note** - If this file does not yet exist, create it.

d. Edit the `$CPDIR/conf/dynamic_id_users_info.lst` file.

e. Add a list of user names and phone numbers, and/or email addresses.

The list must be followed by a blank line. Use this syntax:

```
<Username or Full DN> <Phone number or Email address>
```

| Parameter | Meaning |
|---|---|
| *<Username>* or *<Full DN>* | Either a user name or, for users that log in using a certificate, the full DN of the certificate. |
| *<Phone number>* | All printable characters can be used in the phone number, excluding the space character, which is not allowed. Only the digits are relevant. |
| *<Email address>* | A valid email address in the format user@domain.com |

Example of acceptable ways to enter users and their phone numbers or email addresses in `$CPDIR/conf/dynamic_id_users_info.lst`

```
bob +044-888-8888
jane.tom@domain.com
CN=tom,OU=users,O=example.com +044-7777777
CN=mary,OU=users,O=example.com +mary@domain.com
```

### Configuring Multiple Phone Numbers

You can let users choose from multiple phone numbers when resending the verification code.

#### To configure choice of numbers:

Edit the configuration file `$CPDIR/conf/dynamic_id_users_info.lst` on the Security Gateway.

- Enter one number in the LDAP directory in the **Mobile** field and one or more phone numbers in configuration file.
- Enter multiple phone numbers separated by white space in the configuration file.

  For example: `user_a 917-555-5555 603-444-4444`

**Note** - If the configuration file `$CPDIR/conf/dynamic_id_users_info.lst` does not yet exist, create it.

3. **Perform basic configuration of DynamicID in SmartDashboard**

   Configure the **Authentication** settings to make two-factor authentication necessary for all mobile devices.

   This 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.

| Parameter | Meaning |
|---|---|
| $APIID | The value of this parameter is the API ID. |
| $USERNAME | The value of this parameter is the username for the SMS provider. |
| $PASSWORD | The value of this parameter is the password for the SMS provider. |
| $PHONE | User phone number, as found in Active Directory or in the local file on the Security Gateway, including digits only and without a + sign. |
| $EMAIL | The email address of the user as found in Active Directory or in the local file on the Security Gateway - `$CPDIR/conf/dynamic_id_users_info.lst`. If the email address should be different than the listed one, it can be written explicitly. if the file does not exist, create it. |
| $MESSAGE | The value of this parameter is the message configured in the Advanced Two-Factor Authentication Configuration Options in SmartDashboard. |
| $RAWMESSAGE | The text from `$Message`, but without HTTP encoding. |

**Configuring DynamicID settings in SmartDashboard for all Security Gateways**

a. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access**.

   Click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

b. From the navigation tree, click **Authentication**.

c. From the **Dynamic ID Settings** section, click **Edit**.

d. Select **Challenge users to provide the DynamicID one time password**.

e. Fill in the **SMS Provider and Email Settings** field using one of these formats:

   i. To let the DynamicID code to be delivered by SMS only, use the following syntax:

   ```
   https://api.example.com/http/sendmsg?api_
   id=$APIID&user=$USERNAME&password=$PASSWORD&to=$PHON
   E&text=$MESSAGE
   ```

ii. To let the DynamicID code to be delivered by email only, without an SMS service provider, use the following syntax:

- For SMTP protocol:

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

- For SMTPS protocol on port 465:

```
mail:TO=$EMAIL;SMTPSERVER=smtps://username:passw
ord@smtp.example.com;FROM=sslvpn@example.com;BOD
Y=$RAWMESSAGE
```

- For SMTP protocol with START_TLS:

```
mail:TO=$EMAIL;SSL_
REQUIRED;SMTPSERVER=smtp://username:password@smt
p.example.com;FROM=sslvpn@example.com;BODY=$RAWM
ESSAGE
```

- For SMTP protocol on port 587 with START_TLS:

```
mail:TO=$EMAIL;SSL_
REQUIRED;SMTPSERVER=smtp://username:password@smt
p.example.com:587;FROM=sslvpn@example.com;BODY=$
RAWMESSAGE
```

iii. To let the DynamicID code to be delivered by SMS or email, use the following syntax:

```
sms:https://api.example.com/sendsms.php?username=$US
ERNAME&password=$PASSWORD&phone=$PHONE&smstext=$MESS
AGE
mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslv
pn@example.com;BODY=$RAWMESSAGE
```

**Note** - If the SMTP username and password contain special characters, use these:

| ! | # | $ | % | & | ' | ( |
|---|---|---|---|---|---|---|
| %21 | %23 | %24 | %25 | %26 | %27 | %28 |
| ) | * | + | , | / | : | ; |
| %29 | %2A | %2B | %2C | %2F | %3A | %3B |
| = | ? | @ | [ | ] | | |
| %3D | %3F | %40 | %5B | %5D | | |

f. In the **SMS Provider Account Credentials** section, enter the credentials received from the SMS provider:
   - **Username**
   - **Password**
   - **API ID** (optional)

g. For additional configuration options, click **Advanced**.

h. Click **OK**.

i. Click **Save** and then close SmartDashboard.

j. In SmartConsole, install policy.

**Configuring the Mobile Access Security Gateway to let computers and devices use DynamicID**

a. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.

b. From the navigation tree, click **Mobile Access > Authentication**.

c. In the **Two-Factor Authentication** section, configure these settings:
   - For a Security Gateway that uses the global authentication settings, select **Global settings**.
   - For a Security Gateway that uses different authentication settings, select **Custom settings**.
   - For mobile devices, select **Allow DynamicID for mobile devices**.

d. Click **OK**.

e. Install the policy.

4. **Test DynamicID Two-Factor Authentication**

   a. Browse to the URL of the Mobile Access Portal.

   b. Log in as a user.

   c. Supply the Security Gateway authentication credentials.

   d. Wait to receive the DynamicID code on your mobile communication device or check your email.

e. Enter the DynamicID code in the portal.

Make sure that you are logged in to the Mobile Access Portal.

# Advanced Two-Factor Authentication Configuration

**To configure settings for a specified Security Gateway:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Authentication**.
3. From the **Two-Factor Authentication with DynamicID** section, click **Custom settings for this gateway**.
4. Click **Configure**.

   The **Two-Factor Authentication with DynamicID** window opens.

**To configure global settings for all the Security Gateways:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Authentication**.
3. From the **DynamicID Settings** section, click **Edit**.
4. Click **Advanced**.

   The **Two-Factor Authentication with DynamicID** window opens.

## 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**.

| Parameter | Meaning |
|---|---|
| `$NAME` | User name used in the first phase of authentication to the portal. |

| Parameter | Meaning |
|---|---|
| `$CODE` | Replaced with the One Time Password.<br>By default, `$CODE` is added to the end of the message. |

## DynamicID Settings

- **Length of one time password** - By default, it is 6 digits.
- **One time password expiration (in minutes)** - By default, it is 5 minutes. 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 Security 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 Security Gateway.

  The LDAP account unit is defined in the **Users and Authentication > Authentication > LDAP Account Units** page of the SmartDashboard Mobile Access tab.

  The local phone directory on the Security Gateway is in the `$CPDIR/conf/dynamic_id_users_info.lst` file.

  **Note** - If this file does not exist yet, create it.

- **Active Directory Only**

  Retrieve phone numbers from Active Directory user record without using the local file on the Security 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 Security Gateway.

  The local phone directory on the Security Gateway is in the `$CPDIR/conf/dynamic_id_users_info.lst` file.

  **Note** - If this file does not exist yet, create it.

# Configuring Resend Verification and Match Word

The DynamicID troubleshooting and match word features are configured in Database Tool (GuiDBEdit Tool) (see sk13009) or `dbedit` (see sk13301).

The Database Tool (GuiDBEdit Tool) 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** > **Authentication**.

- If your DynamicID One Time Password settings are global across all of your Security Gateways (use the global settings configured in the Mobile Access tab is selected), in the Database Tool (GuiDBEdit Tool) select **Other > Mobile Access Global Properties**.
- If your DynamicID One Time Password settings are configured for a specific Security Gateway (this Security Gateway has its own two-factor authentication settings is selected), in the Database Tool (GuiDBEdit Tool) select **network_objects** and then select the specific Security Gateway you want to edit.

This table shows the DynamicID features that can be configured, and where in Database Tool (GuiDBEdit Tool) to configure them.

| Feature | Attributes to Edit | Values and their Descriptions |
|---|---|---|
| Match Word | `use_message_matching_helper` | **true**: match word provided<br>**false**: match word not provided (default) |
| Resend message | `enable_end_user_re_transmit_message` | **true**: enable resend SMS feature (default)<br>**false**: disable resend SMS feature |
| Display multiple phone numbers | `enable_end_user_select_phone_num` | **true**: enable option to choose from multiple phone numbers or email addresses when resending the verification code (default)<br>**false**: one phone number or email address from the LDAP server or local file is used automatically without choice |

| Feature | Attributes to Edit | Values and their Descriptions |
|---|---|---|
| Conceal displayed phone numbers | Edit these attributes: `reveal_partial_phone_num` and `number_of_digits_revealed` | For `reveal_partial_phone_num`:<br>**true**: conceal part of the phone number or email address (default)<br>**false**: display the full phone number or email address<br>For `number_of_digits_revealed`:<br>**1-20**: Choose the amount of digits to reveal (default is 4) |

After editing the values in the Database Tool (GuiDBEdit Tool):

1. Save all changes: **File** menu > **Save All**.
2. Close the Database Tool (GuiDBEdit Tool).
3. Open SmartConsole.
4. Install the Access Control policy on the Security Gateway.

## 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 this command in the Expert mode on the Security Gateway:

```
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 the "`cvpnrestart`" command to activate the settings.

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

# Two-Factor Authentication per Security Gateway

**To configure two-factor authentication "Globally on, with custom settings per Security Gateway":**

1. Set up basic two-factor authentication.
2. For each Security Gateway, in the Security Gateway Properties, go to **Gateway Properties > Mobile Access > Authentication**.
3. Configure one of these options:
   - **To use the global settings** - Select **Global settings** and the global settings are used from the **Authentication to Gateway** page of the Mobile Access tab. This is the default.
   - **To turn off two-factor authentication for the gateway** - Select **Custom Settings for this Gateway** and click **Configure**. In the window that opens, do not select the check box. This turns off two-factor authentication for this Security 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 Security Gateway. Optionally, configure **Advanced** options.
4. Repeat **step 2** and **step 3** for all other Security Gateways.
5. Install the Access Control policy.

# Two-Factor Authentication per Application

**To configure two-factor authentication per application:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. Configure basic two-factor authentication (see *"Basic DynamicID Configuration for SMS or Email" on page 160*).
   a. Configure the phone directory.
   b. Configure the application settings in **Mobile Access** tab **> Authentication**.
   c. Configure the Mobile Access Security Gateways to let the mobile devices use DynamicID.
3. Configure the *"Mobile Access Applications" on page 55*.

a. In the **Protection Level** window, from the navigation tree click Authentication.

b. Select **User must successfully authenticate via SMS**.

c. Click **OK**.

4. Assign the protection level to Mobile Access applications that require *"Mobile Access Applications" on page 55*.
5. Click **Save** and then close SmartDashboard.
6. In SmartConsole, install the Access Control policy.

### Changing the SMS Provider Certificates and Protocol

By default, it is recommended to use a secure (https) protocol for communication with the SMS provider. Mobile Access also validates the provider server certificate using a predefined bundle of trusted CAs.

If your SMS provider uses a non-trusted server certificate you can do one of the following:

- Add the server certificate issuer to the trusted CA bundle in `$FWDIR/database/{}` and run this command in the Expert mode:

  ```
  $CVPNDIR/bin/rehash_ca_bundle
  ```

- Ignore the server certificate validation by editing the `$CVPNDIR/conf/cvpnd.C` file 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 `("")`.

# Configuring Multiple Log-in Options for Security Gateways Using Database Tool (GuiDBEdit Tool)

On Security Gateways R77.30 and lower, "Multiple Log-in" options is called "Multiple Realms" and is configured in the Database Tool (GuiDBEdit Tool) (see sk13009) or `dbedit` (see sk13301). It gives support for multiple authentication realms in the Mobile Access Portal. If you use this feature, we recommend that you upgrade your Security Gateways to this release and configure Multiple Login Options in SmartConsole.

If you upgrade your Management Server and Security Gateways to this release, see sk115856 for information about upgrading the multi-realms configuration.

If you upgrade only your Management Server and do not upgrade the Security Gateways, reconfigure Multiple Realms in Database Tool (GuiDBEdit Tool) after the upgrade.

# How the Security 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 Security Gateway searches in this order:

1. The internal users database.
2. If the specified user is not defined in this database, the Security Gateway queries the User Directory (LDAP) servers defined in the Account Unit one at a time, and according to their priority.

   If more than one Account Unit exists, the Security Gateway searches in all at the same time. .With multiple servers, the priority for servers can be set only in the scope of one account unit, but not between several account units.
3. If the information still cannot be found, the Security 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.

# Session Settings

**To open the Session window:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Additional Settings > Session**.

## Simultaneous Logins to the Mobile Access 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 Security Gateway to automatically disconnect a remote user who is logged more than once.

When simultaneous login prevention is enabled, and a user's authentication information used to log in from two different computers, only the later login is considered legitimate, and the earlier session is logged out.

**Note** - The Simultaneous Login is not supported for the SNX client when the Office Mode Method is configured to allocate IP addresses from the `$FWDIR/conf/ipassignment.conf` file. See sk176343.

## 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 enabled. This is the default option.

- **User is allowed only a single login to the portal**

  Inform user before disconnecting his previous session (option is not selected)

  The earlier user is disconnected and the later user is allowed. The earlier user is logged out. For Mobile Access Portal users, the following message appears:

  **"Your Mobile Access session has timed out. would you like to sign in again now?"**. The later user is not informed that an earlier user is logged in.

- **User is allowed only a single login to the portal** (option selected)

  Inform user before disconnecting his previous session(option selected)

  The later user is informed that an earlier user is logged in, and is given the choice of canceling the login and retaining the existing session, or logging in and terminating the existing session. If the existing session is terminated, the user is logged out with the message:

  **"Your Mobile Access session has timed out. would you like to sign in again now?"**.

## Tracking of Simultaneous Logins

To track simultaneous login events, select **All Events** in the **Tracking** section of the **Additional Settings > Session** page.

When the Security Gateway disconnects a user, the Security 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

These 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**.

## 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.

**For Capsule Clients:**

1. Go to **SmartDashboard > Mobile Access** tab > **Capsule Workspace Settings** > **Mobile Profiles**.
2. Create or edit the applicable profile.
3. In the **Access Settings** section, configure the applicable value in the **Session timeout** field.

## Roaming

The **Roaming** option allows users to change their IP addresses during an active session.

**Note** - SSL Network Extender users can always change IP address while connected, regardless of the Roaming setting.

## Tracking

Configure Mobile Access to log session activity, including login attempts, logouts, timeouts, activity states and license expiration warnings.

## Securing Authentication Credentials

Having multiple users on the same machine accessing the Mobile Access Portal can be a security hazard. A user logged in to the Mobile Access Portal can open a new browser window and get the access of the earlier session. Then the user can browse directly to the Mobile Access Portal without entering the login credentials again.

To make sure authentication credentials are not stolen by others, recommend to users that they log off or close all browser windows when done using a browser.

# Mobile Access Authentication Use Cases

## Use Case: Two-Factor Authentication with Certificates in Security Gateways R77.30 and lower

Select a main authentication method for Security Gateways R77.30 and lower. If you also select **Require client certificate when using Mobile applications** on the **Authentication** page, you require two-factor authentication for Capsule Workspace users: the main authentication method, and certificate.

With these settings, users authenticate to the Mobile Access Portal with only the main authentication method.

Capsule Workspace users receive the certificate information and register only one time. They provide the main authentication method credentials one time per session. Users might also need to enter a passcode, based on settings in the **Capsule Workspace Settings** in the **Mobile Access** tab.

**To configure two-factor authentication with certificates for mobile devices on Security Gateways R77.30 and lower**

1. Open the Security Gateway object.
2. Select **Mobile Access** > **Authentication**.
3. Select a main authentication method from these options:
   - Username and Password
   - RADIUS
   - SecurID
4. Select **Require client certificate when using Mobile applications** or **Require client certificate when using ActiveSync applications**.
5. Click **OK**.
6. Install the Access Control policy.

To configure two-factor authentication with the Mobile Access Portal in Security Gateways R77.30 and lower, see sk86240.

# Use Case: Two Factor Authentication with Certificates on Security Gateways R80.10 and higher

You can configure two factor authentication with certificate on a Security Gateway R80.10 and higher in these ways:

- Create a new Login Option with Personal Certificate as the first factor and one or more additional methods that you choose as additional factors.
- Use the default Login Option, **Cert_Username_Password**, which includes a personal certificate as the first factor, and username and password as the second factor.

**To create a new multi-factor login option that includes certificates:**

1. Open the Security Gateway object.
2. Click **Mobile Access** > **Authentication**.
3. In the **Multiple Authentication Clients Settings** table, click **Add** to create a new option.

4. Click **New**.
5. In the **Multiple Login Options** window, enter the Login Option's **Name** and **Display Name**.

   The **Display Name** represents this Login Option to the user upon login and can be a descriptive name.
6. Under **Authentication Methods**, click **Add** to add the first factor.
   a. In the Authentication Factor window, select **Personal Certificate**. Note that Personal Certificate must be the first authentication factor.
   b. Configure the Authentication settings.
   c. Click **OK**.
7. Under **Authentication Methods**, click **Add** to add the second factor.
   a. In the Authentication Factor window, select RADIUS, SecurID, DynamicID or Username and Password.
   b. Configure the Authentication settings, if necessary.
   c. Click **OK**.
8. To apply this Login Option only to the Mobile Access Portal or only to Capsule Workspace on mobile devices, under **Usage in Gateway**, select one or both client types.
9. Click **OK**.
10. Install the Access Control policy.

**To use the built-in default Login Option Cert_Username_Password:**

1. Open the Security Gateway object.
2. Click **Mobile Access** > **Authentication**.
3. In the **Multiple Authentication Clients Settings** table, click **Add**.
4. Select **Cert_Username_Password** from the list.
5. To apply this Login Option only to the Mobile Access Portal or only to Capsule Workspace on mobile devices:
   a. In the **Multiple Authentication Clients Settings** table, select **Cert_Username_Password** and click **Edit**.
   b. Under **Usage in Gateway**, select one or both client types.
6. Click **OK**.
7. Install the Access Control policy.

**Note** - The Login Options configured in the Multiple Authentication Clients Settings list are only available to clients that support multiple login options. To see which clients support the new multiple login options, see sk111583.

## Use Case: Users Selecting a Login Option on Security Gateways R80.10 and higher

When more than one Login Option is configured, and users connect with clients that support Multiple Login Options, users select a Login Option to use when they log in.

In the Mobile Access Portal, in the login page, users see a drop-down list with all available login options, shown by their Display Name.

In the Capsule Workspace mobile application, users select the Login Option on the first connection to the Security Gateway. On subsequent connections, the same login option is shown automatically.

# The Mobile Access Portal

## Security Gateway Portals

The Security Gateway runs different web-based portals over HTTPS:

- Gaia Portal
- Identity Awareness (Captive Portal)
- DLP portal
- Mobile Access Portal
- SSL Network Extender portal
- Reverse Proxy SSL portal
- Reverse Proxy Clear portal
- UserCheck portal
- Endpoint Security portals (CCC)

All of these portals can resolve HTTPS hosts to IPv4 and IPv6 addresses over port 443.

These portals (and HTTPS inspection) support the latest versions of the TLS protocol. In addition to SSLv3 and TLS 1.0 (RFC 2246), the Security Gateway supports:

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

Support for TLS 1.1 and TLS 1.2 is enabled by default, but can be disabled in SmartDashboard (for web-based portals) or Database Tool (GuiDBEdit Tool) (see sk13009) (for HTTPS Inspection).

**To configure TLS protocol support for portals:**

1. In **SmartDashboard**, open **Global Properties > SmartDashboard Customization**.
2. In the **Advanced Configuration** section, click **Configure**.

   The **Advanced Configuration** window opens.
3. On the **Portal Properties** page, set minimum and maximum versions for SSL and TLS protocols.

**To Configure TLS Protocol Support for HTTPS inspection:**

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

# Portal Settings

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.

## Portal URL

Remote users access the portal from a Web browser with https://<Gateway_IP>/sslvpn, where <Gateway_IP> is one of these:

- FQDN that resolves to the IP address of the Security Gateway
- IP address of the Security Gateway

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

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

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

**To change the Mobile Access Portal URL:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Settings**.
3. Change the **Main URL**.
4. Optional: 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.
5. Install policy.

# Portal Certificate

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 Security Gateway's management. All portals on the same IP address use the same certificate.

**To configure the accessibility settings for the portal:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Settings**.
3. Click **Import** to import a p12 certificate for the portal website to use.
4. Click **OK**.
5. Install policy.

# Portal Accessibility Settings

Configure from where users access the Mobile Access Portal. The options are based on the topology configured for the Security Gateway.

**To configure the accessibility settings for the portal:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Portal Settings**.
3. In the **Accessibility** area, click **Edit**.
   - **Through all interfaces**
   - **Through internal interfaces**
   - **Including undefined internal interfaces**
   - **Including DMZ internal interfaces**
   - **Including VPN encrypted interfaces** - Interfaces used for establishing route-based VPN tunnels (VTIs)
   - **According to the Firewall policy** - Select this if there is a rule that states who can access the portal.
4. Install policy.

# Portal Customization

**To customize the Mobile Access end user portal:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.

2. From the navigation tree, click **Mobile Access > Portal Customization**.

   The **Portal Customization** page opens.

3. Configure the following settings.
4. Install the policy.

# 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 Security Gateway in the **Portal Settings > Portal Customization page** to use these 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 the 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

**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 SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree, click **Portal Settings > Alternative Portal**.
3. Click **Add**.

The **Mobile Access Sign-In Home Page** window opens.

4. In the **User Groups** tab, specify user groups that may access the alternative user portal.
5. In the **Install On** tab, specify the Mobile Access Security Gateways and Clusters that host the alternative portal.
6. 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.
7. Click **OK**.
8. Click **Save** and then close SmartDashboard.
9. In SmartConsole, install policy.

# User Workflow for Mobile Access Portal

The user workflow includes these steps:

1. Sign in and select the portal language.
2. On first-time use, if you will use SSL Network Extender to access native applications, install ActiveX and Java Components.
3. Initial setup.
4. Access applications.

## Signing In

In a browser, type in the URL assigned by the system administrator for the Mobile Access Security Gateway.

**Best Practice** - Some popup blockers can interfere with aspects of portal functionality. Tell users to configure popup blockers to allow pop-ups from Mobile Access.

If the Administrator 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 Authentication Manager. After the remote users are authenticated, and associated with Mobile Access groups, access is given to corporate applications.

**Note** - If the Endpoint Compliance Scanner is enabled, users computers might be scanned before they can access the Mobile Access **Sign In** page. This is to make sure that credentials are not compromised by 3rd party malicious software.

# First Time Installation of ActiveX and Java Components

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

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

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

For general information about the Mobile Access Portal and Java compatibility see sk113410.

**Note** - To install using ActiveX after a component was installed using Java, delete the browser cookies.

# 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 Security 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.

# Endpoint Security on Demand

## 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 can make sure that the endpoint client has updated Anti-Virus software 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 Security Gateways, a combination of Endpoint Compliance Policy and Secure Workspace Policy can require the following Policy: Any client connecting to the Security 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 Security 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 Security 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 Security Gateway, users can be required to use Check Point Secure Workspace.
- To provide additional protection to an application, it is possible to "harden" the Endpoint Compliance protection that is enforced by the Security Gateway by assigning an Endpoint Compliance policy to a Protection Level, and then assigning that Protection Level to an application.

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 Security Gateway.

In either case, the scan takes place *before* logging in to the portal. Only one scan is performed. Compliance to policies is determined according to the results of the scan.

# Endpoint Compliance Policy Rule Types

There are different types of Endpoint Compliance policy rules, for different types of security applications. It is possible to have multiple rules of the same type, each with different settings.

## Windows Security Rule

Windows security rules perform Windows-specific checks. For example:

- Check for the latest Windows Service Pack on endpoint.
- Check the enabled/disabled state of the built-in Microsoft Windows Automatic Updates system.
- Check for Microsoft Windows Hotfixes and patches on the endpoint.
- Enforce Windows patches by their ID.

Endpoint computers running Windows must pass these checks in order to gain access to the network.

At least one of the Hotfixes in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

## Anti-Spyware Application Rule

Choose which Anti-Spyware applications endpoint computers (on the Windows platform) must have to gain access to the network.

Ensure that appropriate Anti-Spyware software is running on endpoint computers, and that the software version and virus signature files are up-to-date.

At least one of the Anti-Spyware applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Anti-Spyware enforcement rules are pre-configured with supported Anti-Spyware providers. To require a non-supported Anti-Spyware provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

## Anti-Virus Application Rule

Choose which Anti-Virus applications the endpoint computer must have in order to gain access to the network.

Ensure that appropriate Anti-Virus software is running on endpoint computers, and that the software version and virus signature files are up-to-date.

At least one of the Anti-Virus applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Anti-Virus enforcement rules are pre-configured with supported Anti-Virus providers. To require a non-supported anti-virus provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

## Firewall Application Rule

Choose which personal Firewall applications endpoint computers (on Windows, Linux or Macintosh platforms) must have to gain access to your network.

Ensure that appropriate Firewall software is installed, enabled and running on endpoint computers.

At least one of the Firewall applications in the rule must be active on the endpoint computer in order for the endpoint to be considered compliant and be granted access to the portal.

For convenience, Firewall enforcement rules are pre-configured with supported Firewall providers. To require a non-supported Firewall provider, use a custom check rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

## Custom Check Rule

Perform custom checks on endpoint computers (on the Windows, Linux or Macintosh platforms) that are not covered by any of the other rule types. For example:

- Custom applications. These applications may include proprietary spyware scanners that supplement the predefined types and/or other special security solutions.
- Specific files.

- Registry keys or processes running on the endpoint computer.
- Non-English or localized names of processes and files.

Custom check rules can be configured to check for specific versions and modification dates.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule, and the error message that is presented to users in the event of non-compliance, such as remediation information.

## OR Group of Rules

An "OR Group of Rules" rule includes a list of previously defined rules. An endpoint satisfies a rule of type "OR Group of Rules" if it satisfies one or more of the rules included in the "OR Group of Rules" rule.

The rules also specify the action to be taken if an endpoint computer fails to comply with a rule and the error message that is presented to users in the event of non-compliance, such as remediation information.

## Spyware Scan Rule

Select the action that should take place for each type of spyware present on endpoint computers. You can change the protections for types of spyware threats.

| Spyware Type | Description |
|---|---|
| Dialer | 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. |
| Worm | Programs that replicate over a network for the purpose of disrupting communications or damaging software or data. |
| Keystroke Logger | Programs that record user input activity (keystrokes or mouse activity). Some keystroke loggers transmit the recorded information to third parties. |
| Hacker Tool | Tools that facilitate unauthorized access to a computer and/or extraction of data from a computer. |
| Remote Administration Tool | Commercially developed software that allows remote system access and control. |
| Trojan | Malicious programs that masquerade as harmless applications. |

| Spyware Type | Description |
|---|---|
| Adware | 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. |
| Other | Any unsolicited software that secretly performs undesirable actions on a user's computer and does not fit any of the above descriptions. |
| Screen Logger | Software that record what a user's monitor displays. |
| Tracking Cookie | Cookies that are used to deliver information about the user's Internet activity to marketers. |
| Browser Plug-in | Software that modifies or adds browser functionality. Browser plug-ins change the default search page to a pay-per-search site, change the user's home page, or transmit the browser history to a third party. |

Endpoint Security on Demand. For example, you can allow that a signature that is recognized as spyware by Mobile Access, but which you see as legitimate.

In the rule, set the action to take if an endpoint computer fails to comply. Set the error message that users see in the event of non-compliance, such as remediation information.

# Endpoint Compliance Logs

If the end user machine is not compliant with one or more of the Endpoint Compliance policy rules, Mobile Access generates Endpoint Compliance-specific logs with the category "Endpoint Security on Demand". The log entries appear in SmartLog, and include the:

1. Rule ID and name that causes the authorization failure.
2. Policies that this rules belongs to.
3. A description in the "info" field of the log. Two logging levels are available to the administrator: (For configuration details, see the "Configuring Endpoint Compliance Logs" section.)

   **Note** - Mobile Access logs non-compliant rules from all policies, not only the Endpoint Compliance policy that is assigned to the Security Gateway or to an application. This means that there may be entries in SmartLog for rules that do not appear in the report presented to the end user.

   - **Summary**: Only one log entry per scan is written to SmartLog. The log entry shows endpoints that do not comply with the Endpoint Compliance policy. The date and time of the scan, the source IP, and the Endpoint Compliance scan ID are logged.

- **Details**: In addition to the Summary mode information, this adds a log entry for each non-compliant rule. For example, in the case of a Spyware Scan rule that screens for tracking cookies, a log entry is generated that contains the following fields:
  - Malware name: `unwantedexample`.
  - Malware type: `3rd party cookie`.
  - Description: `symptom type: URL. Symptom value: cookie:bob@unwantedexample.net.`

# Configuring Endpoint Compliance

The workflow for configuring Endpoint Compliance enforcement is below. Each step is described in detail in the sections that follow:

1. **Plan the Endpoint Compliance Policy**

   Decide on security clearance levels for Mobile Access Portals and applications. For example, is it OK for users to gain access to all Mobile Access applications as long as they comply with a single policy? If some resources are more sensitive than others, you may wish to draw up a more stringent policy for some applications than for others.

2. **Use the ICSInfo Tool**

   Set up a stand-alone test computer with all the endpoint security applications you want to create enforcement rules for, and the run the `ICSinfo` tool to obtain the information needed to correctly define Endpoint Compliance policy rules.

3. **Create Endpoint Compliance Policies**

   Policies are made up of rules. In order to comply with the policy, endpoints must comply with all rules in the policy. Rules can be used in more than one policy. Rules that are not in a policy are not used.

   There are different types of rules for different security applications. The Endpoint Compliance policy configuration tool comes with a number of predefined rules which can be edited to match the needs of the organization.

4. **Configure Endpoint Compliance Settings for Applications and Gateways**

   Configure which Endpoint Compliance Policies should be assigned to which applications and Security Gateways.

   - To make access to the *portal* conditional on passing an Endpoint Compliance scan, assign a policy to a Security 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 Security 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 Security Gateway and all applications accessed via the Security Gateway. In this approach, all applications accessed via the Security Gateway are protected by the Endpoint Compliance policy of the Security Gateway. Users whose client machines comply with the policy have access to the portal and all applications.

For example:

| Resource | Endpoint Compliance Policy |
|---|---|
| Security Gateway A | Low Security |
| Web App P | Rely on Security Gateway requirements |
| Web App Q | Rely on Security Gateway requirements |
| File Share R | Rely on Security Gateway requirements |

### 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 Security Gateway policy. To access the Mobile Access Portal, all users must fulfill the threshold security requirements of the Security 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:

| Resource | Endpoint Compliance Policy |
|---|---|
| Security Gateway A | Low Security |
| Web App P | Rely on Security Gateway requirements |
| Web App Q | High Security |
| File Share R | Rely on Security Gateway requirements |

### 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 Security 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:

| Resource | Endpoint Compliance policy |
|---|---|
| Security Gateway A | None |
| Web App P | Low Security |
| Web App Q | High Security |
| File Share R | Medium Security |

## Example Rules for Endpoint Compliance Policies

The following table illustrates Endpoint Compliance policies with different rules, for different security requirements.

| Rule | Description | High Security Endpoint Compliance Policy | Medium Security Endpoint Compliance Policy | Low Security Endpoint Compliance Policy |
|---|---|---|---|---|
| 1 | Default Windows Security rule | Yes | Yes | No |
| 2 | Anti-Virus applications check | Yes | Yes | Yes |
| 3 | Firewall applications check | Yes | Yes | Yes |
| 4 | Spyware Scan rule | Yes | No | No |

# 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 the ICSinfo tool 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 Security 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 configure Endpoint Compliance policies:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.

3. Click **Edit policies**.

   The Endpoint Compliance policy configuration tool opens at the **Policies** page.

4. Either create a new Endpoint Compliance policy or edit an existing policy.

   - To create an Endpoint Compliance policy click **New Policy**.

     The **Policies > New Policy** page opens.

   - To edit an existing policy, select the policy and click **Edit**.

     The **Policies > Edit Policy** page opens.

5. Give the policy a **Name**, and a **Description**.

6. For policies with Spyware Scan rules, if an endpoint computer has a valid Anti-Spyware of Anti-Virus application, make sure that the Endpoint Security on Demand Spyware Scan is necessary.

   If not, 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.

7. 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.

   - 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**.

8. Define the rules.

   **Note** - For explanations of fields in the Endpoint Compliance rules, see the online help.

9. Click **OK**.

   This takes you back to the Edit Policy or the New Policy page.

10. Click **OK**.

    This takes you back to the Policies page.

11. 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 polices.

12. Close SmartDashboard.
13. In SmartConsole, install the policy.

# Configuring Endpoint Compliance Settings for Applications and Security Gateways

**To configure Endpoint Compliance:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.

2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.
3. Click **Scan endpoint machine when user connects**.
4. Choose one of the available approaches:
   - Basic Approach - Configuring a Common Policy for the Portal and all Applications
   - Medium Approach - Configuring a Threshold Policy for the Portal, Hardened for Specific Applications
   - Advanced Approach - Configuring Individual Policies for Each Application

## Basic Approach - Configuring a Common Policy for the Portal and all Applications

**To assign a policy to the Security Gateway and require an Endpoint Compliance scan to connect to the Security Gateway:**

1. Click **Threshold policy to access any application via this gateway, the endpoint must comply with the following policy**.

2. From the drop-down list, select the Endpoint Compliance policy that is used for all applications accessed with this Security Gateway.
3. Click **OK**.

**To make sure that the applications use the Security Gateway settings for their Endpoint compliance:**

1. From the Objects Bar, click **Custom Application/Sites > Mobile Applications > Web Applications**.
2. Double-click the application.

   The Web Application settings window opens.
3. From the navigation tree, click **Additional Settings > Protection Level**.
4. Make sure that **This application relies on the security requirements of the gateway** is selected.
5. Click **OK**.
6. Repeat these steps for each application.
7. Install policy.
8. Configure the Endpoint Compliance logs.

## Medium Approach - Configuring a Threshold Policy for the Portal, Hardened for Specific Applications

**To configure the Security Gateway settings:**

1. Click **Threshold policy: to access any application via this gateway, the endpoint must comply with the following policy**.
2. From the drop-down list, select the default Endpoint Compliance policy to be used for applications accessed via this Security Gateway.
3. Click **OK**.

**To make sure that the applications use the Security Gateway settings for their Endpoint compliance:**

1. From the Objects Bar, click **Custom Application/Sites > Mobile Applications > Web Applications**.
2. Double-click the application that requires hardened endpoint security.

   The Web Application settings window opens.
3. From the navigation tree, click **Additional Settings > Protection Level**.

4. Click **This application has additional security requirements, specified by the following protection level**.
5. From the drop-down list, select a Protection Level for this application.

   To define a new Protection Level, click **Manage** and *"Mobile Access Applications" on page 55*.
6. Click **OK**.
7. Repeat these steps for each application.
8. Install policy.
9. Configure the Endpoint Compliance logs.

## Advanced Approach - Configuring Individual Policies for Each Application

**To configure the Security Gateway settings:**

1. In the **Endpoint Compliance** page of the Security Gateway, click **No threshold: to protect applications, configure endpoint compliance requirements individually per application**.
2. Click **OK**.

**To configure an individual policy for each application:**

1. From the Objects Bar, click **Custom Application/Sites > Mobile Applications > Web Applications**.
2. Double-click the application that requires hardened endpoint security.

   The Web Application settings window opens.
3. From the navigation tree, click **Additional Settings > Protection Level**.
4. Click **This application has additional security requirements, specified by the following protection level**.

   **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.
5. From the drop-down list, select a Protection Level for this application.

   To define a new Protection Level, click **Manage** and *"Mobile Access Applications" on page 55*.
6. Click **OK**.
7. Repeat these steps for each application.

8. Install policy.
9. Configure the Endpoint Compliance logs.

# Configuring Advanced Endpoint Compliance Settings

You can edit the Advanced Endpoint Compliance Settings to configure whether or not to allow access to the Security Gateway and applications if the Endpoint Compliance scanner is not supported on the endpoint operating system.

1. In SmartDashboard, from the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance** page.
2. Click **Edit**.

   The **Advanced Endpoint Compliance Settings** window opens.

   In this window you can decide whether or not to allow access to the Security 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.

## Platform-Based Bypass Per Protection Level

Configuring Endpoint Compliance Settings per Protection Level lets you set Platform-Based Bypass per application.

By default all Advanced Endpoint Compliance Settings are taken from the SmartDashboard configuration, in the Advanced Endpoint Compliance Settings page.

### Enabling Platform Based Bypass per Protection Level

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

```
cvpnd_settings set useICSRelaxedModeInProtectionLevel true
```

To return to the default setting, change `true` to `false` in the above command.

### Configuring the Protection Levels that are Bypassed

In the Mobile Access tab of SmartDashboard, under **Additional Settings > Protection Levels**, is a list of Protection Levels. From this page you can edit the Authentication and Endpoint Security settings that are required for applications assigned to each Protection Level. You can also create new Protection Levels.

In the Mobile Access application properties, assign a Protection Level to an application. For example, if you want to allow access to an application only if the user is compliant with Endpoint Compliance policy1, but you also need to accommodate the user connecting from an endpoint that does not support Endpoint Compliance scanning (such as an iPhone), then:

1. Create or use a Protection Level named ESOD_Relaxed_PL which enforces Endpoint Compliance Policy policy1.
2. Assign the Protection Level to the application.
3. Configure the Protection Level as "Bypassed".

   To configure different access permissions for various Protection Levels for Endpoint Compliance, from the Mobile Access CLI, in expert mode, run:

   ```
   cvpnd_settings listAdd ICSRelaxedModeProtectionLevelNames
   ESOD_Relaxed_PL
   ```

You can add other Protection Levels as well.

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

1. Run:

   ```
   cvpnd_settings listRemove ICSRelaxedModeProtectionLevelNames
   ```

2. Follow the on-screen instructions.

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

1. Restart the Mobile Access services by running `cvpnrestart`

   If the Mobile Access Security 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 in SmartLog, and have the category **Endpoint Security on Demand**. The Endpoint Security on Demand information is in the **info** field of the logs.

**To configure tracking options for the Endpoint Compliance scanner:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.
3. 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.
4. Select **Details** or **Summary** to determine the level of detail to record in the log file.
5. Click **Save** and then close SmartDashboard.
6. In SmartConsole, install the policy.

The Tracking options are:

- **Summary**: Only one log entry per scan is written to SmartLog. The log entry shows endpoints that do not comply with the Endpoint Compliance policy. The date and time of the scan, the source IP address, 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:
  1. Malware name: `unwantedexample`.
  2. Malware type: `3rd party cookie`.
  3. Description: `symptom type: URL. Symptom value: cookie:bob@unwantedexample.net.`

# Assign Policies to Security Gateways and Applications

**To assign policies to Security Gateways:**

1. On the **Endpoint Compliance** page, add all Mobile Access Security Gateways to the **Endpoint Security Settings on Mobile Access Security Gateways** section.
2. **Edit** each Security Gateway, whose access will be conditional on passing an Endpoint Compliance scan. Choose the **Threshold policy** and select **Scan the endpoint machine when a user connects**.

**To assign policies to applications:**

1. To make access to applications conditional on passing an Endpoint Compliance scan, assign a policy to a **Protection Level**.
2. Assign Protection Levels to **Mobile Access applications**.

# Excluding a Spyware Signature from a Scan

**To exclude a spyware signature from a scan:**

1. Configure Mobile Access so that endpoint computers must undergo an Endpoint compliance scan before they connect. The Endpoint Compliance policy must include a Spyware Scan rule.
2. Set up a stand-alone test computer that has the spyware to be excluded from the scan.
3. Run an Endpoint compliance scan on the test computer by connecting from it to Mobile Access.

   When Endpoint Security on Demand detects the spyware (irrespective of the action configured in the Spyware Scan rule), the name of the spyware (something like `Win32.megaspy.passwordthief`) is included in the report.
4. Make a note of the name of the spyware.
5. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
6. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance**.
7. Click **Edit Policies**.
8. Select the policy that is applicable to the clients, and click **Edit**.
9. Select the Spyware Scan rule from the list and click **Edit**.
10. In the **Software exception list** section, click **Add**.
11. Type the **Name** of the spyware, and a **Description**.
12. Click **OK** three times to close the Endpoint Compliance policy editor.
13. Click **Save** and then close SmartDashboard.
14. In SmartConsole, install policy.

# 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.

# 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 > the**Medium** setting, and then click **Advanced**.
7. Enable **Override automatic cookie handling** and in the **1st party cookies** section, enable **Accept**.
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.

The Endpoint Compliance Scanner is installed on the endpoint machine, by using ActiveX (for Windows with Internet Explorer), or *"The Mobile Access Portal" on page 179*.

**Note** - The Endpoint Compliance scan starts if Endpoint compliance is configured for a Mobile Access application in a portal, even if portal access does not require compliance with a policy.

**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 you are using the Endpoint Compliance scanner for the first time on a particular endpoint computer, you are prompted to download and install the Check Point Mobile Access Portal Agent.

   You may see these warnings:

   **1. Do you trust the Mobile Access site you are connecting to?**

   **2. Do you trust the certificate of the server of the Mobile Access site?**
3. During the scan, a progress bar is displayed.
4. If the endpoint computer successfully passes the Endpoint compliance scan, the Mobile Access Portal login screen appears.

   If the endpoint computer fails to pass the scan, Endpoint Security on Demand displays a result screen showing the potentially harmful software and security rule violations detected during the scan.

   - Click on a potentially harmful software item to display a short description of the detected malware, what it does and recommended removal method(s).
   - If the **Continue Anyway** button appears, you can continue and log on to the Mobile Access Portal without removing the malware or correcting the security rule violation.
   - If there is no **Continue Anyway** button, you must remove the detected malware or correct the security rule violation before you can log on to the Mobile Access Portal. When you have corrected the problem, click **Scan again** to repeat the scan.
5. When the Mobile Access Portal login page appears, you can log on normally.

**Note** - The user and administrator see the scan results as log entries in the Traffic Log. Each entry shows the user name, user group, source computer, malware name, malware type, and malware description.

# Using Endpoint Security on Demand with Unsupported Browsers

Endpoint Security on Demand for Mobile Access requires browsers that support ActiveX or Java.

The following sections describe Endpoint Security on Demand behavior when users attempt to access the Mobile Access Portal using an unsupported browser.

- If the **Block access to all applications** option on the Endpoint compliance scan **Policy** page is enabled, and *either* of the following conditions exist, the endpoint computer cannot connect to the Mobile Access Portal.
  - The **Prevent Connectivity** option is enabled for at least one malware protection rule.
  - The **Restrict** action is selected for at least one enforcement rule (anti-virus or custom).

    In this case, Endpoint Security on Demand presents an error message and generates a log entry in the administrator's traffic log.
- In all other cases, users can log on to the Mobile Access Portal without passing an Endpoint compliance scan. In some cases, an incompatibility message appears with a **Continue** button that allows users to proceed with Mobile Access login. Endpoint Security on Demand generates a log entry in the administrator's traffic log.
- When an application's Protection Level is configured to require an Endpoint Compliance scan, users can still gain access to the Mobile Access Portal, but cannot run that application.

### Preventing Portal Access with Unsupported Browsers

The following steps can prevent users using unsupported browsers from gaining access to the Mobile Access Portal and applications without passing an Endpoint Compliance scan:

- Enable the **Scan endpoint machine when user connects option**, and set a **threshold policy**. This setting is found on the **Endpoint Security on Demand > Endpoint compliance** page.
- Assign Protection Levels that require passing an Endpoint Compliance scan to all applications.
- Prevent users from using an unsupported browser to access the Mobile Access Portal by forcing Endpoint Security on Demand to reject all connections from unsupported browsers. See the "Configuring Advanced Endpoint Compliance Settings" section.

# Completing the Endpoint Compliance Configuration

The Endpoint Compliance page shows:

- Number of Mobile Access Security Gateways configured to scan endpoint machines.
- Security policy required on the Security Gateway.
- Number of Mobile Access applications, with Level of Enforcement (full, partial, or none).

If this is correct for your organization:

1. Click **Save** and then close SmartDashboard.
2. In SmartConsole, install 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. Secure Workspace users cannot access any applications, files, system tools, or other resources from the virtual workspace unless they are explicitly permitted by the Secure Workspace policy.

Administrators can easily configure Secure Workspace policy to allow or prevent activity according to enterprise requirements.

Secure Workspace creates an encrypted folder called **My Secured Documents** on the virtual desktop that contains temporary user files. It deletes this folder and all other session data when the session terminates.

After Secure Workspace is enabled, configure a Security Gateway to either require all users to connect to the Mobile Access Portal through Secure Workspace, or to give users the option of connecting through Secure Workspace or from their endpoint computers.

## Enabling Secure Workspace

**To enable Secure Workspace for an Mobile Access Security Gateway:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand > Secure Workspace**.
3. To configure the Secure Workspace policy, click **Edit policy**.

   For details, see the "Configuring the Secure Workspace Policy" section.
4. Click **Save** and then close SmartDashboard.
5. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

The Security Gateway window opens and shows the **General Properties** page.

6. From the navigation tree, click **Mobile Access > Check Point Secure Workspace**.
7. To enable Secure Workspace on the Security Gateway, click **This gateway supports access to applications from within the Secure Workspace**.
8. Select the options to define 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 lets you to set a rule that if a certain Endpoint Compliance policy is not satisfied by the client connecting to the Security Gateway, the client must use Secure Workspace. If the Endpoint Compliance policy is satisfied, using Secure Workspace is optional.
9. Select the Endpoint Compliance Policy that is enforced on the Security Gateway. If the criteria of the selected policy are not satisfied, the client connecting must use Secure Workspace.
10. Click **OK**.
11. In SmartConsole, install 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 Security Gateway and applications if Secure Workspace is not supported on the endpoint operating system.

To configure advanced operating system-specific settings, see sk34989.

## Configuring Platform-Based Bypass Per OS in Secure Workspace

If you want to let 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.

## 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 for Secure Workspace

1. Run:

   ```
   cvpnd_settings listRemove ISWRelaxedModeProtectionLevelNames
   ```

2. Follow the on-screen instructions.

**Finalize the Configuration for Secure Workspace**

1. Restart the Mobile Access services by running `cvpnrestart`.

   If the Mobile Access Security Gateway is part of a cluster, make the same change on each cluster member.

2. In SmartDashboard, assign the Protection Levels to the applications.

3. Install the policy.

# Applications Permitted by Secure Workspace

In its default configuration, Secure Workspace allows access to a limited group of applications. This is usually sufficient for most end-users working with the Mobile Access Portal and retrieving information from network hosts.

See sk114454 for the list of supported applications.

# 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 controls access to applications and directories on endpoint computers based on the Secure Workspace policy.

Each Mobile Access Security Gateway has its own 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.

You can add to the list of *Approved Applications*, and can add, edit, or delete applications from the list.

You can define locations where the application is allowed to save files that remain after Secure Workspace shuts down. These locations are called *Allowed Save locations*. There is no need to define locations for files that are not needed after Secure Workspace shuts down. Temporary files are deleted when the Secure Workspace is closed.

Secure Workspace includes a built-in Firewall that lets 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 to access 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.

# 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. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree, click **Endpoint Security on Demand** > **Secure Workspace**.

3. Configure the Secure Workspace policy, click **Edit policy**.

   The **Secure Workspace Settings** window opens.

4. Fill in the fields in the tabs described in the next sections.

## General Settings

### Self Protection

- **Enable Secure Workspace Self Protection** - Best Practice is to select this to add driver-level protection for Secure Workspace and prevent attempts to tamper with the environment.

  This requires administrative privileges and the User Access Control (UAC) prompt might show during the Secure Workspace startup.

  - **Prevent Secure Workspace startup if the Self Protection driver fails to install** - When selected, Secure Workspace can only start if the Self Protection driver is successfully installed.

### SSL Network Extender

- **Allow SSL Network Extender connections only from within Secure Workspace** - Select this option to use corporate resources from within Secure Workspace only. Use this if your organizational security policy requires access to corporate resources from within a clean, segregated environment, and with a strict set of allowed applications.

### Data Protection

- **Prevent the host PC from printing secure documents** - Users cannot print documents from Secure Workspace.
- **Prevent copying clipboard content to the host PC** - Users cannot copy content from inside Secure Workspace to paste or save it outside of Secure Workspace.

## Application Control Settings

- **Enable Reputation Services to validate the integrity of allowed applications in the Applications Table** - When a user starts an application that is not an Approved Application, Secure Workspace contacts Check Point Reputation Services to ask if the application is legitimate. Reputation Services 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 Reputation Services responses:
  - **Allow Trusted only**
  - **Allow Trusted and Unknown**

### Application Table

Approved applications show on the Secure Workspace desktop, and are allowed to run on endpoint computers. You can add, edit, or remove applications from the list.

### Configuring Applications in the Application Table

- To add an application: Click **Add Application**.
- To remove an application: Click **Remove**.
- To edit the information for the application: Click the application **Display Name** in the table.

### When you add a new application or edit an application, you can include this information:

- **Display Name** (required)- The name of the approved application as it shows on the desktop.
- **Executable File** (required) - The path and filename for the application selected. .

  Enter the path in one of these formats:
  - Absolute path in this format: `<disk>:\<folder_path>\<binary_name>`. Secure Workspace allows the endpoint to run the binary from specified location only. The full path is necessary 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 all locations on the disk. Use if the location appears in the PATH.
  - Path with environment variable, for example: `<path_with_env_variable>\<binary_name>`. Secure Workspace resolves the environment variable on the endpoint, and uses its value as part of the path to the executable.

- **Executable Original File Name** (optional) - Enter this if you also select an **Executable Vendor Name**, so Secure Workspace can make sure that the application certificate meets the requirement. The original filename shows in the details of the application's certificate.
- **Executable Vendor Name** (optional) - When a vendor is selected, Secure Workspace checks the application's certificate to make sure that it is signed by this vendor. The same application is blocked with a different vendor.
- **File hash** (optional) - Enter the MD5 or SHA256 signature of the application. You can add multiple hashes, for example, one for each version of the application.
- Select the hash type that you use: **MD5** or **SHA256**.
- **Comment** (optional) - Add a comment that describes the application.
- **Add shortcut to Start Menu** (optional) - Select to add 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. You can also enter a command line argument to run as a shortcut.
- **Add shortcut to Desktop** (optional) - Select to add a shortcut to the application to the Desktop in Secure Workspace. The shortcut is only added if the application exists on the client computer. You can also enter a command line argument to run as a shortcut.

## Vendor Control Settings

You can configure which applications users can access from Secure Workspace. If a vendor is trusted then all applications from this vendor are trusted. See sk114526 for the vendors trusted by default. You cannot add a vendor to the list.

- To block a vendor: Clear the checkbox for the vendor.
- To allow a vendor: Select the checkbox for the vendor.

## Allowed Save Locations

**Allowed Save locations** are locations where applications are allowed to save files that remain after Secure Workspace shuts down. There is no need to define locations for temporary files that can be deleted after Secure Workspace shuts down.

**To add an allowed save location:**

1. In the **Allowed Save locations** tab, click **Add Location**.
2. In the window that opens enter:

- **Name** - A descriptive name of the location.
- **Path** - The complete path to the location.
- **Description** (optional) - A longer description.

3. Click **Save Location**.

## Outbound Firewall Rules

Outbound Firewall Rules define which IP addresses and ports approved applications are allowed to access when they make outbound connections.

These options are available:

- **Localhost Connection. Do not allow connection to application on host PC** - When selected Secure Workspace users can only use applications in Secure Workspace and cannot access the host PC. When cleared, users can access the host PC when Secure Workspace is active, but can only save things in the defined locations.
- **Accept Rules** - Select a rule in the table to enable it. Clear a rule in the table to disable it. Only connections that match enabled rules are allowed. The default rules are:
  - **Everywhere** - Allows desktop applications to access all addresses and ports.
  - **Localhost connection** - Required for Internet Explorer. Not recommended to delete.

Best practice is to use the default rules. You can delete the default rules and replace them with more restrictive rules, but do so carefully.

## Virtual Registry Rules

You can add custom rules to the Secure Workspace virtual registry. Contact Check Point support for more information about this feature.

## User Experience Settings

In the User Experience settings, configure what users see and how they interact with Secure Workspace.

### General

- **Prevent Host PC/ Secure Workspace desktop switching** - Users cannot switch between the host PC and Secure Workspace environments. Access to the regular desktop is only allowed if Secure Workspace is closed.
- **Display welcome window** - When selected, "Welcome to Secure Workspace" is shown to users. Select if it always shows or if users can disable it.

- **Disable "Run" option in Start menu inside Secure Workspace** - Users cannot run programs with the **Run** command from the Start menu in Secure Workspace.
- **Hide all system drives** - Local drives are hidden when in Secure Workspace.
- **Prevent to start browser inside Secure Workspace** - Disable the automatic launch of an internet browser in Secure Workspace after Secure Desktop is started. As a result SSL Network Extender does not start and automatically establish a VPN tunnel.

**Desktop Background** - Change the Secure Workspace desktop background picture and its position.

**Display Start dialog** - Show a Start window that you customize.

### Configuring a Secure Workspace Policy per Security Gateway

A Secure Workspace policy that is configured in SmartDashboard applies to all Mobile Access Security Gateways. To configure a Secure workspace policy for each Security Gateway, see sk34939.

## Integration with Endpoint Security Reputation Service

Secure Workspace can work together with the Check Point Endpoint Security Reputation Services to check whether an application that is not an approved application is legitimate. Reputation Services identifies programs according to their filename and MD5 hash.

For details of the Endpoint Security Reputation Services, see your version of the *R80.40 Harmony Endpoint Security Server Administration Guide*. If you use Reputation Services, the sequence of Secure Workspace is:

1. The 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 Reputation Services about the program.
4. Reputation Services returns one of three responses about the application: Trusted, Untrusted, or Unknown.
5. Secure Workspace allows or blocks the application according to the Reputation Services responses, as defined in the policy:
   - **Allow Trusted only**.
   - **Allow Trusted and Unknown**.

## Secure Workspace End-User Experience

This section provides an overview of the Secure Workspace workflow.

## Disabling Internet Explorer Protected Mode

If users use Internet Explorer to open the Mobile Access Portal on Windows Vista or higher, they must disable Internet Explorer Protected Mode. If Protected Mode is not disabled, SSL VPN might run, but they can have unexpected errors.

On Windows 7 and higher, protected mode is enabled by default. You can see that it is enabled:

- In the **Internet Options** > **Security** tab. See that **Enable Protected Mode** is selected.
- In the bottom right of the Internet Explorer browser window, it says **Protected Mode On**.

If Endpoint Security on Demand is configured on the Security Gateway, the scan detects that Protected mode is on and instruction to disable Protected Mode open.

If Endpoint Security on Demand is not configured on the Security Gateway, users are not alerted that they must disable Protected Mode. However they must do the same steps to disable Protected Mode so that they can access the SSL VPN portal without problems.

### To disable Protected mode for the SSL VPN Portal:

In Internet Explorer, select **Tools** > **Internet Options**.

1. In the **Internet Options** window, select the **Security** tab.
2. In the **Security** tab, select **Trusted Sites** and clear the **Enable Protected Mode** checkbox.
3. Click **Sites**.
4. In the **Trusted sites** window:
    a. Click **Add**.
    b. In **Add this website to the zone**, enter the web address of the SSL VPN portal.

       The portal web address shows in the **Websites** area of the window.
5. Click **Close**.
6. Click **OK**.

All users must do these steps even if they do not get the instructions automatically. After these steps, close all Internet Explorer windows. The next time you open Internet Explorer, Protected Mode is off.

## Logging on to the Mobile Access Portal Using Secure Workspace

Secure Workspace initializes when a user logs on to the Mobile Access Portal. If the administrator has configured the Mobile Access Security Gateway to require Secure Workspace, this occurs automatically. If the administrator has configured the Security Gateway to allow users to choose whether or not to use Endpoint Security on Demand, an option appears on the Login screen.

## 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 Security Gateway to "real" desktop folders. Conversely remote users may need to upload files to the corporate network from the endpoint computer.

To allow this, the administrator must configure the Secure Workspace policy to allow endpoints to switch between the secure and regular desktops. This is accomplished in the **User Experience Settings** section of the Secure Workspace policy editor.

### Accessing Files and Applications on the Endpoint Computer

Generally, users can access files and run applications in Secure Workspace in the same manner as on the "real" desktop. Since, by default, users have read-only (access) privileges to all folders and files, they can freely navigate the file system using Windows Explorer. When attempting to run a program or open a file for which a user does not have Secure Workspace permission, an error message appears.

Likewise, if a user attempts to save a file to a "real" desktop folder without Secure Workspace permissions, an error message appears.

## Accessing Endpoint Applications in Secure Workspace

When SSL Network Extender *network mode* users initiate a Secure Workspace session, permitted Endpoint Applications are available in the virtual desktop as follows:

| An Endpoint Application defined in the Native Application as... | ... is available to Users as a |
|---|---|
| Path and executable name (already installed) | Shortcut in the Windows **Start** menu. |
| Runs via default browser | Shortcut on the desktop. |
| Downloaded-from-Mobile Access application | Link in the Mobile Access Portal. |

**Note** - During a Secure Workspace session, SSL Network Extender cannot toggle between the Network Mode and the Application Mode. User can change the mode, but must start a new Secure Workspace session after doing so.

### Switching Between Secure Workspace and the "Real" Desktop

You can switch back and forth between the Secure Workspace virtual workspace and the "real" desktop at any time. To do so, click the lock icon, located in the tray area of the taskbar.

### Exiting Secure Workspace

To exit Secure Workspace:

1. From the Windows **Start** menu, select **Close Secure Workspace**.

   A confirmation and reminder to save open files appears.

2. Click **Yes, close it now** to continue closing Secure Workspace.

## Troubleshooting Secure Workspace

Secure Workspace logs are automatically saved in `%temp%\IswTmp\Logs` when the environment variable `ISWLOG` is set to 0 (zero). If you have issues with Secure Workspace, you can examine these logs or send them to Check Point technical support.

If an application stops working, a Secure Workspace window opens to help you send technical information to Check Point. Users can manually open this window if a process hangs or they experience instability.

**To collect technical information:**

1. Press Ctrl+Alt+End.

   A Secure Workspace window opens to help you send technical information to Check Point.

2. Fill in the required information and click **Collect and Send**.
3. Send the file to Check Point support.

# 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. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.

2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance Updates**.

3. In the **Update Configuration** section, click **Configure**.

   The **Automatic Updates** window opens.

4. On the **Activation** tab, click **Enter User Center credentials**.

5. Enter your User Center email address and password.

6. Click the **Endpoint Security on Demand** tab.

7. Configure these update settings:

   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.

8. In the **Tracking Configuration** tab, select the various tracking options from the lists. You can select logging events or a variety of alert types.
9. 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).
10. Click **OK** to complete the definition.
11. Click **Save** and then close SmartDashboard.
12. In SmartConsole, install policy.

# Performing Manual Updates

**To perform a manual Endpoint Security on Demand update:**

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Endpoint Security on Demand > Endpoint Compliance Updates**.
3. Click **Update Databases Now**.
4. Enter your Check Point User Center credentials and click **Next**.
5. Choose the **All supporting gateways** option to download to all available Mobile Access Security Gateways. Alternatively, choose the **Select** option to select specific Mobile Access Security Gateways for update, and then select the applicable Mobile Access Security Gateways in the left-hand list and then click **Add**.
6. Click **Finish**. A progress bar appears during the download.
7. Click **Save** and then close SmartDashboard.
8. In SmartConsole, install policy.

# Advanced Password Management Settings

If your organization uses Microsoft Active Directory (AD) to manage users, you can use these password settings allow continuous remote access for your users.

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

# Password Expiration Warning

Administrators can configure SmartDashboard to tell users to change their passwords before they expire. This is an efficient way to ensure that users have continuous access to resources. See sk33404.

# 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 Security Gateways R71 or higher. Make sure that the LDAP server is configured to work with LDAP over SSL.

**To enable password change after expiration:**

1. In SmartDashboard, select **Global Properties > User Directory (LDAP)**.
2. Under **User Directory (LDAP) Properties**, select **Enable Password change when a user's Active Directory password expires**.
3. In the **LDAP Account Unit Properties** window, make sure the assigned **Profile** is **Microsoft_AD**.

4. Make sure that the Login DN for the LDAP server, as configured in SmartDashboard, has sufficient permissions to modify the passwords of Active Directory users.
5. In the LDAP Server Properties window in the **Encryption** tab, select **Use Encryption (SSL)**.
6. If the LDAP schema of the Active Directory is not extended with Check Point's LDAP schema, use Database Tool (GuiDBEdit Tool) (see sk13009) to make these changes:
   - Select **Managed Objects > LDAP > Microsoft_AD > Common**
   - Find `SupportOldSchema` and change its value to `1`

For more about LDAP and user management, see the *R80.40 Security Management Administration Guide*.

# Session Visibility and Management Utility

## Introduction to Session Visibility and Management

When the Session Visibility and Management Utility is enabled, each time a user connects remotely to an R77.30 or higher Security Gateway, the data is recorded in an SQL database.

You can run queries on this database with the Session Visibility and Management Utility.

You can use the Utility to:

- Show session information based on constraints
- Terminate user sessions based on constraints

The main commands are described below. You can also edit the configuration XML file to create custom commands. See sk104644 for advanced configuration.

These Check Point clients are fully supported with the Session Visibility and Management Utility:

- Capsule Workspace for iOS and Android
- Mobile Access Portal with SSL Network Extender (Application and Network modes)
- Remote Access VPN as part of the Endpoint Security Suite
- Remote Access clients: Endpoint Security VPN, Check Point Mobile for Windows, SecuRemote

These clients are supported but sessions on them cannot be terminated:

- Capsule Connect
- Capsule VPN
- Windows 8.1 Check Point VPN Plugin

# Enabling the Utility

By default the Session Visibility and Management Utility is disabled.

**To enable or disable the Session Visibility and Management Utility:**

1. For SecurePlatform only, run on the Security Gateway this long command:

   ```
   $CVPNDIR/bin/cvpnd_settings $FWDIR/conf/sessionIS.C set
   "database_conf:dataDir" "/var${FWDIR}/datadir/postgres/sessions"
   nobackup ; chown cp_postgres
   /var$FWDIR/datadir/postgres/sessions/postgresql.conf
   ```

2. To enable: On the Security Gateway, run: `RAsession_util on`

   To disable:On the Security Gateway, run: `RAsession_util off`

3. Run: `cpstop`
4. Run: `cpstart`
5. In a cluster environment, make the change on all cluster members.

# Seeing the Number of Open Sessions

**To see the number of sessions open at a given time:**

```
RAsession_util show sessions_num
```

# Disconnecting Remote Access Users

**To disconnect a user:**

```
RAsession_util terminate {all | byuser <user> | bysession_id <id> |
custom <SQL constraint>}
```

| Parameter | Description |
|---|---|
| `all` | Disconnect all Remote Access users |
| `byuser` | Disconnect a user by user name |
| `bysession_id` | Disconnect the session with the given session ID |
| `custom` | Disconnect users that match an SQL constraint |

**Examples:**

```
# RAsession_util terminate all
```

```
# RAsession_util terminate byuser james_wilson
# RAsession_util terminate bysession_id 521bd4788
# RAsession_util terminate custom "src_ip='1.1.1.1'"
```

# Seeing User Data

**To see data of connected users:**

`RAsession_util show users {all | byname <user_name> | where <where_clause>}`

| Parameter | Description |
|---|---|
| `all` | Show all users |
| `byuser` | Show data of the given user name |
| `where` | Show users by constraint |
| `certs` | Show user certificates by constraints |

**Examples:**

```
# RAsession_util show users all
# RAsession_util show users byuser "james_wilson"
# RAsession_util show users where "client_name='Mobile Access Portal'"
```

(This command shows all the users connected from the Mobile Access Portal.)

# Using Constraints

To disconnect or see data of users that match a non-default definition, use constraints. First, become familiar with the Check Point scheme for Remote Access sessions. Then, use the field names or types to run a `terminate` or `show users` command on matching users.

**To see valid constraint fields:**

`RAsession_util show scheme`

**Examples:**

This command shows the given fields where the client is the **Mobile Access Portal**, and the results are ordered according to the **creation time**:

```
RAsession_util show custom -FIELDS "session_id,user_name,client_
name,browser_name,machine_name,os_name" -WHERE "client_name='Mobile
Access Portal'" -ORDERBY "creation_time"
```

This command shows the given fields where the client type is **Capsule Workspace**:

```
RAsession_util show custom -FIELDS "user_name,sessionid,client_
ver,client_build_number,os_name,os_ver,device_type" -WHERE "client_
name='Capsule Workspace'"
```

# Session Visibility and Management Commands

### SCHEME

**Description:** Shows the table scheme of the database.

**Usage**: SCHEME

**Parameters:** None

### SESSION_OP

**Description**: Performs an operation on a session or session based on the defined constraints.

**Usage**: SESSION_OP <Operation_type> <Sql_constraint [list_of_parameters]>

**Parameters**:

| Parameter | Description |
|---|---|
| Operation_ type | Type of operation to perform on sessions. Only `terminate` is supported in this release. |
| Sql_ constraint | Criteria to select the sessions on which to perform the operation. For example, "username='aa'". It can also be a parametric SQL "`WHERE`" clause that includes $ signs instead of values, for example, `"username=$1 and srcip=$2"`. The "`WHERE`" clause means that the first parameter in the `List_of_parameters` will be placed instead of $1, and the second will be as $2. |
| List_of_ parameters | Can be empty or list of parameters to be placed instead of the $ signs in the "`WHERE`" clause. |

**Examples**:

```
SESSION_OP terminate "username='James Wilson'"
```

```
SESSION_OP terminate "username=$1 and srcip=$2" "James
Wilson,192.0.2.10"
```

### SELECT

**Description**: Run a query on the sessions table.

**Usage**: `SELECT <-FIELDS <fields>> [-WHERE <where_clause> [list_of_parameters]] [-GROUPBY <group_by_fields>] [-ORDERBY <order_by_fields>] [-LIMIT <limit_size> [-OFFSET <offset_number>]]`

**Parameters**:

| Parameter | Description |
|---|---|
| FIELDS <fields> | FIELDS flag with list of fields to select delimited by ",". |
| WHERE <where_clause> | WHERE flag with the SQL WHERE clause.<br><where_clause> can also include $ signs instead of values, for example, "username=$1 and srcip=$2". This where_clause means that the first parameter in the "List_of_parameters" will be placed instead of $1, and the second will be as $2 . |
| List_of_parameters | Can be empty or list of parameters to be placed instead of the $ signs in the WHERE clause. |
| GROUPBY <group_by_fields> | GROUPBY flag with list of fields to group by delimited by ",". |
| ORDERBY <order_by_fields> | ORDERBY flag with list of fields to order the result by delimited by ",". |
| LIMIT <limit_size> | LIMIT flag with the limit size. |
| OFFSET <offset_number> | OFFSET flag with the result offset. |

**Example**:

```
SELECT -FIELDS "login name,clientname,sessionid" -WHERE
"loginname='aa'" -ORDERBY "clientname"
```

# Reverse Proxy

You can configure a Mobile Access Security Gateway to be a reverse proxy for Web Applications on your servers. Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Then the Security Gateway passes the request to an internal server, based on the Reverse Proxy rules. This lets external clients access resources on internal servers, while the internal addresses of the servers are hidden.

Configure the reverse proxy with rules that:

- Map the external addresses of the internal servers to their real network addresses.
- Give permission to external clients to access specified resources on the servers.
- Define if the connections between users and resources use HTTP or HTTPS.

By default, reverse proxy is disabled. Enable and configure it in the CLI.

# Configuring Reverse Proxy

In CLI, you can:

- Enable or disable reverse proxy.
- Show the reverse proxy rules and applications.
- Add a new rule or an application.
- Edit an existing rule.
- Delete a rule.
- Apply reverse proxy rule configuration changes.

**Note** - After each change in the Reverse Proxy rules that you make in the CLI, you MUST run this to apply the changes: `ReverseProxyCLI apply config`

### Syntax

```
ReverseProxyCLI {on | off | show {rules|applications} | add {rule
<rule_name> | application <app_name> {capsule_docs | outlook_
anywhere} <ext_hostname> <int_hostname>} | edit rule <rule_name> |
remove rule <rule_name> | apply config}
```

### Parameters

| Parameter | Description |
|---|---|
| `on` | Enable the reverse proxy. |
| `off` | Disable the reverse proxy. |
| `show {rules\|applications}` | Show the reverse proxy rules and applications. |
| `add {rule <rule_name> \| application {capsule_docs \| lync \| outlook_anywhere} <ext_hostname> <int_hostname>}` | Add a reverse proxy rule or application.<br>The **Add** rule command runs in interactive mode. Select actions as prompted. Note that for external hostname and internal hostname, when you enter the URL, you can specify:<br>■ The protocol: http or https<br>■ The internal port<br>The **Add** application command adds a set of one or more reverse proxy rules that allows access to supported internal applications. The supported applications are: Outlook Anywhere and Capsule Docs. |
| `edit rule <rule_name>` | Edit a reverse proxy rule. This command option runs in interactive mode. Select actions as prompted. |
| `remove rule <rule_name>` | Delete a reverse proxy rule. |
| `apply config` | Apply the reverse proxy configuration changes.<br>**Note** - To apply reverse proxy rule configuration changes, you must run the apply command at the end of each configuration session. |

### Important Notes:

- The external ports allowed through the reverse proxy are 80 and 443. All internal ports are allowed.
- If the Gaia Portal of the Mobile Access Security Gateway is:

  `https://<IP Address of Security Gateway>/` with a "/" at the end, you MUST change either the URL or the port.

  For example, change the URL one of these:

- `https://<IP Address of Security Gateway>/gaia`
- `https://<IP Address of Security Gateway>:4434`

**To change the Gaia Portal URL:**

1. In the Security Gateway object, click **Platform Portal**.
2. Change the **Main URL**.
3. Click **OK**.
4. Install policy.

If you do not change either the URL or the port, the Gaia Portal is not accessible.

For complete examples and advanced CLI and XML configuration, see sk110348.

# Troubleshooting Reverse Proxy

You can troubleshoot the reverse proxy through standard Check Point monitoring tools, such as SmartLog.

**Note** - The destination is not shown in logs.

For advanced troubleshooting instructions, contact Check Point Technical Support.

**To configure reverse proxy to send traffic logs:**

1. In SmartDashboard > **Mobile Access** tab, go to **Additional Settings** > **Logging**.
2. In the **Tracking** area, select **Log Access for Web Applications**, and select one of the events to log:
   - **Unsuccessful access events** (Denied and Failed logs)
   - **All access events** (Allowed, Denied and Failed logs)
3. Install Policy.

The logs are available in SmartLog > **Mobile Access logs**.

**Identify Reverse Proxy logs by these criteria:**

- **Category**: Mobile Access
- **Application**: Reverse Proxy

The **Access** section of the log can show:

- **Allowed - Authorized URL** - The Reverse Proxy allowed the URL request (only shows if the **All access events** logging option is configured).

- **Denied - Unauthorized URL** -The Reverse Proxy blocked the URL request. If this is a mistake, you can allow the URL.

  To allow a blocked URL:

  - In the command line, run: `ReverseProxyCLI show rules`
  - Look in the relevant rule in the **Paths** column, find the path that is unauthorized in the log, and add the path that was blocked to the rule.

- **Failed** - The Reverse Proxy failed to forward the request for the Endpoint Security Management Server with one of these messages:

  - **Internal Server Error** - The internal server aborted the connection with the Security Gateway. Make sure the server is up and running.
  - **Proxy not found** -The given proxy host could not be resolved.
  - **Can't resolve host name** - The `<internal_host>` configured in your application or rule cannot be resolved.

    You can see it in the **Internal Server** column with one of these commands:

    - `ReverseProxyCLI show applications`
    - `ReverseProxyCLI show rules`

    Make sure that this hostname can be resolved from the Security Gateway.

    To do this, run `nslookup` on the host to see that the Security Gateway can resolve it.
  - **Internal host connection failed** -Failed to connect to the internal server, make sure the server is up and running.
  - **Invalid URL** -The URL from the Security Gateway to the internal server was not formatted correctly.
  - **SSL handshake failed** -A problem occurred somewhere in the SSL/TLS handshake between the Security Gateway and the internal server.
  - **Server response was too slow** - Operation timeout
  - **Page not found**

**To turn on debugging for reverse proxy:**

1. In the `/opt/CPcvpn-R80.40/conf/ReverseProxy_conf/httpd_common.conf` file, find the parameter `ReverseProxyHandlerTraceLog`, and change its value from **Off** to **On**.

   See the reverse proxy trace logs in:

   `/opt/CPcvpn-R80.40/log/trace_log/`

2. For HTTPS:

   In the `/opt/CPcvpn-R80.40/conf/ReverseProxy_conf/httpd_ssl.conf` file, find the parameter `LogLevel`, and change its value from **emerg** to **debug**.

   See the log files for HTTPS:

   `$CVPNDIR/log/reverseproxy_ssl_debug_log`

3. For HTTP:

   In the `/opt/CPcvpn-R80.40/conf/ReverseProxy_conf/httpd_clear.conf` file, find the parameter`LogLevel`, and change its value from **emerg** to **debug**.

   See the log files for HTTP:

   `$CVPNDIR/log/reverseproxy_debug_log`

**To enable cvpnd logs:**

1. Run: `cvpnd_admin debug set TDERROR_ALL_ALL=5`
2. See the logs in: `$CVPNDIR/log/cvpnd.elg`

To disable, run: `cvpnd_admin debug off`

**To make sure that reverse proxy processes are running:**

1. Run: `ps -ef | grep httpd`
2. In the output, find:
   - For HTTPS:

     `ReverseProxySSL/httpd.conf`
   - For HTTP:

     `ReverseProxyClear/httpd.conf`

# Reverse Proxy Known Limitations

- Not supported at this time:
  - No GUI (SmartDashboard).
  - No Access control on user level.
  - No granularity of networks or interfaces.
  - No link translation on sites returned with Reverse Proxy.

- If the Mobile Access policy contains applications configured with the Host Translation link translation method, the host names in these applications must be different from the names of the hosts in the communication through the Reverse Proxy.
- Reverse proxy has one certificate for SSL termination. To support multiple web servers over HTTPS, the certificate must be a wild card certificate, or it must use Subject Alternate Names (SAN).
- Lync (Skype for Business) is not supported.
- When you configure reverse proxy on cluster, the rules are not synchronized automatically between members.

  **Best Practice** - Use `ReverseProxyCLI` to add all rules to one member, and then synchronize the rules with the other members.

  To synchronize reverse proxy rules between Cluster Members:

  1. In the `$CVPNDIR/conf/ReverseProxy_conf/` directory, copy this file from the configured Cluster Member to other Cluster Members:

     ```
     $CVPNDIR/conf/ReverseProxy_conf/ReverseProxyConf.xml
     ```

  2. Apply the configuration on each member.

     Run:

     ```
     ReverseProxyCLI apply config
     ```

# Mobile Access Blade Configuration and Settings

## Interoperability with Other Software Blades

The Mobile Access Software Blade is fully integrated with the other Software Blades. Any Security Gateway running on SecurePlatform or Gaia with the Firewall blade enabled can also have the Mobile Access blade enabled.

Most Network objects, Resources, and Users created in SmartDashboard also apply to Mobile Access and can be used when configuring Access to Applications. Similarly, any Network objects, Users and User Groups that you create or modify in Mobile Access appear in the SmartDashboard navigation tree and are usable in all of the SmartDashboard applications.

## IPS Blade

When you enable Mobile Access on a Security Gateway certain IPS Web Intelligence protections are activated. The settings of these protections are taken from a local file and are not connected to the IPS profile. These IPS protections always apply to Mobile Access traffic only, even if the Security Gateway does not have the IPS blade enabled.

### Disabling Protections for Advanced Troubleshooting

You should only disable the Mobile Access Web Intelligence protections for advanced troubleshooting.

**Important** - We do not recommend that you deactivate these protections because of potential security risks to the Security Gateway while the protections are off.

**To disable the local Web Intelligence protections:**

1. Backup the `$CVPNDIR/conf/httpd.conf` configuration file.
2. Edit `$CVPNDIR/conf/httpd.conf` by deleting or commenting out this line:

   `LoadModule wi_module /opt/CPcvpn-<current version>/lib/libModWI.so`

   Where <*current version*> is the Check Point version installed. For example, R77.20.

## Changing to an IPS Profile Configuration for Mobile Access

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

### To change to a Security Gateway IPS profile configuration for Mobile Access instead of the local configuration:

1. Edit the IPS profile assigned to the Security Gateway to include all of the protections listed in the "IPS Protections Crucial for Mobile Access" section.
2. From the CLI, run:

   ```
   cvpnd_settings set use_ws_local_configuration false
   ```
3. When prompted, backup the `$CVPNDIR/conf/cvpnd.C` file.
4. Restart the Check Point processes. Run: `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. Run: `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.

| Protection Name | In Recommended_Protection Profile? |
|---|---|
| HTTP Format Sizes | yes |
| HTTP Methods | yes |
| ASCII Only Request | yes |
| General HTTP Worm Catcher | yes |

| Protection Name | In Recommended_Protection Profile? |
|---|---|
| Directory Traversal | yes |
| Cross-Site Scripting | no |
| Command Injection | yes |
| Header Rejection | yes |
| Malicious Code Protector | no |
| Non Compliant HTTP | yes |

# Anti-Virus and Anti-Malware Blade

Certain Anti-Virus settings configured for a Security Gateway in the **Traditional Anti-Virus > Security Gateway > HTTP** page of the **Threat Prevention** tab also apply to Mobile Access traffic. To activate traditional Anti-Virus protection, enable the **Traditional Anti-Virus** on the Security Gateway.

These settings apply to Mobile Access traffic when **Traditional Anti-Virus** is configured to scan traffic **By File Direction**:

- **Incoming files arriving to** - Inspects traffic that Mobile Access users upload to Mobile Access. (The drop-down menu is not relevant.)
- **Outgoing files leaving** - Inspects the traffic that Mobile Access users download from Mobile Access. (The drop-down menu is not relevant.)
- The **Internal Files** field is not relevant since Mobile Access uses an external interface.
- **Exceptions** are not supported.

If **Traditional Anti-Virus** is configured to scan traffic **By IPs**, all portal traffic is scanned according to the settings defined for the Mail, FTP and HTTP protocols in SmartDashboard.

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

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

## Enabling Traditional Anti-Virus

The Anti-Virus blade and Traditional Anti-Virus can be activated on Security Gateways in your system.

**Note** - You cannot activate the Anti-Virus blade and Traditional Anti-Virus on the same Security Gateway.

**To configure Traditional Anti-Virus:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Other > More Settings > Enable Traditional Anti-Virus**.
3. Click **OK**.
4. Define rules in the Access Control Policy to allow the specified services. Anti-Virus scans only accepted traffic.
5. From **Anti-Bot and Anti-Virus** tab > **Traditional Anti-Virus**, select the services to scan using these options:
   a. From the **Database Update** page, configure when to perform automatic signature updates or initiate a manual signature update.
   b. From the **Security Gateway** > **Mail Protocol** page, configure Anti-Virus scanning options for **Mail Anti-Virus**, **Zero Hour Malware**, **SMTP**, and **POP3** services.
   c. From the **Security Gateway** > **FTP** page, configure FTP traffic scanning options.
   d. From the **Security Gateway** > **HTTP** page, configure HTTP traffic scanning options.
   e. From the **Security Gateway** > **File Types** page, configure the options to scan, block or pass traffic according to the file type and configure continuous download options.
   f. From the **Security Gateway** > **Settings** page, configure options for file handling and scan failures.

# IPsec VPN Blade

The IPsec VPN blade and Mobile Access blade can be enabled on the same Security 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 Security Gateways R71 and higher. 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 Security 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 Security 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.

# Concurrent Connections to the Security Gateway

In the **Gateway Properties** > **Optimization > Capacity Optimization** section you can configure the maximum limit for concurrent connections.

When users connect to corporate resources through the Mobile Access blade, it creates multiple connections. For example, from the user to the Security Gateway, and from the Security Gateway to the internal server. Therefore, in an environment with over 1000 remote users, we recommend that you increase the maximum concurrent connections.

For example: The default maximum is 25,000. If you have 2000 mobile access users, increase the maximum to 29,000 (2 times 2000).

# Server Certificates

For secure SSL communication, Security 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 Security 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 Security 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, Security Gateways must have a server certificate signed by a known certificate authority (such as Entrust, VeriSign or Thawte). This certificate canbe issued directly to the Security Gateway, or be a chained certificate that has a certification path to a trusted root certificate authority (CA).

The next sections describe how to get a certificate for a Security Gateway that is signed by a known Certificate Authority (CA).

## Generating the Certificate Signing Request

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

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

1. From the Security Gateway command line, log in to the Expert mode.
2. Run:

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

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

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

3. Enter a password and confirm.

   Fill in the data.

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

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

## Generating the P12 File

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

1. Get the Signed Certificate for the Security Gateway from the CA.

   If the signed certificate is in P12 or P7B format, convert these files to a PEM (Base64 encoded) formatted file with a CRT extension.

2. Make sure that the CRT file has the full certificate chain up to a trusted root CA.

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

3. From the Security Gateway command line, log in to the Expert mode.
4. Use the `*.crt` file to install the certificate with the `*.key` file that you generated.
   a. Run:

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

      For example:

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

   b. Enter the certificate password when prompted.

## Generating Wildcard Certificates for Hostname Translation

If you use Hostname Translation, you need a wildcard certificate. This lets clients access Web applications on sub-domains behind the Security Gateway. If Mobile Access uses a fixed domain certificate, client browsers issue certificate warnings when users try to access Web applications in a sub-domain behind the Mobile Access Security Gateway. This is because each Web application URL is translated to a different Mobile Access hostname.

Before you begin, make sure the Hostname Translation support is configured in the *"Mobile Access Applications" on page 55* and in the *"Mobile Access Applications" on page 55*.

**To prepare a request a 3rd-Party wildcard server certificate:**

1. In **Subject DN**, start with `CN=`*`FQDN`*.

   For example: `CN=sslvpn.example.com`
2. In **Alternate Name**, enter two DNS names: the FQDN and the wildcard.

   For example:

   ```
   sslvpn.example.com, *.sslvpn.example.com
   ```

**To configure wildcard certificate generation:**

1. Backup and edit the configuration file of the **csr_gen** script:
   - R75.20 and higher - **$CPDIR/conf/openssl.cnf**
   - R66.x, R71.x, R75, R75.10 - **$CVPNDIR/conf/openssl.cnf**
2. In the `[ req ]` section, uncomment the line:

```
req_extensions = v3_req
```

3. In the `[ v3_req ]` section, add this line:

   `subjectAltName=DNS:`*`FQDN`*`,DNS:*.`*`ParentDomain`*

   For example:
   `subjectAltName=DNS:sslvpn.example.com,DNS:*.sslvpn.example.com`

4. Save **openssl.cnf**.
5. Run **csr_gen** and create the CSR.

   To make sure the CSR was generated properly, run:

   - R75.x - `cpopenssl req -in requestFile.csr -text`
   - earlier versions - `openssl req -in requestFile.csr -text`

6. When asked for the CommonName (CN), enter the FQDN. For example:
   `sslvpn.example.com`
7. Restore the **openssl.cnf** file from the backup.

## Installing the Signed Certificate

**To install the certificate:**

1. Log in to SmartConsole.
2. From the left Navigation Toolbar, click **Gateways & Servers**.
3. Open the Identity Awareness Security Gateway object.
4. In the navigation tree, click the appropriate Software Blade page:

   - **Mobile Access** > **Portal Settings**
   - **Platform Portal**
   - **Data Loss Prevention**
   - **Identity Awareness** > **Captive Portal** > **Settings** > **Access Settings**

   In the **Certificate** section, click **Import** or **Replace**.

5. Install the Access Control Policy on the Security Gateway.

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

# Viewing the Certificate

**To see the new certificate from a Web browser:**

The Security Gateway uses the certificate when you connect with a browser to the portal. To see the certificate when you connect to the portal, click the lock icon that is next to the address bar in most browsers.

The certificate that users see depends on the actual IP address that they use to access the portal - not only the IP address configured for the portal in SmartDashboard.

**To see the new certificate from SmartConsole:**

From a page that contains the portal settings for that blade/feature, click **View** in the **Certificate** section.

# Web Data Compression

Mobile Access can be configured to compress Web content. This can produce a much faster website for users. It also reduces bandwidth needs, and therefore, costs.

Most compression algorithms, when applied to a plain-text file, can reduce its size by 70% or more, depending on the content in the file.

Be aware that compression does increase the CPU usage of Mobile Access, which in itself does have some performance implications.

Most browsers can accept compressed data, uncompress it and display it.

If configured to compress data, Mobile Access compresses the data received from Web servers (the http or https response). If the Web browser at the endpoint compresses the http or https request, Mobile Access uncompresses it and sends it on to the server. This is illustrated in the figure below.

Mobile Access supports the gzip, deflate, and compress compression methods.

It is possible to specify the mime types that will be compressed.


| Item | Description |
|---|---|
| 1 | Web Browser |
| 2 | Compressed Request |

| Item | Description |
|---|---|
| 3 | Mobile Access enabled Security Gateway |
| 4 | Uncompressed request (e.g., gunzip) |
| 5 | Web Server |
| 6 | Response |
| 7 | Compressed Response (e.g., gzip) |

## Configuring Data Compression

Web data compression is configured per Security Gateway in Database Tool (GuiDBEdit Tool) (see sk13009).

**To configure data compression by Mobile Access:**

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with Database Tool (GuiDBEdit Tool) to the Management Server.
3. In the top left pane, go to **Network Objects** > **network_objects**.
4. In the top right pane click Security Gateway / Cluster object.
5. In the bottom pane, 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**.
6. Save the changes in Database Tool (GuiDBEdit Tool) (**File** menu > **Save All**) and close it.
7. Connect with SmartConsole to the Management Server.
8. Install policy on the Security Gateway / Cluster object.

# Using Mobile Access Clusters

A remote access enabled Security Gateway is a business critical device for an organization. A failure of a Security 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 of Mobile Access Security Gateways provides:

- Transparent failover in case of cluster member failure.
- Zero downtime for mission-critical environments.
- Enhanced throughput (in Load Sharing modes).

All cluster members are aware of the sessions tracked through each of the other cluster members. The cluster members synchronize their sessions and status information across a secure synchronization network.

## The Sticky Decision Function

If you are using SSL Network Extender, you must enable the Sticky Decision Function.

A connection is *sticky* when all of its packets are handled, in either direction, by a single cluster member.

The Sticky Decision Function distributes sessions from client IP addresses between the cluster members, and ensures that connections from a given IP always pass through the same member.

## How Mobile Access Applications Behave on Failover

The table below summarizes the end-user experience upon failover for each Mobile Access application.

| Application | Survives failover? | User experience upon failover |
|---|---|---|
| Web browsing through the user portal<br>Domino Web Access<br>Outlook Web Access<br>File Shares | Yes | User is unaware of failover. If the failover happens while a user is clicking a link or waiting for a server response, user may be disconnected and may need to refresh the page. |

| Application | Survives failover? | User experience upon failover |
|---|---|---|
| Web Mail | No | 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. |
| Citrix | No | User is disconnected, and the Citrix session is lost. User must actively re-establish a connection. |
| Endpoint Compliance Scan | Yes | Re-scan may be required if user logs out of the portal, or needs to log in again. |
| Secure Workspace | Yes | 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. |
| Multi challenge login | No | If user is in the middle of a multi-challenge login he/she is redirected to the initial login page. |
| SSL Network Extender Network Mode | Yes | The user may notice the connection stalling for a few seconds, as if there was a temporary network disconnection. |
| SSL Network Extender Application Mode | No | 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). |
| SSL Network Extender - Downloaded-to-Mobile Access applications | Mode dependent | Network Mode - Survives failover.<br>Application Mode - Does not survive failover. |

# Troubleshooting Mobile Access

## 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.

## 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 *"Mobile Access Applications" on page 55*.
2. Go over the Troubleshooting OWA Checklist.
3. Look for a description that matches your issues in the "Common OWA problems" section.

### Troubleshooting OWA Checklist

The following sections describe steps to take if you are experiencing problems using Outlook Web Access with Mobile Access.

1. Check your traffic logs for errors. The logs may help you to pinpoint the problem.
2. Reproduce the scenario without Mobile Access and ensure that the problem does not occur.
3. Verify connectivity. Make sure that:
   - The Mobile Access machine has a network route to all relevant Microsoft Exchange servers and relevant server ports are accessible, usually port 80 or 443.

     HTTP and/or HTTPS packets must be able to reach Microsoft Exchange servers.
   - Mobile Access users have a network route to the Mobile Access machine.
4. Verify that your configuration is valid. Make sure that:

- The Outlook Web Access version is supported by Mobile Access.
- Client-side browsers are supported by OWA and by Mobile Access.
- OWA Services are configured to use protocols acceptable by the servers in question. For example, if an Exchange server is configured to accept HTTPS traffic only, the corresponding OWA Web application on Mobile Access must utilize HTTPS.
- Security restrictions are disabled (see the "Troubleshooting Security Restrictions in OWA" section).
- 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 use one of these features, use SSL Network Extender.

# Common OWA problems

These sections describe issues related to browsing to OWA through Mobile Access.

**Note** - Examine your traffic logs for errors, to pinpoint the problem.

## Troubleshooting Authentication with OWA

After users log in to Mobile Access, and attempt to access an OWA application, they are required by OWA to provide authentication credentials.

Outlook Web Access has two authentication schemes: the regular HTTP-based authentication (HBA), which is the default, and Form-Based authentication (FBA). In addition, Mobile Access supports single sign-on (SSO) through HBA and FBA.

### HBA Problems

If an internal Web Server requests Integrated Windows Authentication (NTLM) or any other HTTP-based authentication, Mobile Access either displays a dialog box requesting login credentials, or tries to use the user's portal credentials, depending on the configuration of the Mobile Access Web application. HBA-related problems may result from the use of IIS web-based password management services.

IIS Web applications (such as Outlook Web Access) can be configured to use IIS Web-based password management services. These services make it possible for users to change their Windows NT passwords via a web server. These services use IIS HTR technology which is known to be vulnerable to attack, and can allow an attacker to run malicious code on the user system. Microsoft has long advocated that customers disable HTR on their Web servers, unless there is a business-critical need for the technology (Microsoft Security Bulletin MS02-028).

In keeping with the Microsoft recommendation, IPS protects against HTR exploits by default. If you wish to allow the use of the HTR mechanism, deactivate the "htr" worm pattern in the IPS **General HTTP Worm Catcher** protection. Install the Security policy from SmartDashboard after making these changes.

### Single Sign On Problems

When troubleshooting, eliminate the possibility of Single Sign On problems by removing the OWA user credentials from the credentials list in the Mobile Access user portal.

## Troubleshooting Authorization with OWA

The authorization mechanisms of Mobile Access allow administrators to grant access to various resources on a per-path, per-host and per-port basis. Mobile Access views Outlook Web Access as a Web application with special properties, connecting to a special Web server.

Authorization-related problems may result from:

- **Discrepancies in the OWA Web Application Configuration versus the setup in Microsoft Exchange server.**

  Possible discrepancies may occur in the configuration of the OWA port, protocol or paths versus the setup of the corresponding Microsoft Exchange server.

  OWA Service must be configured in accordance with the Microsoft Exchange server configuration. Otherwise, Mobile Access will not be able to authorize access to the application.

**Authorization Example Scenario**

A user launches an OWA application, gets to the Form-Based Authentication (FBA) page and authenticates using his/her credentials. Subsequently, the user gets the "Access denied" page.

**Cause:** The Microsoft Exchange server side component (IIS or other) is configured to accept both HTTP and HTTPS traffic, whereas the Mobile Access OWA Web application is configured to authorize HTTP traffic only.

**Explanation:** The Form Based Authentication setting on the Microsoft Exchange server requires clients to use SSL, which means that some server-side component (be it IIS or other) must also accept SSL traffic. The following message is displayed to the Microsoft Exchange administrator upon FBA configuration:

Forms Based Authentication requires clients to use a SSL connection. If SSL encryption is not off-loaded to another source, complete the following steps:

- Configure SSL
- Restart the IIS service

This means that IIS is likely to be configured to work over SSL. However, in complex cases, such as SSL encryption being off-loaded to another source, and the IIS server itself allowing HTTP traffic, the Mobile Accessadministrator 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, Security Gateways, or websites).

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).

# Troubleshooting Security Restrictions in OWA

Mobile Access utilizes many built-in security features that screen inner networks from external threats. In addition, the Mobile Access endpoint security features protect the endpoint devices.

Occasionally, protection mechanisms may interfere with legitimate user activities. To eliminate this possibility, switch off all Web Intelligence protections during troubleshooting and the install the security policy.

User experiences may vary widely so they are not detailed here. Use the following steps to troubleshoot issues with security restrictions.

1. Check the traffic log to see if any relevant URL was blocked due to security restrictions.
2. To reduce the number of false-positives:
   - In SmartDashboard, in the IPS tab, go to **Protections > By Protocol > Integrated > Web Intelligence** and turn all settings of Application Layer Protection Level to *Low*.
   - In the **ASCII Only Request** protection, clear **Block non ASCII characters in form fields**.
   - Install the Security policy from SmartDashboard.
3. If Step 2 did not solve the problem, try the following:
   - Modify the **Endpoint Compliance** page of the Mobile Access Web Application to **Allow caching of all content**.
   - In SmartDashboard, in the IPS tab, go to **Web Intelligence** and
     - In the **HTTP Protocol Inspection > HTTP Methods** protection, clear **Block standard Unsafe HTTP methods**.
     - In the **Malicious Code > General HTTP Worm Catcher** protection, disable the "htr" worm pattern.
   - Install the Security Policy from the administration portal.
4. If Step 3 did not solve the problem, try the following steps in order:
   a. Turn off all Web Intelligence protections.
   b. Turn off all IPS protections.
   c. Install the Security policy from SmartDashboard.

# Troubleshooting Performance Issues in OWA

Performance issues may occur with OWA for the following reasons:

- **Logging Issues**

  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.

  **Note** - To get rid of these logs, turn off Debug logs, Trace logs, and purge the 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 Security Gateway. It takes time to process each particular packet of information.

  There is therefore a difference in latency between connections passing through Mobile Access and those that do not. The overhead in absolute elapsed time is proportional to the amount of data passed through the network.

  Latency and therefore performance problems when working through Mobile Access may be felt in particular by users with large numbers of emails, calendar events, task items and the like.

  **To solve this problem:**

  Minimize the latency overhead by increasing the performance of Mobile Access. You can do this by using a stronger machine.

- **SSL Time-out Problems**

  SSL time-out problems can occur with Internet Explorer while working through Mobile Access. They can cause slowness and even temporary or permanent unresponsiveness of the browser.

**To solve this problem:**

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

**To configure Mobile Access to work without keep-alive packets to specific locations:**

1. Supply additional `LocationMatch` directives for each host used by the Web Application in question. All directives go in the `$CVPNDIR/conf/includes/Main.virtualhost.conf` file, in the `VirtualHost` section.

   For more information, see:
   http://httpd.apache.org/docs/2.0/mod/core.html#locationmatch

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

   For example:

   ```
    <LocationMatch "CVPNHost=208\.77\.188\.166">
     SetEnv nokeepalive
   </LocationMatch>
   ........
   <LocationMatch
   "CVPNHost=myhost\.example\.com|CVPNHost=myhost">
     SetEnv nokeepalive
   </LocationMatch>
   ```

2. Run `cpstop` and then `cpstart`.
3. Repeat for each Mobile Access cluster member.

- Authorization Problems

# Saving File Attachments with OWA

When trying to save a file attachment with Outlook Web Access (OWA), Mobile Access adds the full path to the file name. For example, the file name appears something like:

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

To solve this, configure the Web Application to use Path Translation or Hostname Translation (see *"Mobile Access Applications" on page 55*).

# Troubleshooting Citrix

**Note** - This section refers to Citrix-related issues occurring when working through Mobile Access without the use of SSL Network Extender.

If you have issues with Citrix after the deployment of Mobile Access, see *"Mobile Access Applications" on page 55* > section about Citrix Services. Then try the troubleshooting checklist.

## Troubleshooting Citrix Checklist

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

### Connectivity Issues

1. Make sure that Mobile Access has a network route to all Web Interface servers intended to be used and relevant server ports are accessible. Usually ports 80 or 443.

   HTTP and/or HTTPS protocols must be traversible towards Web Interface servers.

2. Make sure that Mobile Access has a network route to all Presentation servers intended to be used and relevant server ports are accessible. Usually ports 1494 or 2598.

   ICA protocol must be traversible towards Presentation servers.

3. Make sure that Mobile Access machine has a network route to all STA servers intended to be used, if any, and port 80 on STA servers is accessible, and HTTP protocol is traversible.

4. Make sure that Mobile Access users have a network route to the Mobile Access machine.

### Configuration Issues

1. Make sure that Citrix servers and clients are of those versions supported by Mobile Access.

2. Make sure that all necessary STA servers are configured with corresponding Citrix Services on Mobile Access.

3. Make sure that the Mobile Access server certificate:

   - is issued to the Fully Qualified Domain Name (such as www.example.com) of the Security Gateway

- is properly configured
- is trusted by the client-side

# Troubleshooting File Shares

- Mobile Access gives an informative error message when an attempt to access a file share fails. However, if a user tries to access a share that does not exist on the file server, Mobile Access cannot always distinguish this error from an Access Denied error. In this case the user may be presented with the credentials input form again, or get an Access Denied error.
- The Windows Explorer viewer can normally be used for browsing website. However, the Mobile Access SSL Network Extender window may not load properly when using it, and the user may be presented with the Mobile Access login page. It is recommended to use the Web-based viewer instead.
- When browsing file shares through the Mobile Access user portal, users can open most files by clicking them. However, some files, for example .wmv extension files, cannot be opened that way, and must be downloaded to the local desktop and opened from there. When using the Mobile Access Web-based file viewer, download the file by right-clicking on the file and choosing "Save Target As...". When using the Windows File Explorer viewer, download the file by copying or drag-and-dropping it to the local desktop.
- When accessing files via Mobile Access, the client application used to view a file depends on the file type. Some file types (such as jpg files) can be configured to be opened by a Web browser. In some client configurations, the result of opening such a file may show the Mobile Access login page instead of the requested file. If this happens, verify that the client uses the latest recommended browser version including all patches and fixes. Specifically, install Internet Explorer patch Q823353 on the endpoint.
- When using Mobile Access file shares with VSX, the DNS resolving of the hostname might not work correctly with file shares. Make sure that the `/etc/resolve.conf` file is configured correctly or change the value of `vsxMountWithIPAddress` in the `$CVPNDIR/conf/cvpnd.C` from `false` to `true`. The file share will use the host ip for the mount instead of the hostname.
- If you have functionality or UI issues with File Sharing, or when using File Sharing with an unsupported browser, you can switch to the R77 File Sharing UI to resolve issues.

  **To switch between the R77 and R80.x File Sharing UI:**

1. Backup the file: `$CVPNDIR/htdocs/HFS/.include/conf/properties.ini`
2. Edit the file. Change the value of this line: `use.old.design=`

   Use these values:

   - true - to enable R77 File Sharing UI
   - false - to enable R80.x File Sharing UI
3. Save the changes.

# Troubleshooting Push Notifications

**Scenario: Push notifications are configured but users do not see push notification in Capsule Workspace.**

Use the **Push Notification Status Utility** and **Monitoring Push Notification Usage** to troubleshoot Push Notifications with Mobile Access (see *"Mobile Access for Smartphones and Tablets" on page 112*) .

Also see sk109039.

# Mobile Access FAQ

| Question | See: |
|---|---|
| Which browsers and operating systems does Mobile Access support? | *R80.40 Release Notes* |
| Can you store credentials? | *"Single Sign On" on page 87* |
| How to configure Multi-factor authentication? | *"User Authentication in Mobile Access" on page 146* |
| How to configure different authentication for different Security Gateways? | *"User Authentication in Mobile Access" on page 146* |
| How to configure a proxy for Mobile Access? | ■ For an Exchange Server - *"Exchange Mail Applications for Smartphones and Tablets" on page 106*<br>■ For DynamicID with SMS - *"User Authentication in Mobile Access" on page 146*<br>■ For a web application - sk34810 |
| How to allow access to internal resources without the Mobile Access Portal? | *"Reverse Proxy" on page 226* |
| Is WebSocket supported for Web applications? | *"Mobile Access Applications" on page 55* |
| What is SNX? | SSL Network Extender (SNX) Administration Guide |

# Command Line Reference

See the *R80.40 CLI Reference Guide*.

Below is a limited list of applicable commands.

# Syntax Legend

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

| Character | Description |
|---|---|
| TAB | Shows the available nested subcommands:<br>`main command`<br>`→ nested subcommand 1`<br>`→ → nested subsubcommand 1-1`<br>`→ → nested subsubcommand 1-2`<br>`→ nested subcommand 2`<br>Example:<br>`cpwd_admin`<br>`config`<br>`-a <options>`<br>`-d <options>`<br>`-p`<br>`-r`<br>`del <options>`<br>Meaning, you can run only **one** of these commands:<br>■ This command: `cpwd_admin config -a <options>`<br>■ Or this command: `cpwd_admin config -d <options>`<br>■ Or this command: `cpwd_admin config -p`<br>■ Or this command: `cpwd_admin config -r`<br>■ Or this command: `cpwd_admin del <options>` |
| Curly brackets or braces<br>**{ }** | Enclose a list of available commands or parameters, separated by the vertical bar **|**.<br>User can enter only one of the available commands or parameters. |

| Character | Description |
|---|---|
| Angle brackets<br>**< >** | Enclose a variable.<br>User must explicitly specify a supported value. |
| Square brackets or brackets<br>**[ ]** | Enclose an optional command or parameter, which user can also enter. |

# admin_wizard

### Description

Runs the administration client wizard to test connectivity to websites, Exchange server services, or LDAP server.

**Note** - This wizard saves its log messages in these files:

- `$CVPNDIR/log/AdminWizardLog.elg`
- `$CVPNDIR/log/wizard.elg`
- `$CVPNDIR/log/wizardDns`
- `$CVPNDIR/log/wizardEstimation`
- `$CVPNDIR/log/wizardLdap`
- `$CVPNDIR/log/wizardProxy`

### Syntax

```
admin_wizard
      cancel
      estimation
      exchange_wizard <Exchange Server Address> <User Name>
<Password> [<Options>]
      ldap <LDAP server>
      wizard <Web Site Address>
```

### Parameters

| Parameter | Description |
|---|---|
| No Parameters | Shows the built-in help. |
| `cancel` | Kills the administration client wizard that already runs. |
| `estimation` | Estimates how many seconds the wizard will run. |

| Parameter | Description |
|---|---|
| `exchange_wizard <Exchange Server Address> <User Name> <Password> [<Options>]` | Tests the response from an Exchange server:<br>■ Finds the address protocol (HTTP or HTTPS) and authentication method (Basic or NTLM) of the Exchange server services.<br>■ Checks accessibility of Mobile Access ActiveSync and EWS services for users.<br>■ For Web command, checks access to the URL.<br>■ For OWA command, returns the URL to the outlook web access.<br><br>The parameters are:<br>■ *<Exchange Server Address>* - Specifies the Exchange server by its IP address or hostname.<br>■ *<User Name>* - Specifies the user name on the Exchange Server.<br>■ *<Password>* - Specifies the password on the Exchange Server.<br>■ *<Options>* - Specifies the test options. |

| Parameter | Description |
|---|---|
| | The available test options are:<br>■ `-t {as \| ews \| owa \| all}` - Specifies the services to test on the Exchange server:<br>**Note** - To specify more than one service, separate them with a comma. For example: `as,ews`<br>• `all` - Tests all of the services (default)<br>• `as` - Tests ActiveSync<br>• `ews` -Tests Exchange Web Services<br>• `owa` - Searches for the Outlook Web Application (OWA) address of the Exchange server<br>■ `-d <DNS Servers>` - Specifies the DNS servers.<br>■ `-x <Proxy Servers>` - Specifies the Proxy servers.<br>■ `-c <Username>:<Password>` - Specifies the user name and password for Proxy server authentication.<br>■ `-n` - Allows only NTLM authentication instead of Basic and NTLM.<br>■ `-m <Domain Name>` - Specifies the user domain name.<br>■ `-s <ActiveSync Path>` - Tests a specified ActiveSync service path (Default: `/Microsoft-Server-ActiveSync`).<br>■ `-e <EWS Path>` - Tests a specified Exchange Web Services service path (Default: `/EWS/Exchange.asmx`).<br>■ `-f <File Name>` - Writes the test results to the specified file<br>■ `-r` - Sends a request with the configured Proxy, DNS, HTTP protocol, and authentication method.<br>• If you also specify the "`-n`" option, then the NTLM authentication method is used.<br>• If you do not specify the "`-n`" option, then only the Basic authentication method is used. |

| Parameter | Description |
|---|---|
| | ■ `-v` - Makes the HTTP requests verbose. The verbose result files are saved in the `$CVPNDIR/log/trace_log/` directory.<br>■ `-p` - Validates the SSL certificate of the web server. |
| `ldap <LDAP server>` | Tests connectivity to the specified LDAP server. You can specify the LDAP server by its IP address or hostname. |
| `wizard <Web Site Address>` | Tests connectivity to the specified URL. |

**Example 1 - Check URL accessibility of 'www.checkpoint.com'**

```
admin_wizard wizard www.checkpoint.com
```

**Example 2 - Check accessibility to the LDAP server 192.168.0.55**

```
admin_wizard ldap 192.168.0.55
```

**Example 3 - Check accessibility for username 'user1' to ActiveSync and EWS on the Exchange server 'exchange.example.com'**

```
admin_wizard exchange_wizard exchange.example.com username user1 -
t as,ews
```

# cvpnd_admin

### Description

Changes the behavior of the Mobile Access **cvpnd** process.

### Syntax

```
cvpnd_admin
      appMonitor status
      clear_kernel_tables
      clear_portal_cache
      debug <options>
      ics_update
      isEnabled
      license <options>
      policy [{graceful | hard}]
      revoke <Certificate Serial Number>
```

### Parameters

| Parameter | Description |
|---|---|
| `appMonitor` *<options>* | Controls the Application Monitor.<br>The Application Monitor is a software component that monitors internal servers to track their up time.<br>If problems are found, a system alert log is created.<br>The available <*options*> are:<br>■ `restart` - Restarts the Application Monitor.<br>■ `start` - Start the Application Monitor.<br>■ `status` - Shows the status of the Application Monitor feature, the applications monitored by the Application Monitor and their status.<br>■ `stop` - Stops the Application Monitor. |
| `clear_kernel_tables` | Clears all Mobile Access kernel tables. |
| `clear_portal_cache` | Clears the cache for the applications presented in the Mobile Access Portal for all open sessions. |

| Parameter | Description |
|---|---|
| `debug set TDERROR_ALL_ ALL=5` | Enables all `cvpnd debug` output for the running **cvpnd** process. The output is in the `$CVPNDIR/log/cvpnd.elg` file.<br>**Note** - When you enable all debug topics, it might impact the performance. Debug topics are provided by *Check Point Support*. |
| `debug off` | Disables all `cvpnd debug` output. |
| `debug trace on`<br>`debug trace users=<Username>` | The `TraceLogger` feature generates full captures of incoming and outgoing authenticated Mobile Access traffic.<br>The output is saved in the `$CVPNDIR/log/trace_log/` directory.<br>■ `debug trace on` - Enables the `TraceLogger` feature for all users.<br>■ `debug trace users=<Username>` - Enables the `TraceLogger` feature for a specified username<br>**Important:**<br>■ The `TraceLogger` feature has a major effect on performance, because all traffic is saved as files.<br>■ The `TraceLogger` feature uses a lot of disk space, because all traffic is saved as files. After a maximum number of files is saved, the oldest files are removed from the disk, which also has a performance cost.<br>■ The `TraceLogger` feature creates a security concern: end-user passwords that are sent to internal resources might appear in the capture files. |
| `ics_update` | Updates the Mobile Access services after you published a new ICS update. |
| `isEnabled` | Checks if Mobile Access is enabled by policy. |
| `license <options>` | Shows Mobile Access license count and status:<br>■ `all` - Shows information about the MOB and MOBMAIL licenses.<br>■ `mob` - Shows information about the MOB license.<br>■ `mobmail` - Shows information about the MOBMAIL license. |

| Parameter | Description |
|---|---|
| `policy [{graceful \| hard}]` | Updates the Mobile Access services according to the current policy:<br>■ `policy` - For Apache services, each `httpd` process waits until its current request is finished, then exits.<br>■ `policy graceful` - For Apache services, each `httpd` process waits until its current request is finished, then exits.<br>■ `policy hard` - For Apache services, all `httpd` processes exit immediately, terminating all current `http` requests. |
| `revoke <Certificate Serial Number>` | Notifies about revocation of a certificate with a given serial number. |

# cvpnd_settings

### Description

Changes a Mobile Access Gateway local configuration file `$CVPNDIR/conf/cvpnd.C`.

The `cvpnd_settings` commands allow to get attribute values or set them in order to configure the **cvpnd** process.

**Important** - Changes made by with the `cvpnd_settings` command are **not** saved during the Mobile Access Gateway upgrade. Keep a backup of your `$CVPNDIR/conf/cvpnd.C` file after you make manual changes.

**Warning** - The **cvpnd** process may not start, if you make a mistake in the syntax - attribute names or their values.

### General Syntax

```
cvpnd_settings [<Configuration File>] {get | set | add | listAdd |
listRemove | internal} <Attribute-Name> [<Attribute-Value>]
```

### Syntax for DynamicID Resend

```
cvpnd_settings [<Configuration File>] {set | get}
smsMaxResendRetries [<Number>]
```

### Syntax for Kerberos Authentication

```
cvpnd_settings [<Configuration File>] {set | get} useKerberos
{true | false}
```

```
cvpnd_settings [<Configuration File>] {listAdd | listRemove}
kerberosRealms [<Your AD Name>]
```

### Parameters

Run this command to see the full explanation of the parameters: `cvpnd_settings -h`

| Parameter | Description |
|---|---|
| `-h` | Shows built-in help with full explanation of the parameters. |
| *<Configuration File>* | Specifies the path and the name of configuration file to change. |

| Parameter | Description |
|---|---|
| `get` | Gets the value of an existing attribute, or values of a list. |
| `set` | Sets the value of an attribute.<br>If the specified attribute does not exist in the configuration file, then the command adds it. |
| `add` | Adds a new attribute.<br>If the specified attribute already exists in the configuration file, then the command does not change it. |
| `listAdd` | Adds the specified attribute to a list. |
| `listRemove` | Removes the specified attribute from a list. |
| `internal` | Specifies that the command must change the `$CVPNDIR/conf/cvpnd_internal_settings.C` file instead of the `$CVPNDIR/conf/cvpnd.C` file. |
| *<Attribute-Name>* | Specifies the attribute name. |
| *<Attribute-Value>* | Specifies the attribute value. |
| *<Number>* | Specifies the number of SMS resend attempts. |
| *<Your AD Name>* | Specifies the Active Directory name. |

### Examples 1 - Set the value of the attribute 'myFlag' to 1

```
cvpnd_settings set myFlag 1
```

### Examples 2 - See the current value of the attribute 'myFlag'

```
cvpnd_settings get myFlag
```

### Examples 3 - Empty the value of the attribute 'myFlag', or create a new attribute/list 'myFlag'

```
cvpnd_settings set myFlag
```

### Examples 4 - Add the attribute 'myFlag' with the value 'a.example.com' to a list

```
cvpnd_settings listAdd myFlag a.example.com
```

# cvpn_ver

## Description

Shows the version of the Mobile Access Software Blade.

**Best Practice** - Run the "`fw ver -k`" command to get all version details.

## Syntax

```
cvpn_ver
```

## Example

```
[Expert@MyGW:0]# cvpn_ver
This is Check Point Mobile Access R80.40 - Build 123
[Expert@MyGW:0]#
```

# cvpnrestart

### Description

Restarts all Mobile Access blade services.

**Warning** - While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

### Syntax

```
cvpnrestart [--with-pinger]
```

### Parameters

| Parameter | Description |
|---|---|
| `--with-pinger` | Restarts the **Pinger** service, responsible for ActiveSync and Outlook Web Access push mail notifications. |

# cvpnstart

## Description

Starts all Mobile Access blade services, after you stopped them with the *"cvpnstop" on page 271* command.

## Syntax

```
cvpnstart
```

# cvpnstop

## Description

Stops all Mobile Access blade services.

**Warning** - While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

## Syntax

```
cvpnstop
```

# deleteUserSettings

### Description

Deletes all persistent settings (favorites, cookies, credentials) of one or more end-users.

### Syntax

```
deleteUserSettings [-s] <Username1> [<Username2> ...]
```

### Parameters

| Parameter | Description |
|---|---|
| `-s` | Runs in silent mode with no output to the end-user's screen. |
| *<Username>* | Specifies the user name, whose settings to delete.<br>**Notes:**<br>■ When you refer to an internal user, use its username.<br>■ When you refer to an LDAP user, use the full DN according to your LDAP settings. |

### Example 1 - Delete an internal user named 'user1

```
deleteUserSettings [-s] user1
```

### Example 2 - Delete an LDAP user named 'user1', whose DN is 'CN=user1,OU=users,DC=example,DC=com':

```
deleteUserSettings [-s] CN=user1,OU=users,DC=example,DC=com
```

# fwpush

### Description

Sends command interrupts to the **fwpushd** process on the Mobile Access Gateway.

**Note** - Users get the push notifications only while they are logged in.

### Syntax

```
fwpush
      debug <options>
      del <options>
      info
      print
      send <options>
      unsub <options>
```

### Parameters

| Parameter | Description |
|---|---|
| `debug {off \| on \| reset \| set all all \| stat}` | Controls the debug of the Mobile Access Push Notifications daemon. For more information, see sk109039. |
| `del {-token <Token> \| -uid <User-UID>}` | Deletes a specified token, or all tokens for a specified user.<br>The available options are:<br>■ Delete the specified token for all users:<br>`fwpush del -token <Token>`<br>■ Delete all tokens for a specified user:<br>`fwpush del -uid <User-UID>` |

| Parameter | Description |
|---|---|
| `info` | Gets data on notifications in the push queue:<br>■ Number of items in queues<br>■ Number of seconds the oldest item is in the queue<br>■ Number of seconds the newest item is in the queue<br>■ Number of seconds a batch waits in the queue<br>■ Number of seconds to the sending of the next batch<br>■ Number of batch errors and authentication request timeouts |
| `print` | Shows the push notifications queue and the pending batches. |
| `send -token <Token> -os {iPhone \| Android} -msg "<Notification Message>"`<br>`send {-user <Username> \| -uid <User-UID>} -msg "<Notification Message>"` | Sends an on-demand push notification message from a command line.<br>**Important** - Before you use the "`fwpush send`" command, make sure the user is: (A) registered on the Exchange Server, (B) connected. |

| Parameter | Description |
|---|---|
| `unsub {<Token> \| -user <Username> \| -uid <User-UID> \| -all}` | Unsubscribes a user from push notifications.<br>The available options are:<br>■ Unsubscribe all users from the specified token:<br>`fwpush unsub <Token>`<br>■ Unsubscribe the specified user from all tokens:<br>`fwpush unsub -user <Username>`<br>or<br>`fwpush unsub -uid <User-UID>`<br>■ Unsubscribe all users from all tokens:<br>`fwpush unsub -all` |

### Viewing the details of connected users

```
UserSettingsUtil show_exchange_registered_users
```

Example output:

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users
User Name: CN=JohnD,OU=USERS,OU=RND,OU=PO,OU=USA,DC=AD,DC=CHECKPOINT,DC=COM User Settings id:
c4b6c6fbb0c4xxxxxxxx265e93e0e372
Push Token: xxxxxxxxxxxxx65b48e424023ebxxxxxxxxca22ea788cfb3cxxxxxxxxx Device id:
46c5XXXXcc1d10b4e18cf5a1xxxxxxxx
[Expert@MyGW:0]#
```

**Notes:**

- To use the "*<Token>*" parameter in the "`fwpush`" commands, use the value of the **Push Token** attribute.
  In the above example:
  `xxxxxxxxxxxxx65b48e424023ebxxxxxxxxca22ea788cfb3cxxxxxxxxx`
- To use the "*<Username>*" parameter in the "`fwpush`" commands, use the value of the **CN** attribute.
  In the above example: `JohnD`
- To use the "*<User-UID>*" parameter in the "`fwpush`" commands, use the value of the **User Settings id** attribute.
  In the above example: `c4b6c6fbb0c4xxxxxxxx265e93e0e372`

## Example

```
[Expert@MyGW:0]# fwpush send -uid JohnD -msg "Hello - push"
```

# ics_updates_script

### Description

Manually starts an Endpoint Security on Demand (ESOD) update on the Mobile Access Gateway.

For more information, see the contents of the `$CVPNDIR/bin/ics_updates_script` file.

### Syntax

```
$CVPNDIR/bin/ics_updates_script <Path to Local ICS Updates Package>
```

### Parameters

| Parameter | Description |
|---|---|
| *<Path to Local ICS Updates Package>* | Specifies the full path to the local ICS Updates package.<br>Do **not** specify the name of the ICS Updates package. |

### Notes

- Usually, it is not necessary to run this command, and you start the ESOD updates from SmartConsole:
  1. Connect with SmartConsole to the Management Server.
  2. From the left navigation panel, click **Manage & Settings**.
  3. In the Mobile Access section, click **Configure in SmartDashboard**.

     The SmartDashboard opens on the Mobile Access tab.
  4. From the left tree, click Endpoint Security on Demand > **Endpoint Compliance Updates**.
  5. Click **Update Database Now**.
  6. Enter the applicable User Center credentials.
  7. Click **Next**.
  8. Select the applicable Mobile Access Gateways.
  9. Click **Finish**.
  10. Close the SmartDashboard.
- Make sure to run only one instance of this command at a time.

# listusers

## Description

Shows a list of end-users connected to the Mobile Access Gateway, along with their source IP addresses.

## Syntax

```
listusers
```

## Example

```
[Expert@MyGW:0]# listusers
------------------------------
UserName    | IP
------------------------------
Tom , 192.168.0.51
John , 192.168.0.130
Jane , 192.168.0.7
[Expert@MyGW:0]#
```

# rehash_ca_bundle

### Description

Imports all of the Certificate Authority (CA) files from the `$CVPNDIR/var/ssl/ca-bundle/` directory into the Mobile Access trusted CA bundle.

The trusted CA bundle is used when the Mobile Access Gateway accesses an internal server (such as OWA) through HTTPS.

If the SSL server certificate of the internal server is not trusted by the Mobile Access Gateway, the Mobile Access Gateway responds based on the settings for the Internal Web Server Verification feature. The default setting is **Monitor**.

To accept certificates from a specified server, add its server certificate CA to the CA bundle.

### Syntax

```
rehash_ca_bundle
```

### Example

```
[Expert@MyGW:0]# rehash_ca_bundle
Doing /opt/CPcvpn-R80.40/var/ssl/ca-bundle/
AC_Ra__z_Certic__mara_S.A..pem => 6f2c1157.0
AOL_Time_Warner_Root_Certification_Authority_1.pem => ed9bb25c.0
... ... ...
beTRUSTed_Root_CA_-_RSA_Implementation.pem => 16b3fe3c.0
thawte_Primary_Root_CA.pem => 2e4eed3c.0
[Expert@MyGW:0]#
```

# UserSettingsUtil

## Description

Shows details of users connected to the Mobile Access Gateway.

## Syntax

```
UserSettingsUtil show_exchange_registered_users [<Username>]
```

## Parameters

| Parameter | Description |
|---|---|
| *<Username>* | Specifies the user name.<br>**Notes:**<br>■ When you refer to an internal user, use its username.<br>■ When you refer to an LDAP user, use the full DN according to your LDAP settings. |

## Example 1 - To show all users

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users
User Name: CN=JohnD,OU=USERS,OU=RND,OU=PO,OU=USA,DC=AD,DC=CHECKPOINT,DC=COM User Settings id:
c4b6c6fbb0c4xxxxxxxx265e93e0e372
Push Token: xxxxxxxxxxxxx65b48e424023ebxxxxxxxxca22ea788cfb3cxxxxxxxxxx Device id:
46c5XXXXcc1d10b4e18cf5a1xxxxxxxx
[Expert@MyGW:0]#
```

## Example 2 - To show an internal user named 'user1'

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users user1
```

### Example 3 - To show an LDAP user named 'user1', whose DN is 'CN=user1,OU=users,DC=example,DC=com'

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users CN=user1,OU=users,DC=example,DC=com
```

# Glossary

## A

**Anti-Bot**
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

**Anti-Spam**
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

**Anti-Virus**
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

**Application Control**
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

**Audit Log**
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

## B

**Bridge Mode**
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

## C

**Cluster**
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

**Cluster Member**
Security Gateway that is part of a cluster.

**Compliance**
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

**Content Awareness**
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

**CoreXL**
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

**CoreXL Firewall Instance**
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

**CoreXL SND**
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

**CPUSE**
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

## D

**DAIP Gateway**
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

**Data Loss Prevention**
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

**Data Type**
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

**Distributed Deployment**
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

**Dynamic Object**
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

## E

**Endpoint Policy Management**
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

**Expert Mode**
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

## G

**Gaia**
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

**Gaia Clish**
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

**Gaia Portal**
Web interface for the Check Point Gaia operating system.

## H

**Hotfix**
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

**HTTPS Inspection**
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

## I

**ICA**
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

**Identity Awareness**
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

**Identity Logging**
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

**Internal Network**
Computers and resources protected by the Firewall and accessed by authenticated users.

**IPS**
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

**IPsec VPN**
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

## J

**Jumbo Hotfix Accumulator**
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

## K

**Kerberos**
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

## L

**Log Server**
Dedicated Check Point server that runs Check Point software to store and process logs.

**Logging & Status**
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

## M

**Management Interface**
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

**Management Server**
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

**Manual NAT Rules**
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

**Mobile Access**
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

**Multi-Domain Log Server**
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

**Multi-Domain Server**
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

## N

**Network Object**
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

**Network Policy Management**
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

## O

**Open Server**
Physical computer manufactured and distributed by a company, other than Check Point.

## P

**Provisioning**
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

## Q

**QoS**
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

## R

**Rule**
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

**Rule Base**
All rules configured in a given Security Policy. Synonym: Rulebase.

## S

**SecureXL**
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

**Security Gateway**
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

**Security Management Server**
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

**Security Policy**
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

**SIC**
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

**SmartConsole**
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

**SmartDashboard**
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

**SmartProvisioning**
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

**SmartUpdate**
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

**Software Blade**
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

**Standalone**
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

## T

**Threat Emulation**
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

**Threat Extraction**
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

## U

**Updatable Object**
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

**URL Filtering**
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

**User Directory**
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

## V

**VSX**
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

**VSX Gateway**
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

## Z

**Zero Phishing**
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.