Important Information

**Important Information**

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

**Latest Version of this Document**
Download the latest version of this document

To learn more, visit the Check Point Support Center

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

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 December 2016</td>
<td>Added Changing the AD Administrator Password (on page 14).</td>
</tr>
<tr>
<td>24 July 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
## Contents

**Important Information** ................................................................................................... 3

**Introduction** ................................................................................................................... 6

- Understanding SMP Architecture ................................................................. 6
- SMP WebUI........................................................................................................... 6
- Active Directory Database ................................................................................ 6
- SMP Server ............................................................................................................ 6

**Using Service Domains** .............................................................................................. 7

**SMP Server Requirements** ............................................................................................. 8

- Windows Server Requirements .......................................................................... 8
- Dynamic DNS Requirements .................................................................................. 8

**Configuring the Firewall for SMP Server** ................................................................. 9

**Active Directory Database** ........................................................................................... 10

**SMP Server** ..................................................................................................................... 10

**Network Requirements** ............................................................................................... 10

**Configuring IIS Ports on SMP Server** ............................................................................. 10

**Installing SMP Server** ................................................................................................. 11

- Preparing to Install SMP ..................................................................................... 11
  - Installing Active Directory ............................................................................. 11
  - Creating an AD User for the SMP ................................................................. 13
  - Installing the Security Management Server (Single SMP Server) .......... 15
- Installing a Single SMP Server ........................................................................... 17
- Installing Multiple SMP Servers ........................................................................ 18
  - Configuring DNS for Secondary SMP Servers ............................................ 18
  - Installing the Secondary Security Management Server ......................... 19
  - Configuring the Secondary Management in SmartDashboard ................ 20
  - Installing the Secondary SMP .................................................................... 21
  - Adding Log Servers to Synchronize the Logs ......................................... 21
  - Installing SMP on a Server with a Legacy Version ................................ 22
  - Logging in to the SMP .................................................................................. 23
  - Activating the Map License ....................................................................... 24
  - Uninstalling the SMP .................................................................................. 25

**Deploying SMP Server** ................................................................................................. 26

- Managing Licenses ................................................................................................. 26
  - Showing the SMP License ........................................................................... 26
- Using a Dynamic DNS Deployment ...................................................................... 27
  - Overview of Dynamic DNS and SMP ........................................................... 27
  - Configuring the DNS Server ......................................................................... 27
  - Preparing SMP Server (Dynamic DNS) ......................................................... 28
  - Configuring SMP Server for Dynamic DNS ................................................. 29
  - Configuring Dynamic DNS in the SMP WebUI .............................................. 29
  - Installing an SSL Certificate for the SMP .................................................... 30

**Failover from Primary to Secondary SMP Server** ......................................................... 32

- Overview of SMP Failover .................................................................................... 32
  - Changing the Secondary Security Management Server to Active .......... 33
  - Setting the Primary SMP to Standby ............................................................. 33
  - Setting the Secondary SMP to Active .......................................................... 33
Introduction

In This Section:

Understanding SMP Architecture .................................................................6
Using Service Domains ....................................................................................7

This guide explains how to install the SMP (Security Management Portal) on a Windows server. The SMP lets you remotely manage and configure Check Point Small/Medium Business appliances for your customers.

Make sure that you read this guide carefully before you install and deploy the SMP.

Understanding SMP Architecture

SMP WebUI

The SMP WebUI is an Internet browser based application that helps you configure and manage the different SMP components, users, gateways, and system settings. You use a secure HTTPS connection to log in to the WebUI.

The SMP WebUI is hosted on an Apache Tomcat application server.

Active Directory Database

The data and settings for the gateways managed by SMP are stored in the Active Directory database.

SMP Server

SMP Server is the Windows Server on which the SMP is installed. To implement the SMP, it uses:

- Security Management Portal
- Active Directory
- Check Point Security Management Server

Two SMP Server modules that manage the gateways:

- CMLS - Creates a secure connection between the SMP and the gateways
- JMLS - Processes data sent by the CMLS and the gateways
Using Service Domains

SMP Server supports divisions that separately manage gateways and users. Each division is called a Service Domain and acts as a limited virtual SMP. The global SMP administrator can log in to all the Service Domains.

The gateways, Service Domain administrators, and user objects that are assigned to a Service Domain are managed only in that Service Domain. These objects cannot be shared between different Service Domains.

When a Service Domain administrator logs in to the SMP, the window shows all the Service Domains. The Service Domain administrator selects the applicable one.
SMP Server Requirements

In This Section:

Windows Server Requirements .......................................................................................... 8
Configuring the Firewall for SMP Server ......................................................................... 9
Active Directory on SMP Server ....................................................................................... 10
Network Requirements ..................................................................................................... 10

Make sure that you meet the server and network requirements before you install SMP Server.

Windows Server Requirements

  - CPU - At least 4 cores
  - Memory - Minimum 8GB, recommended 16 GB
- Disk space
  - Minimum 100GB
  - Additional disk space is required to store gateway logs. The amount depends on: number of managed gateways, amount of time that logs are stored, and the amount of logs generated by each gateway
    For example, to store one month of logs for 100 typical gateways requires 100 GB of additional disk space.
- The SMP Server log receiving module supports up to 2000 gateways. For SMP deployments that manage more than 2000 gateways, it is necessary to use additional SMP servers.
- VMs (virtual machines) are fully supported by the SMP.

Dynamic DNS Requirements

For deployments that use Dynamic DNS, the interface that communicates with the gateways must have two IP addresses: external and Dynamic DNS. The SMP uses the Dynamic DNS IP address to communicate with the gateways.

When there are multiple IP addresses on an interface, Windows 2008 Server automatically selects which one connects to the gateways. The SMP must use the external IP address to connect to the gateways.

- Make sure that the external IP address is closer to the default Gateway IP address than the Dynamic DNS IP address.
- We recommend that the external IP address is on the same subnet as the default Gateway. The Dynamic DNS IP address uses a different subnet.
For more about how Windows uses multiple IP addresses on one interface, go to Microsoft kb969029 https://support.microsoft.com/en-us/kb/969029.

**Note** - The previous link is to the Microsoft Support web site. Check Point is not responsible for the information on that web site.

## Configuring the Firewall for SMP Server

SMP Server is protected by the Windows firewall and sometimes by a corporate firewall as well. For both firewalls, make sure these ports are open and allow connections between the gateways and the SMP. For the Windows firewall, the ports for outbound traffic are open by default.

### Open Ports for Inbound Traffic

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>SmartDashboard Object</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>DNS</td>
<td>domain-tcp</td>
<td>TCP traffic</td>
</tr>
<tr>
<td>257</td>
<td>N/A</td>
<td>FW1_log</td>
<td>TCP traffic - Security logs</td>
</tr>
<tr>
<td>443</td>
<td>SSL</td>
<td>ssl_v3</td>
<td>TCP traffic</td>
</tr>
<tr>
<td>514</td>
<td>N/A</td>
<td>syslog</td>
<td>UDP traffic - System logs</td>
</tr>
<tr>
<td>18191</td>
<td>N/A</td>
<td>CPD</td>
<td>TCP traffic - SIC</td>
</tr>
<tr>
<td>18210</td>
<td>N/A</td>
<td>FW1_ica_pull</td>
<td>TCP traffic - SIC</td>
</tr>
<tr>
<td>18264</td>
<td>N/A</td>
<td>FW1_ica_services</td>
<td>TCP traffic - SIC</td>
</tr>
</tbody>
</table>

### Open Ports for Outbound Traffic

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>SmartDashboard Object</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>SMTP</td>
<td>smtp</td>
<td>TCP traffic - Standard ports for outgoing SMTP. If the port in your network is different, make sure that it is open</td>
</tr>
<tr>
<td>443</td>
<td>SSL</td>
<td>ssl_v3</td>
<td>TCP traffic - HTTPS traffic that connects to the Check Point UserCenter and other Web services</td>
</tr>
<tr>
<td>18191</td>
<td>N/A</td>
<td>CPD</td>
<td>TCP traffic - SIC</td>
</tr>
</tbody>
</table>
Active Directory on SMP Server

SMP uses AD to store the information and data about the gateways that it manages. You must install AD on the server before you install the SMP.

For deployments that use more than one SMP Server, make sure that the AD is installed on the primary server.

Network Requirements

Make sure that these network requirements are met before you install SMP Server:

- Access to an SMTP server (can be in an external network)
- The Windows server DNS name is able to delegate from smbservice.pnt.com to SMP Server
- The SMP uses AD to help manage the gateways. There must be an AD user that is used only for the SMP and define it as:
  - schema admin
  - domain admin
  - Enable feature Password never expires
- Optional - File with the company logo for the Custom Reports feature
- Optional - FTP server to backup the gateway settings

Configuring IIS Ports on SMP Server

Before you install SMP on the server, make sure that Microsoft IIS (Internet Information Services) does not use ports 80 and 8080. The Installation wizard cannot complete the process if IIS uses these ports.

For more about how to configure the IIS ports, go to Microsoft kb149605

Note - The previous link is to the Microsoft Support web site. Check Point is not responsible for the information on that web site.
Preparing to Install SMP

Configure these server settings for the SMP:

- Configuring the Firewall for SMP Server
- Network Requirements (on page 10)

Before you install SMP on the Windows server, you must install these programs on the server:

- Active Directory
- Check Point Security Management Server

⚠️ Important - If you restore the SMP from a backup file, you must use the exact information for these settings:

- AD and Security Management Server administrator accounts
- IP addresses for the SMP interfaces

Installing Active Directory

SMP uses AD (Active Directory) to configure and manage the gateways. Before you install SMP on the server, configure the AD. The AD is used only as an internal database for the SMP. Do not use it as an LDAP for administrators and users.

You must restart the server after the AD is installed.

To install AD on the Windows 2008 R2 server:

1. From the Start menu, run dcpromo.
   The server prepares to start the AD installation wizard.
2. In the Welcome to Active Directory window, click Next.
3. In the Operating System Compatibility window, click Next.
4. In the Choose a Deployment Configuration window, select the correct option for the deployment:

   - **For a single or primary SMP Server** - Click Create a new domain in a new forest.
     - The AD must be a new installation and not part of an existing forest.
   
   - **For a secondary SMP Server** - Do these steps:
     a) Click Existing forest.
     b) Click Add a domain controller to an existing domain.
     c) Enter the settings for the primary SMP Server.
     d) Click Next.

5. In the Name the Forest Root Domain window, enter the domain name.
   - You can create a new root domain, or a sub-domain. We recommend that you do not use a domain that is already in the network.

6. Click Next.


8. Click Next.


10. Click Next.

11. In the Additional Domain Controller Options window, click Next.
    - A warning window opens.

12. Click Yes.

13. In the Location for Database window, click Next.


15. Click Next.

16. In the Summary window, click Next.
    - The server installs AD.

17. In the Completing the Active Directory window, click Next.
    - The restart window opens.

18. Click Restart Now.
    - The server restarts and completes the installation of the AD.

To install AD on the Windows 2012 R2 server:

1. In the Server Manager > Dashboard, click Add roles and features.
   - The Before you begin window opens.

2. Click Next.

3. In Installation Type, click Role-base or feature-based installation.

4. Select the local server and click Next.

5. Select Active Directory Domain Services and the DNS Server if it has not been provisioned.

6. Click Add Features to add features that are required for Active Directory Domain Services.

7. Select the features you want and click Next.
8. Click **Install**.
   - **AD DS** is now added to the left navigation tree of the Server Manager.
9. Click **AD DS**.
10. On the right navigation pane, click **More** under the message **Configuration is required for Active Directory Domain Services**.
    - The **All Servers Task Details** window opens.
11. In **Action**, click **Promote this server to a domain controller**.
    - The **Deployment Configuration** screen appears.
12. Select **Add a new forest**. This is the first domain controller.
13. Enter your Root domain name and click **Next**.
    - **Note** - You can create a new root domain, or a sub-domain. We recommend that you do not use a domain that is already in the network.
14. In the **Set Forest Functional Level** menu, select **Windows Server 2012 R2**.
15. In the **Set Domain Functional Level** menu, select **Windows Server 2012 R2**.
16. In the **Directory Services Restore Mode Administrator Password** window, enter and confirm your password.
17. Click **Next**.
    - A warning appears. You can safely ignore this and click **Next**.
18. The NetBIOS domain name is entered automatically. If there is a conflict, the name appears as the original name with "0" added at the end.
19. Click **Next**.
20. Confirm or change the location of your database folder, log folder, and SYSVOL folder.
21. Review your selections and click **Next**.
22. Click **Install**.

### Creating an AD User for the SMP

This section describes how to create a different administrator account for the SMP.

If you use the AD administrator account, we recommend that you configure the account to make sure that the password never expires.

To create a different AD administrator for the SMP:

1. From **Administrative Tools**, click **Active Directory Users and Computers**.
2. From the navigation tree, click **Users**.
3. Create a new user. In the password settings window, configure these settings:
   - Clear **User must change password at next logon**
   - Select **Password never expires**
   - **Important** - The AD password cannot use these characters: \ " ^
     Only use standard ASCII characters for the password.
4. Right-click the new user and select **Add to a group**.
5. In the **Select Groups** window, add the user to these groups:
   - Domain Admins
   - Schema Admins

6. Save the AD administrator account for the SMP.
   The settings for the domain, username, and password for this account are also used in SMP Server Installation wizard.

**Finding the CN for the AD User**

When you run the SMP First Time Configuration Wizard, you must enter the CN for AD administrator account. If you do not enter the correct CN in the **Primary Database Information** window, the SMP does not install correctly.

To find the CN for the SMP AD administrator account:
1. From SMP Server, click **Administrative Tools > Active Directory Users and Computers**.
2. From the navigation tree, click **Users**.
3. Double-click the SMP administrator.
   The administrator Properties window opens and shows the **General** tab. The CN is listed at the top of the tab.

**Changing the AD Administrator Password**

To change the AD Administrator Password:
1. From **Administrative Tools**, click **Active Directory Users and Computers**.
2. From the navigation tree, click **Users**.
3. Right click on the user name and click **Reset Password**.
4. Clear the checkbox for **User must change password at next logon**.
5. Click **OK**.
6. Restart your computer.
7. Obfuscate the password using **obf.jar**:
   a) Open command line.
   b) Run:
      ```
      Cd C:\CheckPoint\SMP\helpers
      ```
   c) Run:
      ```
      java -jar obf.jar <password>
      ```
   The obfuscated password shows.
8. Stop these services:
   - stop Apache-Catalina
   - stop Apache Tomcat Jmls
9. Change the password in these configuration files:
   - C:\CheckPoint\SMP\conf\SWManagementServer.ini
     Set attribute **Password**
   - C:\CheckPoint\SMP\jmls\conf\jmls.properties
     Set attribute **password**
   - C:\CheckPoint\SMP\Tomcat\webapps\SMC\WEB-INF\INFO.properties
     Set attribute **DB_PASS**

10. Start these services:
    - start Apache-Catalina
    - start Apache Tomcat Jmls

### Installing the Security Management Server (Single SMP Server)

Install the R77.30 Check Point Security Management Server before you install SMP. Make sure that you install the server in a distributed deployment. After you install the Security Management Server, you cannot change the Administrator username and password.

#### To install a new system:

2. Install R77.30 (or upgrade an existing R77).
3. Install SMP setup.exe.

#### To upgrade an existing system:

1. Upgrade R77 Security Management Server to R77.30
   To learn how to install a Security Management Server, see sk104859
2. Stop the Apache JMLS and Apache Catalina services.
3. Run: `hfa-1220.exe`

Before you upgrade the OS from Windows Server 2008 to Windows Server 2012, go here
[https://technet.microsoft.com/en-us/library/1d502209-cdb9-4e13-9a6c-57ad6c9d1e8b](https://technet.microsoft.com/en-us/library/1d502209-cdb9-4e13-9a6c-57ad6c9d1e8b) or

**Important** - After the installation process is complete, you must clear the browser cache for the new version to show.

This procedure is to install the Security Management Server for a deployment with a single SMP Server. For deployments that use multiple SMP Servers, you must configure the Security Management Server as High Availability.

We recommend that you install the SMP in less than seven days after you install the Security Management Server.
To run the Installation Wizard for the Security Management Server:

1. From the R77.30 Security Management Server folder, run Setup.exe as an administrator.
2. In the Welcome window, click Next.
3. In the License window, accept the Check Point license.
4. Click Next.
5. In the Installation Options window, click New Installation.
   Click Next.
   The deployment window opens.
6. Click Custom.
   Click Next.
7. In the Check Point Security Gateway and Management window, make sure that Security Management and SmartConsole are selected.
   Click Next.
8. In the Select Destination Folder window, click Next.
   The management window opens.
9. Click Primary Security Management.
   Click Next.
   The window shows that you selected to install the Security Management (Primary) and SmartConsole products.
10. Click Next.
    The Security Management Server is installed.
11. In the license window, click Use Trial Period license.
    Click Next.
12. In the Add Administrator window, enter the user name and password for the Security Management Server administrator.
    Note - This administrator is a different account than the AD user.
    Click Next.
13. In the GUI Clients window, configure the IP addresses for the hosts that can connect to the Security Management Server.
    • For the highest security, leave this field empty. You can log in to the Security Management Server only from this server.
    • For the easiest connectivity, enter Any. Any host can connect to it.
    • You can also enter the IP addresses for the specified hosts that can connect to it.
    Click Next.
15. In the Fingerprint window, click Next.
    The window shows Thank you for installing Check Point Software.
16. Click Finish.
17. Click Yes.
    The wizard starts the Check Point services and completes the Security Management Server installation.
Installing a Single SMP Server

Use the SMP Installation Wizard to install SMP on the server. The wizard creates the account for an SMP administrator.

To install the SMP on the server:

1. From the \Checkpoint\SMP\ folder, run setup.exe as an administrator.
2. In the Welcome window, click Next.
3. In the License Agreement window, click Yes.  
   Note - The path cannot contain any blank spaces.  
   Click Next.
4. In the Choose Destination Location window, select the folder where SMP is installed.  
   Note - The path cannot contain any blank spaces.  
   Click Next.
5. In the Setup Type window, click Typical Primary.
   Note - Select Restore from backup to restore SMP settings from a back-up file.
   Click Next.
7. In the Is Active Directory installed locally message window, click Yes.
8. In the Primary Database Information window, configure the Active Directory settings:
   a) Make sure that the Domain is correct.
   b) Enter the User settings for AD user that you created.  
      Note: Make sure that you enter the correct CN for the AD user.
   Click Next.
9. In the Password window, enter the password for the AD user that is the user for the Domain Admin and Schema Admin groups.
10. Click Next.
11. Enter the login credentials for the Check Point Security Management Server administrator account.
12. Click Next.
13. Click Next.
14. In the Secondary Database Information window:
   • If there is no secondary server, make sure that the field is blank
   • For a deployment with a secondary server, enter the settings for a backup database for the SMP.
15. Click Next.
16. In the Installation Summary window, make sure that settings are correct. After you click Next, SMP is installed on the server.
17. Click Next.
   It takes a few minutes to install SMP on the server.  
   The wizard continues and you configure the SMP administrator and email settings for the SMP WebUI.
18. In the SMP Configuration window, enter the SMTP address and email address that SMP uses to send emails.
19. Click Next.
20. In the SMP Admin User Information window, enter the Username and Email address for the new SMP Administrator account.
21. Click Next.
22. Enter and Confirm the Password for the SMP Administrator that you created in the previous window.
23. Click Next.
24. In the Installation Complete window, click Finish.
   You do not need to restart the server.

Installing Multiple SMP Servers

Configure one or more secondary SMP Servers to provide High Availability and Load Sharing support for the SMP.

Each SMP Server must share the same AD domain. Configure each one as a separate domain controller.

Overview
1. Install AD on secondary server as a separate domain controller in the existing forest.
2. Configure the Primary SMP Server as the only DNS server.
4. In SmartDashboard, configure the Secondary Management object.
5. Install SMP on the secondary server.

Configuring DNS for Secondary SMP Servers

To install AD correction on the secondary SMP Server, the primary SMP Server must be configured as the only DNS server.

To configure the DNS server settings for the secondary SMP Server:
1. Click Control Panel > Network and Internet > Network Connections.
   The Network Connections window opens and shows the interfaces.
2. Right-click the interface and select Properties.
4. Click the DNS tab.
5. If there are DNS server addresses configured, select each one and click Remove.
6. Click OK.
7. In Use the following DNS server addresses, enter the external IP address of the primary SMP Server.
8. Click OK.
9. Click OK.
   The interface properties window closes.
Installing the Secondary Security Management Server

Install the Secondary R77.30 Check Point Security Management Server before you install the Secondary SMP. Make sure that you install the server in a distributed deployment. After you install the Security Management Server, you cannot change the Administrator password.

To learn more about how to install a Security Management Server, see the *R77.30 Installation and Upgrade Guide for Non-Gaia Platforms*.

This procedure is to install the Security Management Server for a deployment with multiple SMP Servers. For deployments that use multiple SMP Servers, you must configure the Security Management Server as a single Management server.

We recommend that you install the SMP in less than seven days after you install the Security Management Server.

To run the First Time Configuration Wizard for the Secondary Security Management Server:

1. Log in to the Secondary SMP Server.
2. From the R77.30 Security Management Server folder, run *Setup.exe* as an administrator.
3. In the Welcome window, click Next.
4. In the License window, accept the Check Point license.
5. Click Next.
6. In the Installation Options window, click New Installation.
7. Click Next.
   The deployment window opens.
8. Click Custom.
9. Click Next.
10. In the Check Point Security Gateway and Management window, select Security Management and SmartConsole.
11. Click Next.
12. In the Select Destination Folder window, click Next.
    The management window opens.
14. Click Next.
    The window shows that you selected to install the Security Management (Secondary) and SmartConsole products.
15. Click Next.
    The Security Management Server is installed.
16. In the license window, click Use Trial Period license.
17. Click Next.
18. In the Secure Internal Communication window, enter and Confirm the one-time Activation Key.
    Enter this key in SmartDashboard.
19. Click Next.
20. In the Check Point Configuration Tool window, click OK.
21. Click **Finish**.
22. Click **Yes**.

The wizard starts the Check Point services and completes the Secondary Security Management Server installation.

### Configuring the Secondary Management in SmartDashboard

In SmartDashboard, create SIC between the Primary and Secondary Security Management Servers to create a High Availability deployment.

**To configure the Secondary Security Management Server in SmartDashboard:**

1. Log in to SmartDashboard.
2. Right-click the Network Objects navigation tree, and select **Security Gateway/Management**.
3. In the **Check Point Security Gateway Creation** window, click **Classic Mode**.
4. Configure these server settings:
   - **Name** - Name for the Secondary Security Management Server object
   - **IPv4 Address** - IP address of the internal interface
   - **Hardware** - Open server
   - **Version** - R77.30
   - **OS** - Windows
5. Configure the Management Software Blades:
   a) From the **Network Security** tab, clear **Firewall**.
   b) Click the **Management** tab.
   c) Select these options:
      - Network Policy Management
      - Secondary Server
      - Logging & Status
      - Provisioning
6. Establish SIC between the Security Management Servers:
   a) Click **Communication**.
      The **Trusted Communication** window opens.
   b) Enter and confirm the One-time password that you entered in the **Secure Internal Communication** window.
   c) Click **Initialize**.
   d) Click **OK**.
7. Configure the logging module:
   a) From the navigation tree, click **Logs**.
   b) In the **Logs** page, click Enable **SmartLog**.
   c) From the navigation tree, click **Logs > Additional Logging Configuration**.
   d) Click **Accept Syslog messages**.
8. Click **OK**.
9. Click **Policy > Install Database**.
   The Secondary Security Management Server is configured.

### Installing the Secondary SMP

**To install a secondary SMP Server for High Availability:**

1. Start the First Time Configuration Wizard and configure the settings to install SMP on the secondary server.
2. In the **Setup Type** window, click **Typical Secondary**.
3. Configure the other settings in the First Time Configuration Wizard.

### Adding Log Servers to Synchronize the Logs

When SMP Servers are load-sharing, the gateways can send logs to the Standby servers. You must configure the Standby SMP Servers as Log Servers in SmartDashboard.

After you configure the Standby SMP to send logs to the Active SMP, you can show all the gateway logs in the SMP WebUI.

**To add synchronize the logs for an SMP deployment:**

1. On the Active SMP Server, log in to SmartDashboard.
2. From the navigation tree, click the Servers and OPSEC icon.
3. Right-click **OPSEC Application**, and select **New OPSEC Application**.
   The **OPSEC Application Properties** window opens and shows the **General** tab.
4. Configure the OPSEC Application settings:
   a) Enter these settings:
      - **Name**, **Comment**, and **Color** for the Standby SMP OPSEC object
      - **Host** - Select the network object for the Standby SMP
      - **Vendor** - Select **User defined**
      - **Client Entities** - Select **LEA**
   b) Click **Communication**.
   c) In the window that opens, enter an **Activation Key**.
   d) Click **Initialize**.
      The window shows: **Initialized but trust not established**.
   e) Click **OK**.
5. Click **Policy > Install Database**.
6. Open the CLI on the Active SMP Server.
7. Go to the directory: `%SMARTLOGDIR%`
8. Run this command to initiate SIC with between SMP Server and the Domain Log Server:
   
   ```
   opsec_pull_cert -h <Primary Server IP address> -n <OPSEC Application Name> -p <Activation Key> -o <Name of Certificate File>
   ```
   A message shows that communications is established with the SmartDashboard OPSEC object.
9. Go to the `log_servers` parameter in the file `%SMARTLOGDIR%\smartlog_settings.txt`. These are sample values for the `log_servers` parameter on the Active SMP Server:

```plaintext
:log_servers {
  :name (192.0.2.1)
  :log_files (all)
  :folder ("C:\Windows\FW1\R77.30\FW1\log")
  :is_local (true)
  :read_mode (FILES)
}
```

10. In the same file, add a new `log_server` parameter and configure these values to add a Domain Log Server:

- `name` - IP address of the Domain Log Server
- `log_files` - all
- `is_local` - false
- `certificate_file` - Name of the file you created with the `opsec_pull_cert` command and the `-o` parameter
- `sic_name_client` - The DN that is shown in the General tab for the OPSEC Application object
- `sic_name_server` - The SIC name for the Domain Log Server. Click Test SIC Status in the Domain Log Server object in SmartDashboard

This is a sample parameter for the new Domain Log Server:

```plaintext
: (name (192.168.68.177)
  :log_files (all)
  :is_local (false)
  :certificate_file (Glottis_SL.p12)
  :sic_name_client ("CN=Glottis_SL,O=MANNY.calavera.local.zfpdre")
  :sic_name_server ("CN=cp_mgmt_GLOTTIS,O=MANNY.calavera.local.zfpdre")
  :read_mode (LEA)
)
```

11. Perform the previous steps again for each additional Standby SMP Server.

12. Open `%SMARTLOGDIR%\conf\smartlog_settings.conf`

13. Copy the parameter and value for `log_buffer_count`

14. Paste the `log_buffer_count` parameter to `%SMARTLOGDIR%\smartlog_settings.txt` and increase the value by 1 for each additional Standby SMP Server.

15. From the CLI on the Active SMP Server, run:

   ```plaintext
   smartlogstop
   smartlogstart
   ```

## Installing SMP on a Server with a Legacy Version

You can only install one version of the SMP on a server. If your server already has SMP version R8.1 or earlier installed, you must uninstall it before you can install the new version.

**To install R12.20 SMP on a server with a legacy version:**

1. Uninstall the legacy SMP.
2. Install the R12.20 SMP.
Logging in to the SMP

If you see a warning that the certificate for this site is not trusted, click Continue to safely use the SMP WebUI.

If SMP Server is located behind a NAT device, you can only log in to the SMP WebUI from that same server. After you configure the SMP to use the external NATed IP address, you can remotely log in to the SMP.

These Internet browsers are supported:

- Firefox
- Chrome
- Internet Explorer 9 and higher

To log in to the SMP:

1. If SMP Server is located behind a NAT device, log in to SMP Server.
2. From the Internet browser,
   - If you use the Check Point Cloud Services, go here https://smbmgmtservice.checkpoint.com/SMP
   - If you use a local server, go to https://<SMP Server IP address>/SMP or https://<SMP Server domain>/SMP

   The Check Point Security Management Portal login window opens.
3. From Domain, select or enter your Service Domain.
   For a new installation, there are no Service Domains to select.
4. Enter the Username and Password.
5. Click Login.

   The SMP WebUI opens.

   If this is the first time you log in to the SMP, the Create New Service Domain wizard opens.
6. Configure the settings.
7. Click Finish.

   The new Service Domain opens and shows the General page.
8. Optional - If you applied the SMP license, authorize the permanent license for the map.
9. If SMP Server is located behind a NAT device, configure these settings:
   a) From the navigation tree, select SMP Servers.
   b) From the Server Name column, click SMP Server.
   c) From the Server Edit navigation tree, click Settings.
   d) In SMP NAT Address (external IP address), enter the NATed IP address.
   e) Click Save.
   f) From the Windows Start menu, select Administrative Tools > Services and restart the Apache-Catalina service.

For more information about how to configure the SMP and use Service Domains to manage gateways, go to Implementing SMP in the SMP Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=49605.
Activating the Map License

The SMP Map View window includes a 30-day temporary license. You must activate the temporary license for each SMP session. The functionality of the Map window is the same with the temporary and permanent license. The same license is used for the SMP and gateway Map View windows.

After you add the permanent license to the SMP, you can activate the license for the Map View window.

To activate the permanent Map license:
1. Go to Home > Map.
   The window opens and shows the Map Permission Error message.
2. Click activation request.
   An email message opens with the necessary details to activate the Map license. The To address in the email is: smbmgmtservice@checkpoint.com
3. Optional - In SMP DNS name, enter additional DNS settings.
4. Send the email to Check Point.
   It can take time for Check Point to add apply the Map license for your SMP account.

To use the temporary Map license:
1. From the Map View window, click Continue in trial mode.
   The temporary license is only valid for 30 days.
2. Optional - To activate the permanent license, click Resolve.
   The SMP shows the Map Permission Error message.
Uninstalling the SMP

When you run the SMP Installation wizard, it automatically detects that the SMP is installed on the server. Use the Uninstall wizard to remove the SMP from the Windows server.

To uninstall the SMP:

1. Run the installer package Setup.exe
   The Installation wizard detects that the SMP is already installed on the server.
2. From the Uninstall window, select Uninstall.
3. Click Next.
4. Select Completely remove SMP data from database to remove all the SMP data.
5. If you want to keep the SMP installation logs, clear Completely remove SMP installation logs.
6. Click Next.
7. For a secondary SMP Server, in Host enter the hostname or IP address of the primary SMP Server.
8. Click Next.
9. In the confirmation window, click OK.
   The server deletes the SMP and then restarts.
Managing Licenses

The SMP and the Security Management Server each have a 15 day trial license that is activated when you install them on the server. We recommend that you install the SMP license before the trial license expires.

Overview - SMP License for a New Deployment
1. Install the SMP on the server.
2. Log in to the Check Point User Center and activate the license.
3. Within the next 15 days, open the SMP WebUI and install the license.

Showing the SMP License

The SMP is licensed to manage the specified number of gateways. Add additional licenses to increase the number of managed gateways.

For deployments with multiple SMP Servers, we recommend that you use the CLI or Check Point Configuration Tool to add licenses to Secondary servers. See Managing Licenses without the WebUI

Note - Make sure that the IP address for the license is a real IP address for an interface that is configured on SMP Server. Do not use 127.0.0.1 as the IP address for the license.

To show the SMP system license:
1. Go to System > Settings.
2. Click License Management.
3. Click View License.

To add a license:
1. Go to System > Settings > License Management > View License.
2. Click Add License.
   The Add SMP License wizard opens.
3. For IP address, enter the SMP Server IP address.
4. For Expiration date, enter the date that the SMP license expires.
5. For Signature, copy and paste the string for the license.
6. For SKU, copy and paste the SKU for the license.
7. Click Finish.
8. Click **Apply License**.
9. Click **Save**.

### Using a Dynamic DNS Deployment

The SMP can provide dynamic DNS resolution for gateways even when they use dynamically allocated IP addresses. This feature lets users log in to the WebUI of an appliance when the IP address changes.

**Note** - Make sure that the interface has two IP addresses.

### Overview of Dynamic DNS and SMP

The Dynamic DNS feature uses a second IP address on SMP Server that resolves to a domain name. The SMP uses this domain name and assigns each gateway a unique URL in the format `<gateway name>.<domain name>`. For example, `mygateway.sample.com`.

You must configure the domain name to resolve to the Dynamic DNS address before you enable this feature.

#### Sample Dynamic DNS Workflow

1. An end-user wants to log in to the gateway. The end-user enters the Dynamic DNS URL in an Internet browser.
2. DNS servers resolve the Dynamic DNS name and the request is sent to SMP Server.
3. The SMP converts the Dynamic DNS name to the actual IP address for the gateway.
4. The SMP sends the IP address to the end-user’s Internet browser.
5. The end-user logs in to the gateway.

### Configuring the DNS Server

Before the SMP can use the Dynamic DNS feature, you must configure the DNS records. These records enable the gateway URLs to resolve to the correct subdomain. The DNS server resolves the DNS name and DNS domain of the SMP. This server is usually the DNS server for the company, or is managed by a domain registrar (for example GoDaddy).

The subdomain is a different section of the name server hierarchy for the SMP domain. The Dynamic DNS names for the gateways are placed in the subdomain.

Configure these DNS records:

- **A Record** - Maps the SMP host name to the IP address
- **NS Record** - Maps the subdomain to the SMP domain

Each Service Domain must use a different subdomain which is registered to your company.

To configure the subdomain for a Service Domain:

1. Go to **Service Domain > Settings**.
   - The **General** page for the Service Domain opens.
2. From the Settings tree, click **DNS**.
3. In **Domain Suffix**, enter the subdomain.
4. Click **Save**.
Sample DNS Server Records

These are sample A and NS Records for this deployment:

- Server domain - smpmgmt.sample.com
- External IP address - 192.168.8.10
- Subdomain - smpddns.sample.com

A Record - smpmgmt.sample.com IN A 192.168.10

NS Record - smpddns.sample.com IN NS smpmgmt.sample.com

In this subdomain, the Dynamic DNS name for the gateway mygw1 is:
mygw1.smpddns.sample.com

Preparing SMP Server (Dynamic DNS)

Before you configure Dynamic DNS for the SMP, you must configure these settings on SMP Server:

- Make sure that port 53 is open for TCP and UDP traffic
- Create a second IP address on the interface

The second IP address is used only for Dynamic DNS traffic.

You must register your domain to enable Dynamic DNS. Use a sub-domain that the company maintains, for example mycompany.smbservice.sample.com

To configure the secondary IP address on the server:

1. From the Windows Start menu, search for Network Connections.
   The Network Connections window opens.
2. Right-click the interface and select Properties.
   The interface Properties window opens.
4. Click Advanced.
   The Advanced TCP/IP Settings window opens.
5. Click Add.
   The TCP/IP Address window opens.
6. Configure the IP address and Subnet mask for the Dynamic DNS IP address.
7. Click Add.
8. Click OK.
Configuring DNS Settings for Service Domains

To enable the Dynamic DNS services, you must configure the DNS settings.

To configure the DNS settings:

1. Go to Service Domain > Settings.
   The Settings page opens and shows the General tab.
2. Click DNS.
   The DNS fields show:
3. For Domain Suffix, enter the DNS suffix for the SMP domain registration.
4. For Dynamic IP Time to Live, enter the number of seconds that a dynamic IP address remains in the DNS server’s cache after resolution. A longer time reduces the load on the server. A shorter time makes sure there is less downtime when you change IP addresses.
5. For Static IP Time to Live, enter the number of seconds that a static IP address remains in the DNS server cache after resolution. Static IP addresses include gateways configured with static IP addresses and mail servers (MX records). A longer time reduces the load on the server.
   Note - This is the DNS server for the SMP. It is not the DNS server that is used for Dynamic DNS.
6. Click Save.

Configuring SMP Server for Dynamic DNS

Configure the interface on the server to let the SMP use the Dynamic DNS IP address to communicate with the gateways.

To configure the interface for Dynamic DNS traffic:

1. From the Windows Start menu, click Search.
2. Enter DNS and double-click.
   The DNS management window opens.
3. Click Action > Properties.
4. From the Interfaces tab, configure the Listen on setting to Only the following IP addresses.
5. Select the IP address that is the SMP IP address.
6. Click OK.

Configuring Dynamic DNS in the SMP WebUI

To configure Dynamic DNS in the WebUI:

1. Go to System > SMP Servers.
2. Click SMS Global Settings.
3. From the General page, click DRM.
4. Click Save.
5. Click Actions > Back.
6. From the Server Name column, click SMP Server.
   The Server Edit window opens and shows the General page.
7. From the Server Edit navigation tree, click SMS Module > SMS Settings.
   The General Settings page opens.
8. From the **Server Name** column, click the IP address. The **Edit Server Address** window opens.

9. In **Server name/IP**, enter the Dynamic DNS IP address.

10. Click **Finish**.

11. Click **Save**.

   Dynamic DNS is configured for SMP Server.

**To configure Dynamic DNS for gateways:**

1. Create a plan that includes the Dynamic DNS service. Select the **Dynamic DNS** service on the applicable page in the **Plan** wizard.

2. Assign gateways to the Plan.

3. **Optional** - Configure the DNS settings for each gateway. These settings let you define additional DNS aliases to access the gateway.

---

**Installing an SSL Certificate for the SMP**

Install an SSL certificate to increase the security of the SMP deployment. If you do not install a certificate, SMP Server uses the default internal certificate that is not signed.

When you install a publicly trusted certificate:

- A certificate warning is not shown when you connect to the SMP.
- A certificate warning is not shown the first time that you connect to a gateway.
- Some Internet browsers (for example Chrome) cache web resources and can improve the performance of the WebUI.

To learn more about how to install the SSL certificate on a web server, see the Tomcat documentation [https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html](https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html).

**To install a certificate:**

1. If necessary, create a PKCS12 file of the certificate for your organization.

   **Note** - You can also use OpenSSL [http://www.openssl.org](http://www.openssl.org) to create the file. Perform these steps:

   a) Make sure that these files for the certificate are configured correctly:

      i) **CER file** is a certificate signed by a CA.

         The content in this file must start with **-----BEGIN CERTIFICATE-----** and end with **-----END CERTIFICATE-----**

      ii) **KEY file** is the private key of the server.

         The content in this file must start with **-----BEGIN RSA PRIVATE KEY-----** and end with **-----END RSA PRIVATE KEY-----**

   b) Create one PKCS#12 file from the certificate and the key. Run the command:

      ```
      openssl pkcs12 -export -in <CER file name> -inkey <KEY file name> > certificate.p12
      ```
2. Enter the password for:
   - The KEY file (if necessary, ask the creator of this file for help with the password)
   - The newly created PKCS#12 file

   A new PKCS#12 file named certificate.p12 is created
3. On SMP Server, run this command to import the PKCS#12 file into a Java keystore:
   
   ```
   keytool -importkeystore -srckeystore certificate.p12 -srcstoretype pkcs12 -destkeystore certificate.jks
   ```
4. Enter the password for:
   - The newly created Java keystore
   - The source keystore password that you entered when you created the PKCS#12 file

   The keystore file named certificate.jks is created.
5. Copy the certificate.jks file to %SMP_HOME%\Tomcat\conf on SMP Server. [The default directory is C:\Checkpoint\SMP\Tomcat\conf]
6. From the same folder, edit server.xml.

   Find the connector that contains the keystoreFile parameter, and edit it to include the keystore name and password for your organization. For example:

   ```xml
   <Connector compression="on" compressionMinSize="2048"
   noCompressionUserAgents="gozilla,
   traviata" compressableMimeType="text/html,text/xml,text/plain,text/css,text/
   javascript,text/json,application/javascript"
   SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" server="Apache"
   keystoreFile="C:\CheckPoint\SMP\Tomcat\conf\certificate.jks"
   keystorePass="password" />
   ```
Failover from Primary to Secondary SMP Server

In This Section:

- Overview of SMP Failover
- Changing the Secondary Security Management Server to Active
- Setting the Primary SMP to Standby
- Setting the Secondary SMP to Active
- Creating a New Administrator
- Failover from the Secondary to Primary SMP Server

Perform a failover if the Primary SMP Server fails, or it is necessary to change to the Secondary SMP Server.

Overview of SMP Failover

When you perform a failover from the Primary to Secondary server, change these SMP Server components:

- Security Management Server
- SMP

After a failover, perform a similar procedure to change back to the Primary SMP Server.

Note - You cannot use the SMP WebUI during the failover.

Overview of Failover Procedure

2. Change the Secondary SMP as the Active SMP Management.
   a) Set the Primary SMP to Standby.
   b) Set the Secondary SMP to Active.
3. Update the DNS server to resolve to the IP address for the Secondary SMP Server.
Changing the Secondary Security Management Server to Active

Use SmartDashboard to log in to the Secondary Security Management Server and then change it to the active server.

**Note** - If you cannot connect to the Security Management Server with the administrator account, use the Check Point Configuration Tool to create a new administrator.

To change the Secondary Security Management Server to Active:
1. Use SmartDashboard to log in to the Secondary Security Management Server.
   The **Secondary Server Login** window opens.
2. Click **Change to Active**.
   A confirmation window opens.
3. Click **Yes**.
   The primary Security Management Server is in Standby mode and the Secondary one is Active.
4. Exit SmartDashboard.

Setting the Primary SMP to Standby

On the Primary SMP Server, edit the `INFO.properties` file to change the state from Active to Standby.

To set the Primary SMP to Standby:
1. From the Primary SMP Server, open `C:\CheckPoint\SMP\Tomcat\webapps\SMP\WEB-INF\INFO.properties`
2. Change the value for `SMP_Type` to `standby`.
3. Save the file.
4. Restart the Apache-Catalina service:
   a) From the **Start** menu, click **Administrative Tools > Services**.
      The **Services** window opens.
   b) Right-click **Apache-Catalina**, and select **Restart**.

Setting the Secondary SMP to Active

On the Secondary SMP Server, edit the `INFO.properties` file to change the state from Standby to Active.

To set the Secondary SMP to Active:
1. Log in to the Secondary SMP Server.
2. Open `C:\CheckPoint\SMP\Tomcat\webapps\SMP\WEB-INF\INFO.properties`
3. Change the value for `SMP_Type` to `active`.
4. Save the file.
5. Restart the Apache-Catalina service:
   a) From the Start menu, click Administrative Tools > Services.
      The Services window opens.
   b) Right-click Apache-Catalina, and select Restart.

Creating a New Administrator

If you cannot use the administrator credentials from the Primary Security Management Server to log in to the Secondary one, use the Check Point Configuration Tool to create a new administrator for the Secondary Security Management Server.

To create a new administrator with the Check Point Configuration Tool:
1. Log in to the Secondary SMP Server.
2. From the Start menu, click All Program Files > Check Point SmartConsole R77.30 > Check Point Configuration.
   The Check Point Configuration Tool opens and shows the Licenses and contracts page.
3. Click the Administrator tab.
4. Click Add.
   The Add Administrator window opens.
5. Enter the Administrator Name.
6. Enter and confirm the Password.
7. Click OK.
8. From the Administrator tab, click OK.
   The new administrator is added to the Security Management Server.

Failover from the Secondary to Primary SMP Server

Perform a failover to change back to the Primary from the Secondary SMP Server.
Follow the steps for the failover from Primary to Secondary, but change:
• The Secondary server from Active to Standby
• The Primary server from Standby to Active

To change from the Secondary to the Primary SMP Server:
1. Configure the Primary Security Management Server as the Active server.
2. Change the Primary SMP as the Active SMP Management.
   a) Set the Secondary SMP to Standby. Change the value of the property SMP_TYPE to standby.
   b) Set the Primary SMP to Active. Change the value of the property SMP_TYPE to active.
3. Update the DNS server to resolve to the IP address for the Primary SMP Server.
Back up and Restoring the SMP Database

In This Section:

- Configuring SMP Backup Settings ................................................................. 35
- Starting the SMP Backup ................................................................................... 36
- Restoring SMP Server on a New Server .......................................................... 36

Use the SMP WebUI to back up the SMP database. You must run the SMP First Time Configuration Wizard to restore the SMP from a back-up file.

Configuring SMP Backup Settings

System backup settings are used for both automatic and manual SMP configuration backup.

To save the back-up file:

- For SMP Servers located in the Check Point Cloud Services, upload the back-up file to an FTP server.
- For on-site SMP Servers, you can upload the file to an FTP server or save it to a local folder. The default path is the installation folder: c:\Checkpoint\SMP\n
To configure SMP backup settings:

1. Go to System > Settings.
2. Click System Backup.
3. To enable automatic backups, click Perform and select the time frame:
   - Daily
   - Weekly
   - Monthly
4. In File Storage, select Upload backup file to FTP.
5. Enter the FTP server, Path on server, and Password
   Or
   Click Save the file and enter the path.
6. In File Name, select Automatically generate filename or Use static filename.
7. If you select Use static filename, enter the Filename for the backup file.
8. Select Overwrite file if already exists.
   
   Note - If there is a backup file with the same name, the backup operation stops if you do not select this option.
9. Click Save.
Starting the SMP Backup

To manually start the SMP system backup status:
1. Go to System > Settings.
2. Click System Backup > Status.
3. Click Run Now.
   A confirmation window opens.
4. Click OK.
5. To refresh the fields, click Refresh.

Restoring SMP Server on a New Server

Run the First Time Configuration Wizard to restore saved SMP settings to a new server.

When you run the First Time Configuration Wizard, make sure that the information for these settings is the same as the original SMP Server:

- AD and Security Management Server administrator accounts
- IP addresses for the SMP interfaces

**Note** - Do not use this procedure when you restore settings to a server with the SMP already installed.

You must apply the SMP license again after you restore the settings.

To restore SMP Server from a back-up file:
1. Run the SMP First Time Configuration Wizard.
2. In the Setup Type window, select Restore from backup.
3. Complete the steps in the First Time Configuration Wizard.
   The previous settings are restored to the SMP.
4. Add the SMP license.
Adding the SMP License

To add a license from the WebUI:
1. Click View License.
2. Click Add License.
   The Add SMP License wizard opens.
3. Configure these settings:
   • **IP address** - Enter the SMP Server IP address.
   • **Expiration date** - Enter the date that the SMP license expires.
   • **Signature** - Copy and paste the string for the license.
   • **Number of Gateways** - Maximum number of gateways that the SMP can manage.
   • **SKU** - Copy and paste the SKU for the license.
4. Click Finish.
   The wizard closes.
5. Click Apply License.
   The settings for the license are applied to the SMP.
6. Click Save.
Troubleshooting the Installation

In This Section:

Common Troubleshooting Scenarios .................................................................38
Troubleshooting SMP Licenses ........................................................................38
Restoring SMP Settings on the Same Server .....................................................38

Common Troubleshooting Scenarios

I cannot add gateways to the SMP
Make sure to activate the SMP license within 15 days.

I changed the time zone on SMP Server, but SMP does not show the new time
You must restart the SMP to update the time zone. From the Windows Start menu, select Administrative Tools > Services and restart the Apache-Catalina service.

Troubleshooting SMP Licenses

The SMP includes a 15 day trial license which is activated when you install it on the server. The SMP also uses a Security Management Server to manage the gateways. The license for this server is automatically installed when you activate the SMP license.

If the trial license for the SMP expires, the license for the Security Management Server cannot be activated when you activate the SMP license.

For information on how to activate the license for the Security Management Server, contact Check Point Technical Support http://supportcenter.checkpoint.com.

Restoring SMP Settings on the Same Server

To restore the SMP settings from a back-up file to the same SMP Server, you must first uninstall the SMP.

Run the First Time Configuration Wizard to restore the saved SMP settings to a new server.

When you run the First Time Configuration Wizard, make sure that the information for these settings is the same as the original SMP Server:

• AD and Security Management Server administrator accounts
• IP addresses for the SMP interfaces

To restore the SMP settings on the existing server:

1. Uninstall the SMP from the server.
2. In the Setup Type window, select Restore from backup.
3. Complete the steps in the First Time Configuration Wizard.
   The previous settings are restored to the SMP.