Migration Guide

Revision A

McAfee Next Generation Firewall

Firewall Enterprise to McAfee NGFW upgrade tool 1.1

Overview

This guide describes how to use an upgrade tool to migrate policy from a McAfee® Firewall Enterprise (Firewall Enterprise) appliance to a McAfee® Next Generation Firewall (McAfee NGFW) appliance. With this upgrade tool, you can move key policy elements from Firewall Enterprise version 7.0.1.03 or 8.3.2 to McAfee NGFW version 5.7.

Introduction to the upgrade tool

The upgrade tool captures key policy elements, eliminating the need to manually re-create them. The tool provides an upgrade from a high assurance firewall to a next generation firewall.

The upgrade process consists of several high-level steps.

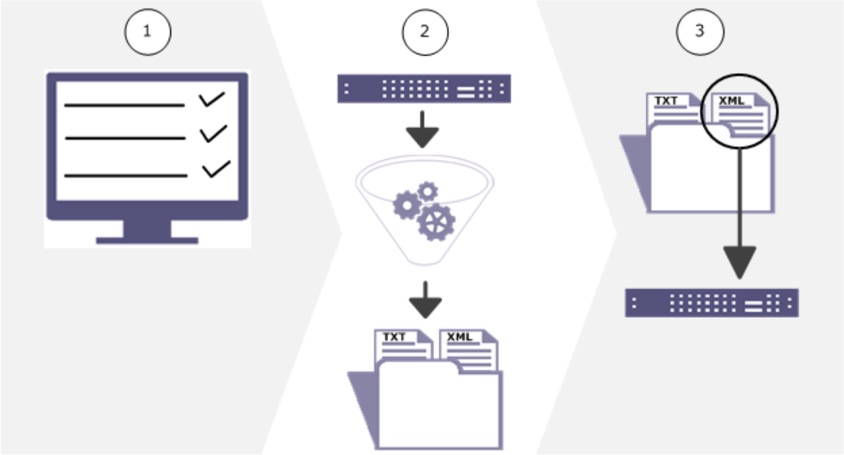

Figure 1 Upgrade steps

1 The Firewall Enterprise must be prepared for the upgrade by verifying product requirements, creating a configuration backup, and creating a policy report.

2 The upgrade tool is applied to the firewall or McAfee® Firewall Enterprise Control Center (Control Center) as a patch. When the tool has been run on the firewall, it generates a .zip file.

3 The .zip file contains an upgrade log report and an .xml file. The .zip file is imported into the Security Management Center (SMC), where the SMC uses the .xml file to create policy elements. After the elements are imported, Professional Services can assist you to create a McAfee NGFW template.

How Firewall Enterprise processes traffic

Firewall Enterprise combines a high assurance, application-layer firewall with these features to provide one security appliance.

- User-based policy
- IPsec VPN capabilities
- SSL decryption
- McAfee® Global Threat Intelligence™ (McAfee GTI)

How McAfee NGFW and SMC work together

McAfee NGFW is an application-aware, stateful inspection firewall that combines IPS and anti-evasion technology. McAfee NGFW firewalls are managed by SMC, a Java-based, centralized management system that can support hundreds of firewalls.

From the SMC Client you can:

- Access firewalls
- Review the audit
- Run reports
- Create policy templates

Templates are a unique concept in SMC. A *template* is a unit of policy comprised of rules built from network objects and services. Templates are created in SMC. You can mix and match top-level and sublevel templates by nesting them within other templates to create the policy hierarchy. These configurable templates provide you with several deployment options. After the full template is finalized, SMC pushes the policy and configuration to the firewall.

In this upgrade process, SMC is used to create the McAfee NGFW template from the upgraded Firewall Enterprise policy elements.

How the upgrade tool works

The upgrade tool converts firewall policy elements and configuration into a .zip file, including an upgrade log report.

The upgrade bundle contains:

- Policy elements in an .xml file that is compatible with SMC
- Firewall Enterprise configuration files for reference
- For managed firewalls, Control Center configuration files for reference
- An upgrade log report that details what policy elements were upgraded, what changes were made, and any elements that were not upgraded

To view configuration files, McAfee recommends opening them on a UNIX computer.

What elements are imported into SMC

These policy elements and configuration information are imported into the SMC.

- Network objects
  - IP addresses
  - IP address ranges

  - Subnets
  - Hosts
  - Netgroups
  - Control Center adaptive objects
- Routing addresses
- VPN addresses
- Zones or burbs
- Zone groups or burb groups

Reading the upgrade log report

The upgrade log report is a reference text file that you can use to review the results of the upgrade process.

After running the upgrade tool, an upgrade log report is generated. This report lists what can be upgraded, what changes were made, and what did not upgrade.

The report is in a .txt file without formatting. You can copy the text into a word-processing program for better readability.

```
----The following log describes the mapping of McAfee Firewall Enterprise (MFE)----
----          objects to Stonesoft Management Center (SMC) objects.            ----

----The following objects were created and renamed during the upgrade----
The MFE IP address '10.1.1.0' became SMC host '10.1.1.0-host'


----The following objects were deleted during the upgrade----
Dropped unsupported MFE domain 'fw.x.co.an' from the SMC configuration
Dropped unsupported MFE geolocation group '261fwexample' from the SMC configuration
Dropped unsupported MFE netmap '610 firewall ipaddr names' from the SMC configuration


----The following SMC objects were created during the upgrade----
The MFE vpn client pool address 'zoo' became SMC network 'net-80.20.4.0/24'
The MFE host 'fw.int.l.test' is used by the SMC domain_name 'fw.int.m.test'
The MFE host 'fw.int.m.test' became SMC domain_name 'fw.int.m.test'
The MFE IP address 'testing.ext.fw.test' became SMC host 'testing.ext.fw.test'
The MFE IP range '25.11.10.10-25.11.10.20' became SMC address_range '25.11.10.10-25.11.10.20'
The MFE netgroup '401fwname' became SMC group '401fwname'
The MFE static route '1.1.1.2/32' became SMC host 'host-1.1.1.2'
The MFE static route '12.12.0.0/14' became SMC network 'net-12.12.0.0/14'
The MFE static route '2607:A600:124:7628::FE/128' became SMC host
'host-2607:A600:124:7628::FE'
The MFE static route '4012:4567:FFFF:EF56::/64' became SMC network
'net-4012:4567:FFFF:EF56::/64'
The MFE gateway from the static route '3331::2/128' is used by the SMC router
'router-4014:AD:12:E453:5656:6AE4:7EE:FE'
The MFE gateway from the static route '40.01.2.2/32' is used by the SMC router
'router-52.88.88.254'
The MFE subnet '60.1.2.0' became SMC network '60.1.2.0'
The MFE vpn endpoint 'fw01' became SMC network 'net-80.2.1.0/24'
The MFE vpn endpoint 'ipv6-fw01' became SMC network 'net-5200:2:1:1::/64'
The MFE zone 'dmz' became SMC interface_zone 'dmz'
The MFE zone group '701fwexample' became SMC group '701fwexample'


----The following areas were not included in this upgrade----
The MFE auditbot, syslog, profiler, reporter, export, filters, smartfilter audit and generic
audit settings were not moved to the SMC configuration.
The MFE authenticators, external certs, firewall certs, SSH hosts CAs, CA groups and
authentication lockout settings were not moved to the SMC configuration.
```

```
The MFE active and passive passport settings were not moved to the SMC configuration.
The MFE LCA certs and state data were not moved to the SMC configuration.
The MFE policy agents, applications, application groups and custom applications were not
moved to the SMC configuration.
The MFE IPS attack and response settings were not moved to the SMC configuration.
The MFE application defenses and application defense groups were not moved to the SMC
configuration.
The MFE policy ACL rules were not moved to the SMC configuration.
The MFE policy SSL rules were not moved to the SMC configuration.
The MFE policy timeperiods were not moved to the SMC configuration.
The MFE policy GTI settings were not moved to the SMC configuration.
The MFE policy URL translations rules were not moved to the SMC configuration.
The MFE policy IPS settings were not moved to the SMC configuration.
The MFE VPN rules and settings were not moved to the SMC configuration.
The MFE ACLD settings were not moved to the SMC configuration.
The MFE antivirus scanner and server settings were not moved to the SMC configuration.
The MFE cmd settings were not moved to the SMC configuration.
The MFE crontabs were not moved to the SMC configuration.
The MFE dhcrelay, ePO, khd, NIA, NTP, shund, SNMP, SSH and UTT server settings were not
moved to the SMC configuration.
The MFE DNS server and named settings were not moved to the SMC configuration.
The MFE sendmail server settings were not moved to the SMC configuration.
The MFE cluster failover and Command Center settings were not moved to the SMC configuration.
The MFE configuration backup settings were not moved to the SMC configuration.
The MFE daemond settings were not moved to the SMC configuration.
The MFE FIPS settings were not moved to the SMC configuration.
The MFE interface, NIC, NIC group and QOS profile settings were not moved to the SMC
configuration.
The MFE license settings were not moved to the SMC configuration.
The MFE messages from McAfee settings were not moved to the SMC configuration.
The MFE package installation settings were not moved to the SMC configuration.
The MFE routes were not moved to the SMC configuration.
The MFE Smartfilter settings were not moved to the SMC configuration.
The MFE system sysclts were not moved to the SMC configuration.
The MFE system timezones were not moved to the SMC configuration.
The MFE system UPS settings were not moved to the SMC configuration.
The MFE administrative user account settings were not moved to the SMC configuration.
The MFE firewall users and usergroups were not moved to the SMC configuration.
The MFE external groups were not moved to the SMC configuration.
The MFE hardware acceleration settings were not moved to the SMC configuration.
The MFE auditdbd and usage report settings were not moved to the SMC configuration.
```

As part of the upgrade process, high ASCII characters might be removed from comment fields. If characters are removed, a message is logged in the report.

Known issues

For known issues in this product release, see KnowledgeBase article KB82694.

Before you begin

Verify that your appliances meet the requirements, create a configuration backup, and create a policy report.

Tasks

- *Check requirements* on page 5
  Download and review the product documentation to verify that your product meets the requirements.
- *Create a configuration backup* on page 5
  Backing up the firewall configuration provides a quick way to restore a firewall to a previous operational state.
- *Create a policy report* on page 7
  You can create a report of the comprehensive details of the original Firewall Enterprise policy, which is helpful in approximating that policy when creating templates.

Check requirements

Download and review the product documentation to verify that your product meets the requirements.

Task

1. Visit support.mcafee.com.
2. Download the appropriate documentation.
   - *McAfee Firewall Enterprise Release Notes*, version 7.0.1.03 or 8.3.2P03
   - *McAfee Next Generation Firewall Release Notes*, version 5.7
   - *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2
3. Verify that your product meets the requirements.

Create a configuration backup

Backing up the firewall configuration provides a quick way to restore a firewall to a previous operational state.

Tasks

- *Create a backup for an unmanaged firewall* on page 5
  You can back up configuration files to the Firewall Enterprise, a USB drive, or a remote system.
- *Create a backup for a managed firewall* on page 6
  For managed firewalls, the configuration backup must be created in the Control Center Client.

Create a backup for an unmanaged firewall

You can back up configuration files to the Firewall Enterprise, a USB drive, or a remote system.

> Disaster recoveries are disabled while the 70103NGFWUP5.7A upgrade patch is installed. Create a disaster recovery before upgrading or uninstall the patch to create a disaster recovery backup.

Task

1. Select **Maintenance | Configuration Backup**.
2. Select **Local McAfee Firewall Enterprise**.

3. Click **Backup now**.

   The **Filename and encryption** window appears.

4. [Optional] In the **File name** field, enter a name that can easily identify this configuration backup.

   A default name consisting of the firewall name plus the current date automatically populates this field.

5. Select a location for the backup file:

   - To save the backup file on the firewall, select **Disk**.
   - To save the backup file on a USB drive inserted in the USB port on the firewall, select **USB Flash Drive**.
     - Insert the USB drive before performing the backup.
     - Do not remove the USB drive from the firewall until the "Configuration backup successful" message appears.

6. [Optional] Enter a key to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).

   - This key is not saved. You must remember it. You are not able to restore the configuration file without this key.
   - You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.

   Enter the key again to verify.

7. Click **OK**.

   A "Configuration backup successful" message appears.

8. Click **OK**.

   The backup appears in the list of current local configuration backups.

> If the firewall has a custom modified /secureos/etc/config.conf file, McAfee recommends creating a manual backup of any files defined by the custom entries before starting the upgrade.

You have finished backing up a configuration file to the firewall.

Create a backup for a managed firewall

For managed firewalls, the configuration backup must be created in the Control Center Client.

Task

1. In the navigation pane, select **Maintenance**.
2. In the **Firewall Maintenance** tree, double-click the **Configuration Backup** node. The **Firewall Configuration Backup** window is displayed.
3. To create a backup of the configuration data for selected firewalls, select the checkbox that is associated with each firewall.

4 Click **Create Backup(s)** to store a backup copy of the firewall configuration for the selected firewalls on the Management Server. The **Confirm Backup** window is displayed.

5 You can edit the description or accept the default value. Then click **OK** to confirm this backup. A message is displayed indicating that this request has been sent to the firewall.

After the backup is complete, the **Description**, **Last Backup Date**, and **Last Backup By** column values are updated on this tab.

Create a policy report

You can create a report of the comprehensive details of the original Firewall Enterprise policy, which is helpful in approximating that policy when creating templates.

Tasks

- *View a policy report for an unmanaged firewall* on page 7
  The firewall policy report can be opened in a web browser.
- *View a policy report for a managed firewall* on page 7
  For managed firewalls, policy reports are viewed in the Control Center Client.

View a policy report for an unmanaged firewall

The firewall policy report can be opened in a web browser.

Task

1 Select **Monitor | Firewall Policy Report**.

2 Click the **Firewall Policy Report** link to open the report in a web browser.

View a policy report for a managed firewall

For managed firewalls, policy reports are viewed in the Control Center Client.

Task

1 In the navigation pane, select **Monitor**.

2 Click the **Reports** tab.

3 Select **Policy Report**. The **Policy Report** window is displayed.

4 Select a device, then click **Request Report**.

The report appears on the **Policy Report** page.

Upgrade tasks

There are several tasks required to create the upgrade bundle.

Tasks

- *Download the tool* on page 8
  The upgrade tool is available on the McAfee downloads page.
- *Upgrade the firewall* on page 8
  A firewall can be upgraded from the command line or, for a managed firewall, from the Control Center Client.
- *Import the upgrade bundle* on page 12
  The .zip file upgrades policy elements to the SMC.

Download the tool

The upgrade tool is available on the McAfee downloads page.

Task

1. In a web browser, navigate to www.mcafee.com/us/downloads/downloads.aspx.
2. Provide your grant number, then navigate to the appropriate product and version.
3. Download the appropriate upgrade package.
   - For unmanaged firewalls, download the appropriate tool for your environment.
     - **7.0.1.03** — 70103NGFWUP5.7A
     - **8.3.2P03** — 8.3.2NGFWUP5.7A
   - For firewalls managed by Control Center, download 532P04.

Upgrade the firewall

A firewall can be upgraded from the command line or, for a managed firewall, from the Control Center Client.

Select the option that is appropriate for your firewall.

Tasks

- *Upgrade an unmanaged firewall* on page 8
  Install the upgrade tool and run it from the command line to create the upgrade bundle.
- *Upgrade a firewall managed by Control Center* on page 11
  Managed firewalls must be upgraded from the Control Center Client application.

Upgrade an unmanaged firewall

Install the upgrade tool and run it from the command line to create the upgrade bundle.

The upgrade bundle is a .zip file that can be stored locally, on a USB drive, or in a remote location. This file is imported into the SMC; it contains the output .xml file, the upgrade log report, and firewall configuration files.

Tasks

- *Make the upgrade package accessible* on page 8
  To perform the upgrade, place the package where the firewall can access it.
- *Load the package* on page 9
  The upgrade package contains required updates for correctly installing the upgrade tool.
- *Install the package* on page 9
  Install the upgrade package to be able to run the upgrade tool.
- *Run the upgrade tool* on page 10
  The upgrade tool creates the upgrade bundle .zip file.

Make the upgrade package accessible

To perform the upgrade, place the package where the firewall can access it.

> The package must be available to one member of a High Availability (HA) pair.

Task

1. Extract the upgrade package.
2. Place the package where the firewall can access it. Choose one of these options:
   - **Local FTP site** — Place the package on an FTP site that the firewall has access to.
   - **HTTPS website** — Place the package on an HTTPS website that the firewall has access to.
   - **CD** — Place the package in a /packages directory on a CD, then insert the CD into the firewall CD drive.
   - **Directory on the firewall** — Use SCP to copy the package to the /home directory of your firewall administrator account.

     > To transfer files to the firewall using SCP, SSH access must be enabled on the firewall.

Load the package

The upgrade package contains required updates for correctly installing the upgrade tool.

Task

For option definitions, click **Help** in the interface.

1. In the Admin Console, select **Maintenance | Software Management**, then click the **Download Packages** tab.
2. Click **Perform Manual Load Now**.
3. Specify where the upgrade package is stored.
   a. From the **Load packages from** drop-down list, select the type of location where the package was stored.
   b. In the **Packages** field, type the name of the package.
      - **7.0.1.03** — `70103NGFWUP5.7A`
      - **8.3.2P03** — `8.3.2NGFWUP5.7A`

   c. Complete the remaining fields as appropriate.
   d. Click **OK**. A confirmation message appears.
   e. Click **Yes**. The firewall loads the package from the specified location. When the operation is complete, a message appears.
   f. Click **OK**.
4. Verify that the upgrade package is loaded on your firewall.
   a. Click the **Manage Packages** tab.
   b. Verify that the status of the upgrade package is **Loaded on <date>**.

Install the package

Install the upgrade package to be able to run the upgrade tool.

Task

For option definitions, click **Help** in the interface.

1. On the **Manage Packages** tab, select the appropriate package.
   - **7.0.1.03** — select **70103NGFWUP5.7A**

     > Disaster recoveries are disabled while the 70103NGFWUP5.7A patch is installed. Uninstall the patch to create a disaster recovery backup.

   - **8.3.2P03** — select **8.3.2NGFWUP5.7A**
2. Click **Install**. The **Manage Packages: Install** window appears.
3. Verify that **Install now** is selected, then click **OK**. A progress window appears.

   When installation is complete, the progress window closes.
4. Verify that the status of the package is **Installed on <date>**.

Run the upgrade tool

The upgrade tool creates the upgrade bundle .zip file.

> For HA pairs, run the tool on one member.

Task

1. From the command line, log on to the firewall.
2. Type `srole` to change to the Admn domain.
3. Enter the command:

   ```
   cf config backup location=<location> file=<file name> format=ngfw
   ```

   where *location* can be local, USB, or a remote option and *file name* is what you would like the .zip file to be named.

   For remote locations, specify the address, user, and password in the command. You can also specify the location directory. See the cf_config man page for details.
4. Move the upgrade .zip bundle from /var/backup/repository/ to a location that is accessible to the SMC Client.

> When the export is complete, do not alter the .xml file in the upgrade bundle. Changes to the file might cause the upgrade to fail.

Upgrade a firewall managed by Control Center

Managed firewalls must be upgraded from the Control Center Client application.

Tasks

- *Make the upgrade package accessible* on page 11
  Place the contents of the upgrade package where the Control Center Management Server can access it.
- *Load the package* on page 11
  Use the Control Center Client application to load the upgrade package on your Control Center Management Server.
- *Install the package* on page 12
  Use the Control Center Client application to install the upgrade package on a managed firewall.
- *Run the upgrade tool from Control Center* on page 12
  For managed firewalls, the upgrade tool allows you to select which domains to export and where to store the upgrade bundle.

Make the upgrade package accessible

Place the contents of the upgrade package where the Control Center Management Server can access it.

Task

1. Extract the upgrade .zip file.

   The .zip file contains the 532P04.tar file and a text file.

2. Place the upgrade 532P04.tar file where the Control Center Management Server can access it. Choose one of these options:

   - **Local FTP site** — Place the file on an FTP site.
   - **HTTP website** — Place the file on an HTTP website.

Load the package

Use the Control Center Client application to load the upgrade package on your Control Center Management Server.

Task

1. In the navigation pane, click **Control Center**, then click the **Control Center Updates** tab.
2. Click **Upload to Server using FTP/HTTP**.
3. From the **Protocol** drop-down list, select the type of location where the package was stored.
4. In the **File** field, type `532P04.tar`.
5. Complete the remaining fields as appropriate, then click **Upload**.

   The Control Center Management Server downloads the package. When the download is complete, a message appears.

6. Click **OK**.

Install the package

Use the Control Center Client application to install the upgrade package on a managed firewall.

Task

1. In the navigation pane, click **Control Center**, then click the **Control Center Updates** tab.
2. Select the **532P04** package, then click **Apply**. The Control Center Client disconnects.
3. Reconnect and log on again to the Control Center Client. A **Download Package** window appears.
4. Click **Yes**. The update is downloaded. An **Install Package** window appears.
5. Click **Yes**. The **InstallShield** wizard appears.
6. Click **Next**. The installation begins. A status bar indicates the progress of the installation.

   When the installation is done, the **Update Complete** window appears.
7. Click **Finish** to complete the installation. The Control Center Client restarts.
8. Reconnect to the Control Center Client.

Run the upgrade tool from Control Center

For managed firewalls, the upgrade tool allows you to select which domains to export and where to store the upgrade bundle.

Task

1. Log on to the Control Center Client application.

   > ℹ Administrators must have two types of permission, one to run the tool and another to make a domain available for export. To run the tool, **Update** permission is needed for **System Objects** in the **Administrator** domain. To export a domain, the administrator must have **View** permission on **All Objects** in that domain.

2. In the navigation pane, select **Control Center | NGFW Upgrade**.

   The **NGFW Upgrade** window opens.
3. Select the domain to export.

   > ! The **Shared** domain must be exported and imported into the SMC shared domain first, so that objects in other domains map correctly.

   McAfee recommends importing one domain at a time. Match each domain to the equivalent domain on the SMC to create similar policy to the Control Center and reduce conflicts during import. Only the active domain version is migrated.
4. Select the location to store the upgrade bundle.
5. Click **Export**.

> ! When the export is complete, do not alter the .xml file in the upgrade bundle. Changes to the file might cause the upgrade to fail.

Import the upgrade bundle

The .zip file upgrades policy elements to the SMC.

> **Before you begin**
> The SMC must be installed and running.

Task

1. From the SMC Client, select **File** | **Import** | **Import Elements**.
2. Select the upgrade bundle .zip file and click **Import**.

   The SMC shows which elements are imported as new elements, which ones were already there, and where it found conflicts with existing elements.
3. If any import conflicts are identified in the .xml file, review and resolve them before proceeding with the import.
4. Click **Continue** to accept the changes.
5. When complete, click **Close**.

The imported policy elements can now be used to build rules and create templates in the SMC. For more information, see the *McAfee SMC Administrator's Guide*, version 5.7.