Migration Guide

Revision A

McAfee Firewall Enterprise

version 7.0.1.03 to 8.1.2

The *McAfee Firewall Enterprise Migration Guide* describes how to migrate a McAfee® Firewall Enterprise (hereinafter Firewall Enterprise) appliance from version 7.0.1.03 to version 8.1.2.

You can find additional information by using the resources listed in the following table.

Table 1 Product Resources

Resource	Location
Online Help	Online Help is built into Firewall Enterprise and Control Center. • **Firewall Enterprise** — Click **Help** on the toolbar or from a specific window. • **Control Center** — Press **F1**.
McAfee Technical Support ServicePortal	Visit mysupport.mcafee.com to find: • Product documentation • Product announcements • Technical support • KnowledgeBase
Product updates	Visit go.mcafee.com/goto/updates to download the latest Firewall Enterprise patches.
Product installation files	1 Visit www.mcafee.com/us/downloads. 2 Provide your grant number, then navigate to the appropriate product and version.

About this migration

This process migrates the Firewall Enterprise 7.0.1.03 policy to version 8.1.2 and installs version 8.1.2 on your firewall.

Version 7.x and 8.x comparison

There are a few key differences in the way version 8.x and 7.x firewalls process traffic.

Firewalls at version 7.x process traffic based on services, which are defined by port and protocol. Firewalls at version 8.x process traffic based on application identities, which are defined by port, protocol, and the data within the network packets. Sessions are inspected for application data. McAfee AppPrism™ is the technology that allows for an application-based policy.

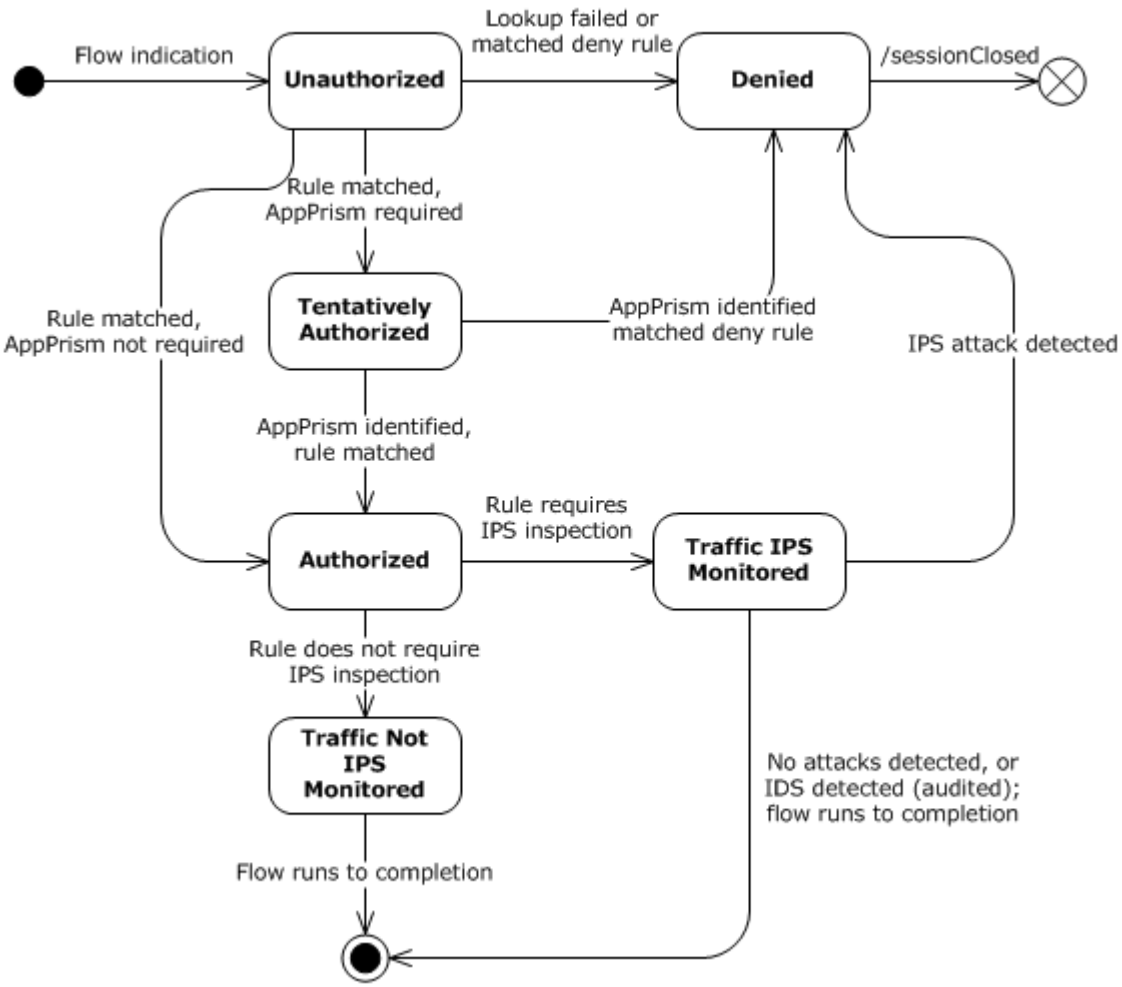

Figure 1 Version 8.x data flow

For complete information about version 8.x, see the *McAfee Firewall Enterprise Product Guide*.

Migration process overview

During the upgrade process, the 70103UP812 migration software converts the existing policy, and the firewall backs up the existing policy and installation.

Installation process

You can expect the installation to affect the firewall in several ways.

- The firewall continues to operate normally until installation is complete and the firewall restarts.
- The 70103UP812 migration software runs, and the policy is converted to version 8.1.2.

  During the migration process, the firewall performs these tasks:

  - Inserts TCP deny rules after HTTP allow rules to preserve the behavior of the 7.0.1.03 policy
  - Converts bidirectional rules into two unidirectional rules
  - As needed, splits rules with service groups into multiple rules to preserve the network behavior

  The firewall does not perform these tasks:

  - Migrate unused default services that are not used in the policy rules
  - Create predefined Application Defense profiles and groups

  A number of validations are performed before and after installation to detect policy issues that cannot be automatically migrated. For an explanation of these issues, refer to KnowledgeBase article KB74054.

- A backup of the 7.0.1.03 configuration is made and saved on the firewall as Pre-Install.<*date-stamp*>.
- A copy of the current installation is made and placed on the inactive (alternate) slice of the disk. The migration installation runs in a protected (chroot) environment on the inactive slice.

Post-installation

After installation completes on the inactive slice and the migration software has been successfully applied, a policy validation is performed.

- If errors occur during the migration or the final policy validation, the errors are logged to the /var/packages/statusX/install_output file for the inactive slice (where x is the slice number) and potentially in the audit log. For instructions on determining the slice number of the inactive slice, see *View the install_output file for the migration*.
- If no error occurs, the firewall restarts at version 8.1.2.

While the firewall restarts, the newly migrated policy is applied for the first time. If errors occur, the firewall automatically reverts to version 7.0.1.03.

Migration options

You can upgrade from version 7.0.1.03 to version 8.1.2 using Firewall Enterprise or Control Center.

These interfaces are supported:

- Firewall Enterprise Admin Console
- McAfee® Firewall Enterprise Control Center (hereinafter Control Center) Client application

The firewall must be at version 7.0.1.03. If the firewall is at an earlier version, refer to the appropriate migration kit instructions for instructions to migrate the firewall to version 7.0.1.03.

Unsupported features

Two features are unavailable after migration.

Firewall Enterprise version 8.x and later does not support:

- **CAC authenticator certificate validation with OCSP** — Common Access Card (CAC) configuration is not supported for certificate validation. The related configuration items on the CAC authenticator have been removed.
- **SNMP** — Cryptographic algorithms cannot be configured for SNMPv3 users. After the migration, the algorithms revert to MD5 authentication and DES privacy, regardless of their settings in 7.0.1.03.

Known issues

For known issues in this product release, refer to KnowledgeBase article KB74054.

Before you begin

You must disable or prepare several features of the firewall prior to migration. If these changes are not made, the migration could fail or have errors.

Tasks

- *Disable FIPS mode* on page 4
  Disable FIPS mode before you migrate.
- *Remove SafeWord authenticators* on page 4
  Replace all SafeWord® authenticators with RADIUS authenticators, then delete all SafeWord authenticators.
- *Modify Application Defenses* on page 5
  Prepare the Application Defenses for the migration.
- *Modify network objects* on page 5
  Prepare the network objects for the migration.
- *Modify services* on page 5
  Prepare the services and service groups that are used by active rules.
- *Modify rules* on page 6
  Modify rules for the migration.

Disable FIPS mode

Disable FIPS mode before you migrate.

Migrations to version 8.1.2 are not supported for firewalls with FIPS enabled. If FIPS mode is enabled, the migration fails.

Remove SafeWord authenticators

Replace all SafeWord® authenticators with RADIUS authenticators, then delete all SafeWord authenticators.

Version 8.1.0 and later versions do not include support for SafeWord. For detailed instructions on how to configure RADIUS access, see KnowledgeBase article KB70883.

Modify Application Defenses

Prepare the Application Defenses for the migration.

Task

1. Limit the IP address ranges in the SMTP Application Defense to 256 addresses.

   Version 8.1.2 does not support IP address ranges in the mail message recipients list within the SMTP Application Defense.

2. Verify SSL settings for decrypting HTTPS Application Defenses.
   - **DSA certificate** — If the Application Defense uses this type of certificate, select SSL3, TLS1, or both.

     Version 8.1.2 does not allow SSL2 to be selected with a DSA certificate.
   - **RSA certificate** — If the Application Defense uses this type of certificate, select at least one SSL or TLS version.

     Version 8.1.2 does not allow an RSA certificate with no SSL or TLS version selected.

Modify network objects

Prepare the network objects for the migration.

Task

1. Make sure each group object contains at least one member object. This applies to netgroups, user groups, service groups, and burb groups.

   If any of these group objects are empty during the migration, version 8.1.2 does not allow the definition of the specific group object.

2. Make sure each Geo-Location object contains at least one country.

   If any of the network objects are empty during the migration, version 8.1.2 does not allow the definition of the specific network object.

Modify services

Prepare the services and service groups that are used by active rules.

If a service is not used by an active rule, it is not migrated.

Task

1. Make sure services within the same service group do not use conflicting ports.

   The migration to 8.1.2 fails if any rules have conflicting ports for services within the same service group.

2. If any rule uses a service based on the Other Protocol Packet Filter agent for IP Protocol 0, take one of these actions:
   - Delete the rule.
   - Select a different service.

Application sigset 3.46 and later support IP Protocol 0. After the newer application sigset has been updated, you can re-add the rule to the policy.

Modify rules

Modify rules for the migration.

Task

1. Disable the **Preserve source port** option for all rules that use services based on the FTP Packet Filter agent.

   The migration to 8.1.2 fails if **Preserve source port** is enabled for any FTP Packet Filter rules.

2. For the Passport rule, select **<Any>** from the **Allow users in the following groups** drop-down list.

   Authentication groups on Passport server (ssod) rules are not allowed in version 8.1.2.

3. For bidirectional packet filter rules, make sure the Redirect address is an IP address or a non-DNS host.

   Version 8.1.2 does not have an equivalent setting for the bidirectional attribute in the packet filter services.

4. Place the administrative access policy before intraburb rules.

   After the migration, the intraburb rule restricts administrator rights. If you fail to perform this step before upgrading, restore access manually at the physical console after the migration.

5. Modify all stateless bidirectional rules with NAT and multiple source endpoints to use a single IP address as the source endpoint.

   When no state information is recorded, connections from multiple hosts cannot share the same NAT address.

6. Make sure no rules use **Firewall (IP)** as the NAT address; select **localhost (Host)** instead.

   The Firewall network object is not a valid NAT address because it corresponds to the firewall loopback IP address (127.0.0.1).

If you encounter any issues during the migration, see the install_output file for specific reasons.

Migration process

The migration process consists of several high-level steps.

Task

1. Prepare your policy for the migration using the *Before you begin* instructions.
2. Retrieve the migration kit from the McAfee downloads site.
3. Load and install the 70103UP812 package.

   The 70103UP812 package preloads the software necessary to migrate the firewall configuration from version 7.0.1.03 to version 8.1.2. It also contains an update to the package installation software.

4. Load the 8.1.1 and 8.1.2 packages.
5. Install the 8.1.1 and 8.1.2 packages at the same time.
6. Relicense migrated firewalls.
7. Perform the post-migration tasks.

Download the migration kit

The migration kit is a .zip file that includes the 70103UP812, 8.1.1, 8.1.2, and Control Center 5.2.1P01 packages.

Use this task to retrieve the migration kit.

Task

1. In a web browser, navigate to www.mcafee.com/us/downloads.
2. Provide your grant number, then navigate to the appropriate product and version.
3. Download the Firewall Enterprise migration package.

Migrate using the Admin Console

For unmanaged firewalls, use the Firewall Enterprise Admin Console to migrate from version 7.0.1.03 to version 8.1.2.

Before you begin

- Review any known issues.
- McAfee recommends creating a disaster recovery backup. See the *McAfee Firewall Enterprise Product Guide* for instructions.

Tasks

- *Make the migration kit accessible* on page 8
  To perform the migration, you must place the contents of the migration kit where they can be accessed by the firewall.
- *Load the 70103UP812 package* on page 8
  The 70103UP812 package contains required updates for correctly loading and installing the 8.1.1 and 8.1.2 packages.
- *Install the 70103UP812 package* on page 9
  You must install the 70103UP812 package before loading the 8.1.1 and 8.1.2 packages.
- *Load the 8.1.1 and 8.1.2 packages* on page 9
  Both the 8.1.1 and 8.1.2 packages must be loaded before they can be installed using the Admin Console.
- *Install the 8.1.1 and 8.1.2 packages* on page 10
  Install both the 8.1.1 and 8.1.2 packages at the same time.
- *Install the Admin Console for 8.1.2* on page 10
  Run the setup program to install the 8.1.2 Admin Console.
- *Relicense the firewall* on page 10
  You must relicense the firewall after upgrading to version 8.1.2.

Make the migration kit accessible

To perform the migration, you must place the contents of the migration kit where they can be accessed by the firewall.

Task

1 Extract the migration kit .zip file.

2 Place the migration kit contents (70103UP812, 8.1.1, and 8.1.2 packages) where the firewall can access them. Choose one of these options:

- **Local FTP site** — Place the packages on an FTP site that the firewall has access to.
- **HTTPS website** — Place the packages on an HTTPS website that the firewall has access to.
- **CD** — Place the packages in a /packages directory on a CD, then insert the CD into the firewall CD-ROM drive.
- **Directory on the firewall** — Use SCP to copy the packages 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 70103UP812 package

The 70103UP812 package contains required updates for correctly loading and installing the 8.1.1 and 8.1.2 packages.

Task

1 In the Admin Console, select **Maintenance** | **Software Management**, then click the **Download Packages** tab.

For option descriptions, click **Help**.

2 Click **Perform Manual Load Now**.

3 Specify where the 70103UP812 package is stored.

a From the **Load packages from** drop-down list, select the appropriate method to load the package.

- If you placed the upgrade kit packages on a local FTP site, select **FTP**.
- If you placed the upgrade kit packages on an HTTPS website, select **HTTPS**.
- If you created a CD that contains the upgrade kit packages, select **CDROM**.
- If you copied the upgrade kit packages to your home directory on the firewall, select **File**.

b In the **Packages** field, type `70103UP812`.

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 70103UP812 is loaded on your firewall.

a Click the **Manage Packages** tab.

b Verify that the Status of the 70103UP812 package is **Loaded on <date>**.

Install the 70103UP812 package

You must install the 70103UP812 package before loading the 8.1.1 and 8.1.2 packages.

Task

1 On the **Manage Packages** tab, select the **70103UP812** package.

For option descriptions, click **Help**.

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 70103UP812 package is **Installed on <date>**.

Load the 8.1.1 and 8.1.2 packages

Both the 8.1.1 and 8.1.2 packages must be loaded before they can be installed using the Admin Console.

If you have not installed the 70103UP812 package before loading the 8.1.1 and 8.1.2 packages, the migration will fail.

Task

1 In the Admin Console, select **Maintenance** | **Software Management**, then click the **Download Packages** tab.

For option descriptions, click **Help**.

2 Load the 8.1.1 and 8.1.2 packages.

a Click **Perform Manual Load Now**.

b From the **Load packages** from drop-down list, select the appropriate method to load the package.

- If you placed the migration kit packages on a local FTP site, select **FTP**.
- If you placed the migration kit packages on an HTTPS website, select **HTTPS**.
- If you created a CD that contains the migration kit packages, select **CDROM**.
- If you copied the migration kit packages to your home directory on the firewall, select **File**.

c In the **Packages** field, type `8.1.1, 8.1.2`.

d Complete the remaining fields as appropriate, then 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**.

3 Verify that the 8.1.1 and 8.1.2 packages are loaded on your firewall.

a Click the **Manage Packages** tab.

b Verify that the status for the 8.1.1 and 8.1.2 packages is **Loaded on <date>**.

Install the 8.1.1 and 8.1.2 packages

Install both the 8.1.1 and 8.1.2 packages at the same time.

Task

1 In the Admin Console, select **Maintenance** | **Software Management**.

For option descriptions, click **Help**.

2 Click **Schedule**. The **Schedule Install/Uninstall** window appears.

3 In the **Select packages to install** area, select the **8.1.1** and **8.1.2** packages.

4 Select **Install/Uninstall now**, then click **OK**. A warning message appears.

5 Click **Yes**.

When the migration and installation is complete, the firewall restarts and the Admin Console connection is lost.

6 Close the Admin Console.

Install the Admin Console for 8.1.2

Run the setup program to install the 8.1.2 Admin Console.

Task

1 Double-click the .exe file from the migration kit to start the setup program.

The welcome window appears.

2 Follow the on-screen instructions to complete the setup program.

McAfee recommends using the default settings.

Relicense the firewall

You must relicense the firewall after upgrading to version 8.1.2.

Use one of these tasks to relicense a firewall.

Tasks

- *Relicense an Internet-connected firewall* on page 10
  Relicense a firewall that is connected to the Internet.
- *Relicense an isolated firewall* on page 11
  Relicense a firewall on an isolated network.

Relicense an Internet-connected firewall

Relicense a firewall that is connected to the Internet.

Task

1 In the Admin Console, select **Maintenance** | **License**, then click the **Firewall** tab.

2 Verify the fields are populated correctly, then click **Activate firewall**. A notice message appears.

3 Click **Yes**. The information on the **Firewall** tab is updated.

Relicense an isolated firewall

Relicense a firewall on an isolated network.

Task

1 Locate the McAfee Firewall Enterprise serial number on the **Dashboard** (top tree node). The serial number is a 16-character alphanumeric code.

2 Look up the system ID to use when relicensing your system:

   a Select **Maintenance** | **License**, then click the **Firewall** tab.

   b Record the number in the **System ID** field.

3 Complete the activation webpage:

   a From any workstation with Internet access, open a web browser and navigate to: go.mcafee.com/cgi-bin/sidewinder-activation.cgi

   b Complete the form on the website, making sure to correctly type or select:

   - Serial number
   - System ID
   - Version 8.1.0 or later
   - End-user information

   c Click **Submit**. A confirmation screen appears.

   d Verify that the information is correct.

   - If incorrect, use the **Back** button to return to the form and correct the information.
   - If correct, click **Submit**. The system processes the information, and a new webpage appears displaying the activation key.

4 Using the on-screen instructions, save the activation key.

You can continue following the on-screen instructions for importing the file from the command line or use the Admin Console instructions given here.

5 [Conditional] If you are using a computer that does not have the Admin Console installed, transfer the saved activation key to the Admin Console computer.

6 In the Admin Console, select **Maintenance** | **License**, then click the **Firewall** tab.

7 Click **Import Key** to import the key into the firewall. Complete these fields:

- **Source** — Select **Local File**.
- **File** — Type the name of the file that contains the activation key. Click the **Browse** button if needed.

8 Click **OK** to approve the specified file. The activation key is extracted from the file and written to the **Activation Key** field.

The license key is activated immediately. Your firewall software and any additional features you purchased are now licensed.

Migrate using a Control Center Management Server

Upgrade a managed firewall from version 7.0.1.03 to version 8.1.2 using the Control Center Management Server.

Before you begin

- McAfee strongly recommends that the Control Center Management Server be at version 5.2.1P01 or later to manage version 8.1.2 firewalls.
- Review any known issues.
- McAfee recommends creating a configuration backup for the firewalls you will be migrating. See the *McAfee Firewall Enterprise Control Center Product Guide* for instructions.

Tasks

- *Make the migration kit accessible* on page 12
  Place the contents of the upgrade kit where they can be accessed by the Control Center Management Server.
- *Load the 70103UP812 package* on page 12
  Use the Control Center Client application to load the 70103UP812 package on your Control Center Management Server.
- *Install the 70103UP812 package* on page 13
  Use the Control Center Client application to install the 70103UP812 package on a managed firewall.
- *Load the 8.1.1 and 8.1.2 packages* on page 13
  Use the Control Center Client application to load the 8.1.1 and 8.1.2 packages.
- *Install the 8.1.1 and 8.1.2 packages* on page 14
  Use the Control Center Client application to install the 8.1.1 and 8.1.2 packages.
- *Retrieve policy from the firewall* on page 14
  Use the Control Center Client application to retrieve policy from the upgraded firewall.
- *Relicense the firewall* on page 15
  You must relicense the firewall after upgrading to version 8.1.2. Use the Control Center Client application to relicense managed firewalls.

Make the migration kit accessible

Place the contents of the upgrade kit where they can be accessed by the Control Center Management Server.

Task

1. Extract the migration kit .zip file.
2. Place the migration kit contents (70103UP812, 8.1.1, and 8.1.2 packages) where the Control Center Management Server can access them. Choose one of these options:
   - **Local FTP site** — Place the packages on an FTP site.
   - **HTTP website** — Place the packages on an HTTP website.

Load the 70103UP812 package

Use the Control Center Client application to load the 70103UP812 package on your Control Center Management Server.

The 70103UP812 package contains updates that are required to correctly load and install the 8.1.1 and 8.1.2 packages.

Task

1 In the navigation bar, click **Maintenance**, then click the **Store Updates** tab.

For option descriptions, press F1.

2 Click **Manual Download**.

3 From the **Protocol** drop-down list, select the appropriate method to load the package:

- If you placed the upgrade kit packages on a local FTP site, select **FTP**.
- If you placed the upgrade kit packages on an HTTP website, select **HTTP**.

4 In the **File** field, type `70103UP812`.

5 Complete the remaining fields as appropriate, then click **OK**. The Control Center Management Server downloads the package. When the download is complete, a message appears.

6 Click **OK**.

Install the 70103UP812 package

Use the Control Center Client application to install the 70103UP812 package on a managed firewall.

Task

1 In the navigation bar, click **Maintenance**, then click the **Firewall Updates** tab.

For option descriptions, press F1.

2 Select the firewall to upgrade, then click **Manage Firewall**. The **Manage Firewall** window for the selected firewalls appears.

3 Select the **70103UP812** package, then click **Save**. The **Manage Firewall** window closes.

Select only the 70103UP812 package.

4 On the **Firewall Updates** tab, click **Update Firewalls**. A "perform chosen action" message appears.

5 Click **OK**. The Control Center downloads and installs the 70103UP812 package on the selected firewall.

Load the 8.1.1 and 8.1.2 packages

Use the Control Center Client application to load the 8.1.1 and 8.1.2 packages.

Task

1 In the navigation bar, click **Maintenance**, then click the **Store Updates** tab.

2 Load the 8.1.1 package.

a Click **Manual Download**.

For option descriptions, press **F1**.

b From the **Protocol** drop-down list, select the appropriate method to load the package

- If you placed the upgrade kit packages on a local FTP site, select **FTP**.
- If you placed the upgrade kit packages on an HTTP website, select **HTTP**.

c In the **File** field, type the file name of the package. *Example:* 8.1.1.

d Complete the remaining fields as appropriate, then click **OK**. The Control Center Management Server downloads the package. When the download is complete, a message appears.

e Click **OK**.

3 Repeat steps 1 and 2 for the 8.1.2 package.

4 Verify that the status for each package is **Available on Mgmt. Server**.

Install the 8.1.1 and 8.1.2 packages

Use the Control Center Client application to install the 8.1.1 and 8.1.2 packages.

Task

1 In the navigation bar, click **Maintenance**, then click the **Firewall Updates** tab.

For option descriptions, press **F1**.

2 Select the firewall to upgrade, then click **Manage Firewall**. The **Manage Firewall** window for the selected firewalls appears.

Only firewalls that have the 70103UP812 package installed can be upgraded to version 8.1.2. If you are migrating a cluster and want to individually migrate the firewalls, deselect the **Apply packages on all synced members** checkbox.

3 Select the **8.1.1** and **8.1.2** packages.

4 Click **Save**. A confirmation message appears.

5 Click **OK**.

6 On the **Firewall Updates** page, click **Update Firewalls**. A confirmation message appears.

7 Click **OK**. The Control Center Management Server loads and installs the packages on the selected firewalls.

When the installations are complete, the upgraded firewalls restart.

Retrieve policy from the firewall

Use the Control Center Client application to retrieve policy from the upgraded firewall.

Task

1 In the navigation bar, click **Policy**.

2 In the Policy tree, expand the **Firewalls** node.

3 Right-click the firewall, then select **Retrieve Firewall Objects**. The **Firewall Retrieval Options** window appears.

4 Select all items, then click **OK**. A confirmation message appears.

5 Click **Yes**. The Control Center Management Server retrieves objects from the firewall.

After retrieving the upgraded firewall policy, manually delete the 7.x rules.

Relicense the firewall

You must relicense the firewall after upgrading to version 8.1.2. Use the Control Center Client application to relicense managed firewalls.

Task

1. In the navigation bar, click **Maintenance**.
2. In the Firewall Maintenance tree, double-click **Firewall License**.
3. From the **Firewall** drop-down list, select the firewall you upgraded.
4. Verify the firewall information, then click **Activate firewall**. A warning message appears.
5. Click **OK** to close the warning message.
6. Click **OK** to close the **Firewall License** window.

Post-migration tasks

Perform these tasks to avoid post-migration errors.

Task

1. If you are using the remotely managed SmartFilter, re-enter the SmartFilter Admin password. In the Admin Console, select **Policy** | **Application Defenses** | **SmartFilter**.
2. After the system restarts to 8.1.2, initialize the AV runtime and pre-filter caches to avoid AV scanner errors.

   ```
   cf antivirus verify
   ```

3. If the audit logs show that the UDP port 514 traffic from the firewall's localhost address is being denied, send a SIGHUP signal to the auditd process.

   ```
   kill -s HUP <PID of auditd process>
   ```

   Example

   ```
   % kill –s HUP `cat /var/run/audit/auditd.pid`
   ```

4. Recover the settings for 7.0.1.03 sendmail mail forwarding setup.
   a. Copy /etc/mail/aliases.bak to /etc/mail/aliases.
   b. Type this command:

      ```
      newaliases
      ```

   c. Type this command:

      ```
      cf daemond restart agent=sendmail_daemon
      ```

5. Use the install_output file instructions to retrieve any missing CRL files from /var/saved_crls/ directory.
6. Verify that HTTP traffic is passing as expected.

   In order to preserve the policy enforcement behavior from 7.0.1.03, the migration process might insert TCP deny rules after HTTP allow rules.

7 Clean up policy items.

These areas might need additional attention.

- Access control rules
- Application Defenses
- Network objects
- SSL rules

Post-migration best practices

McAfee recommends viewing several resources and reviewing updates to the Admin Console navigation in version 8.x.

There are several video tutorials regarding migration and version 8.x on the KnowledgeBase; see KB71733. (You will need to log on to view them.)

Familiarize yourself with the Admin Console locations of these items in version 8.x:

Monitor

- SNMP Agent properties — **Monitor** | **SNMP Agent**

Policy

- Passport Agent settings — **Policy** | **Rule Elements**
- Max connections — **Policy** | **Application Defenses** | **Defenses** | **Generic (Required)** | **Set Expected Connections**
- Service Timeouts, IP filter connection settings, IP filter audit settings — **Policy** | **Application Defenses** | **Defenses** | **Generic (Required)**

  For complete information about the Generic (Required) Application Defense, see the *McAfee Firewall Enterprise Product Guide*.

- Transparency settings — **Policy** | **Application Defenses** | **Defenses** | **Generic (Required)** | **Connection settings**
- URL Translation — **Policy** | **Application Defenses** | **Defenses** | **HTTP** | **URL Translation Rules**
- Sendmail Properties — **Policy** | **Application Defenses** | **Defenses** | **Mail (Sendmail)** | **Sendmail Properties**
- SSH Proxy Agent Properties (Known Hosts) — **Policy** | **Application Defenses** | **Defenses** | **SSH** | **SSH Known Hosts**

Network

- ISAKMP agent settings — **Network** | **VPN Configuration** | **ISAKMP Server** | **Properties**
- DHCP Relay Agent settings — **Network** | **DHCP Relay**
- BGP Routing Agent settings — **Network** | **Routing** | **Dynamic Routing**
- OSPF and OSPF IPv6 Agent settings — **Network** | **Routing** | **Dynamic Routing**
- XORP Agent settings — **Network** | **Routing** | **Dynamic Routing** | **PIMSM**
- RIP and RIP Unbound Agent settings — **Network** | **Routing** | **Dynamic Routing**

Maintenance

- Admin Console settings — **Maintenance** | **Remote Access Management**
- SSH Server properties — **Maintenance** | **Remote Access Management**

Configuration of the fastpath proxy setting is now a global setting available through the command line.

```
>cf acl set fastpath=off
```

Troubleshooting and log inspection

If there are problems during the migration, inspect the log files to identify the source of the problem.

- If the installation of the 8.1.2 package fails during the migration processing on the inactive disk slice, inspect the install_output file for that slice.
- If the upgrade to the 8.1.2 release package fails during the restart, a rollback is automatically initiated. View the audit logs and the /var/log/swedeautotranslate file to identify the cause of the failure.
- If there is SSOD startup failure after rolling back to 7.0.1.03, create a Passport rule.
- If the migration succeeds, view the package installation log for details. Check for any post-migration warnings.

Review the known issues for advice on reports logged during the upgrade.

View the install_output file for the migration

Use this task to view the install_output file.

Task

1. From the 7.0.1.03 command line, log on as the Admin user.
2. Use the mount command to find what disk the root (/) file system is mounted on.
   - If the disk device ends in s2a, the inactive slice is 3.
   - If the disk device ends with s3a, the inactive slice is 2.

   In this example, the /dev/ad0s2a disk is mounted on the root file system, so the inactive slice is 3; therefore, the install_output file is /var/packages/status3/install_output.

   Example

   ```
   firewall1:Admn {6} % mount | grep ' / '
   ```

   /dev/ad0s2a on / (ufs, local, multilabel)

   ```
   firewall1:Admn {7} % less /var/packages/status3/install_output
   ```

   

   The argument to the grep command contains spaces before and after the slash (/).

1. In the Admin Console, select **Maintenance** | **File Editor**. A warning message appears.
2. Click **Start File Editor**. The **File Editor** appears.
3. Select **File** | **Open** . The **Open File** window appears.
4. Select the **Firewall File** option, then browse to or type the location of the install_output file.

   Example: `/var/packages/status2/install_output`

5 Click **OK**. The file opens.

Do not edit the install_output file.

6 Search for **8.1.1** and **8.1.2** to locate information about the migration.

Example: `var/packages/status3/install_output`

View the package installation log

View the package installation log from the Admin Console.

Task

1 From the Admin Console, select **Maintenance** | **Software Management**. The **Manage Packages** tab appears.

2 Click **View Log**.

View audit logs after rollback

The 7.0.1.03 /usr/bin/acat program is not able to read 8.1.2 audit records; all subsequent 7.0.1.03 auditing to the current audit.raw file is masked by 8.1.2 audit records.

The 70103UP812 package provides a release 8.1.2-compatible acat utility, acat8, that should be used to examine audit files that contain records generated during the attempt to start the migrated 8.1.2 installation. This utility is used in exactly the same way as the standard acat.

Example

```
firewall1:Admn {6} % /usr/bin/acat8 > out.txt
```

Tasks

- *Roll the audit* on page 18
  Roll the audit.raw log file to log all subsequent 7.0.1.03 audit records to a new audit file. Use the Admin Console and the standard acat utility to view this log file.
- *Manual rollback* on page 18
  The instructions for viewing audit logs also apply to cases where you manually roll back from version 8.1.2 to version 7.0.1.03.

Roll the audit

Roll the audit.raw log file to log all subsequent 7.0.1.03 audit records to a new audit file. Use the Admin Console and the standard acat utility to view this log file.

Rolling the audit.raw log file can be initiated from:

- **Admin Console** — Select **Monitor** | **Audit Management**, then click **Roll Now**.
- **Command line** — Use the rollaudit(8) utility.

Manual rollback

The instructions for viewing audit logs also apply to cases where you manually roll back from version 8.1.2 to version 7.0.1.03.

Manual rollbacks can be initiated from:

- **Admin Console** — Select **Maintenance** | **Software Management** | **Rollback**
- **Command line** — Use the cf package rollback command.

If the migration fails and rolls back to version 7.0.1.03, there might also be valuable information in the /var/log/swedeautotranslate.log and /var/log/daemond.log files. McAfee recommends preserving these files to provide support information when debugging the problem.

Copyright © 2012 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

McAfee
An Intel Company