opentext™

ESM Appliance E8400 Model

Software Version: 24.3

Administrator's Guide to Hardware Appliances for ArcSight ESM

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://www.microfocus.com/en-us/contact-support/stackb
Support Web Site	https://www.microfocus.com/en-us/support
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/#gsc.tab=0

Contents

About this Guide

This installation guide provides instructions on how to install and initialize the standalone ESM E8400 appliance.

For more information, see "How the ESM Appliance Works" on page 6.

Intended Audience

This book provides information for admins who need to install, initialize, and restore ESM appliances.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact OpenText Customer Care.

Chapter 1: Overview

ESM is a Security Information and Event Management (SIEM) solution that collects and analyzes security data from different devices on your network and provides you a central, real-time view of the security status of all devices of interest to you. ESM uses the Correlation Optimized Retention and Retrieval Engine (CORR-Engine) storage, a proprietary framework that processes events, and performs searches. E8400 is the hardware appliance custom built for ESM.

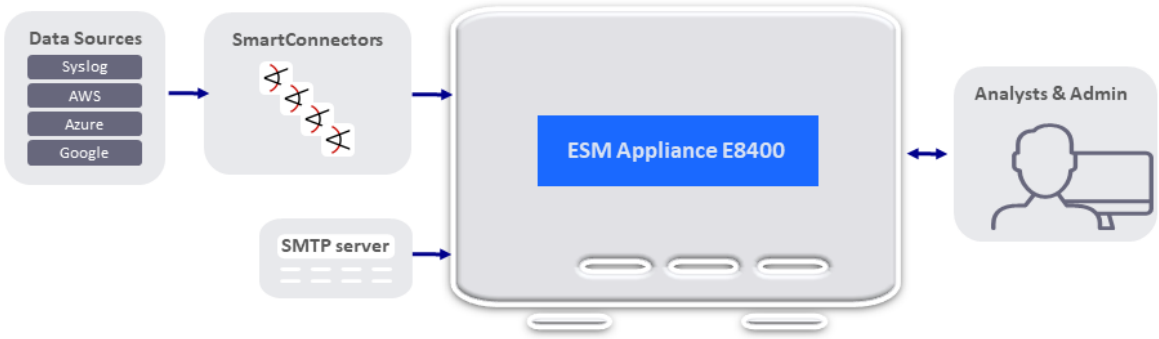
ESM collects, normalizes, aggregates, and filters millions of events from thousands of assets across your network into a manageable stream that is prioritized according to risk, vulnerabilities, and the criticality of the assets involved. These prioritized events can then be correlated, investigated, analyzed, and remediated using ESM tools, giving you situational awareness and real-time incident response time.

- Correlation—Many interesting activities are often represented by more than one event. Correlation is a process that discovers the relationships between events, infers the significance of those relationships, prioritizes them, then provides a framework for taking actions.
- Monitoring—Once events have been processed and correlated to pinpoint the most critical or potentially dangerous of them, ESM provides a variety of flexible monitoring tools that enable you to investigate and remediate potential threats before they can damage your network.
- Workflow—The workflow framework provides a customizable structure of escalation levels to ensure that events of interest are escalated to the right people in the right timeframe. This enables members of your team to do immediate investigations, make informed decisions, and take appropriate and timely action.
- Analysis—When events occur that require investigation, ESM provides an array of investigative tools that enable members of your team to drill down into an event to discover its details and connections, and to perform functions, such as NSlookup, Ping, PortInfo, Traceroute, WebSearch, and Whois.
- Reporting—Briefing others on the status of your network security is vital to all who have a stake in the health of your network, including IT and security managers, executive management, and regulatory auditors. ESM's reporting and trending tools can be used to create versatile, multi-element reports that can focus on narrow topics or report general system status, either manually or automatically, on a regular schedule.

The purpose of this guide is to help you perform the initial configuration of your ESM appliance, so that you can start taking advantage of all its features. For more information on the usage and settings of specific features, please refer to the ArcSight Command Center User's Guide for ArcSight ESM 24.3 and the ArcSight Console User's Guide for ArcSight ESM 24.3.

How the ESM Appliance Works

Each appliance consists of a **single-node** version of ESM, also known as Compact Mode. You do not need to modify any settings.



Chapter 2: Setting Up an ESM Appliance

This section describes how to rack mount your ESM E8400. These basic steps enable you to start using your ESM appliances.

	Task	See
❑	1. Power on the Appliance	Powering On the ESM Appliance
❑	2. Set up Remote Access	Setting Up the Appliance for Remote Access
❑	3. (Optional) Encryption of SEDs	"Encryption of SEDs" on page 9
❑	4. Appliance Initialization Procedures	"Initializing the ESM Appliance " on page 9
❑	5. Appliance Licenses	"Appliance Licenses" on page 17

Powering On the ESM Appliance

Before you Begin:

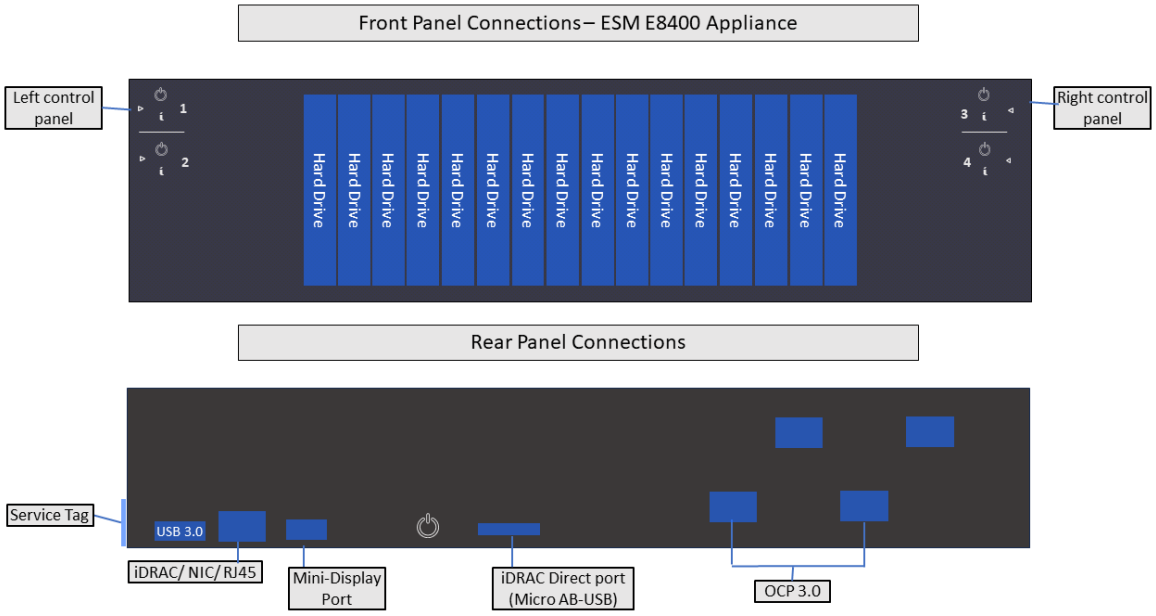
Redeem your license key by following the instructions in the documents you received when purchasing. Redeeming this key gets you the license that you need to access the ESM functionality.

To install the appliance:

1. Unpack the appliance and its accompanying accessories.

   Note: Read carefully through the instructions, cautions, and warnings that are included with the appliance shipment. Failing to do so can result in bodily injury or appliance malfunction.

2. Follow the rack installation instructions to securely mount it.
3. Make the front and rear panel connections. The diagram below offers a general view of the basic connections:



4. To enable local access to the Appliance, connect a keyboard, monitor, and mouse to the Appliance ports.
5. Power on the appliance.

Setting Up the Appliance for Remote Access

All appliances are equipped with an `iDRAC Service Module (iSM)` for remote access. OpenText strongly recommends setting up and configuring your appliance for out-of-band remote access. Doing so ensures that you or Customer Support (with your permission and assistance) can remotely access the console of your appliance for troubleshooting, maintenance, and control over the powering on and off of the box.

Changing the `iDRAC` password on your Appliance

Appliance boxes come with a random `iDRAC` password. For information on how to locate the password, see Secure Default Password.

This is a unique password, which will be required the first time `iDRAC` is accessed. The appliance then will prompt for a new password to be chosen. For security reasons, OpenText recommends to change this password as soon as possible.

To set up your appliance for remote access, follow the instructions in the EMC iDRAC Service Module.

Firewall

The firewall for the ESM appliance comes pre-configured, with the following TCP ports open by default to facilitate the initial setup:

Port	Description
22	Used by the appliance installer
7443	Used by the appliance installer
8443	SmartConnectors and consoles
9000	Peering

Note: If you do not plan to use peering in your environment, disable port 9000.

Encryption of SEDs

The ESM Appliances support FIPS enabled self-encrypting disks (SEDs).

A SED is a data storage device with built-in cryptographic processing to encrypt and decrypt the data it contains. This process occurs within the device itself, independent of any connected information system, and it provides data protection against the loss or theft of the disks, as well as certain levels of hacking attempts.

This protection consists of setting up passphrase-access-only.

The SEDs ship without the passphrase, allowing you to chose your own. To set up a passphrase, first follow the steps to establish a security key.

The chosen passphrase can then be applied to pre-existing virtual disks by following the steps in Secure a pre-existing virtual disk.

To change or disable a security key, please follow the specific procedures listed under this section.

Initializing the ESM Appliance

The initialization of a ESM appliance consists of two parts: the first boot (bootstrapping) of the process through the console, and the installation of the software through the appliance UI.

First Boot Initialization of the ESM Appliance (Bootstrapping)

Tip: Be aware that this process will require network information for the appliance, such as:

- Static IP address
- Resolvable FQDN hostname
- NTP server that's both accessible and running

All of this information must be available to successfully complete the bootstrapping.

1. Log into your appliance using iDRAC (see Setting Up the Appliance for Remote Access for instructions), and launch the Virtual Console.
2. Turn on the appliance using the Power Controls option, in case the appliance is off.
3. Using the local drive (NVMe), select from the menu the version of Red Hat you want to boot from.
4. From the console, login using your default username (otadmin) and password (change_me).
5. Once the default credentials are entered, you will be asked to change the password for otadmin:

```
You are required to change your password immediately (administrator
enforced).
Current password:
New password:
Retype new password:
```

Note: The STIG-compliant password policy rules for both the arcsight and the root password require:

- A minimum of 15 characters
- A minimum of 1 number
- A minimum of 1 lowercase character
- A minimum of 1 uppercase character
- A minimum of 1 special character
- A maximum of 2 consecutive repeating characters
- A maximum of 4 consecutive repeating characters of the same class
- A minimum of 8 different characters
- To not be a word from the dictionary
- To be different from the last seven passwords

6. The **OpenText Appliance** splash screen will appear, with the **User must set 'root' password to proceed** message. You will be required to enter the `otadmin` user password you just reset to make the change to the `root` password:

```
password for otadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

> Once your passwords have been set, you will need to wait for at least one day to update to a different one. And the maximum expiration period for a password is 60 days.

7. Set the `arcsight` user password.

```
password for arcsight
Changing password for user arcsight.
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

8. Complete the **Network Configuration**. The screen will display a list of network interfaces and their status:

```
********************************************************************************
Network Configuration
********************************************************************************
WARNING: You must specify static IP address and resolvable hostname
(FQDN).
********************************************************************************
List of network interfaces
********************************************************************************
enoxxxxnp0      UP             xx:xx:xx:xx:xx:xx       <BROADCAST, MULTICAST, UP, LOWER
enoxxxx         DOWN            xx:xx:xx:xx:xx:xx       <NO-CARRIER, BROADCAST, , MULTI
ensxxxx         DOWN            xx:xx:xx:xx:xx:xx       <NO-CARRIER, BROADCAST, MULTICA
ensxxxx         DOWN            xx:xx:xx:xx:xx:xx       <NO-CARRIER, BROADCAST, MULTICA

********************************************************************************
Select one active connection to configure:
********************************************************************************
1) enoxxxxnp0
#? 1
```

   Select the number of the active connection you want to configure.

9. Configure the network using an IPv4 address by providing this information:

```
**********************************************************************
Configure the network connection enoxxxxnp0 for device enoxxxxnp0:
**********************************************************************
Hostname: your_appliance_host_fqdn

What type of Networking do you want to setup? 1. IPv4

IP Address:
Netmask [1-31]:
Default Gateway:
Primary DNS server:
Secondary DNS server (optional):
DNS Search Domains: your_appliance_domain
```

10. (Optional) Enter the date and time information.
11. Configure the NTP server.

```
(one entry per line, press enter when done)
NPT Servers:
```

Once all this information has been provided, the console will display a summary of the network configuration and NTP server configuration, and will ask you to verify by entering y:

```
Do you want to apply this configuration? (y/n)
```

If you need to correct the information, enter n, and the process will ask you for each item again. If you enter y, the process will continue:

```
Generate self-signed certificate and first time login token...
```

12. If the configuration ends successfully, you will see the following message:

```
**********************************************************************
The appliance network and NTP server have been setup successfully
**********************************************************************
Go to https://<your_appliance_host_fqdn>:7443 to install ESM product
IMPORTANT: You will need the token to login for the first time:
xxxxxxxx
**********************************************************************
```

The console will not allow you to copy the token, which you will need for your first login to the **ESM Installer Web App**. Access the URL provided above in your browser, and type the token manually as shown in the console.

Regeneration of the First Login Token

If you need to obtain a First Login Token again (other than with the preceding procedure), you can regenerate it by running the following command as the `otadmin` user in the console:

```
/var/opt/appliance/appliance_scripts/generate_first_login_token.sh
```

The command output should appear as follows:

```
================================================================
Go to https://<your_appliance_host_fqdn>:7443 to install ESM product
IMPORTANT: You will need the token to login for the first time:
xxxxxxxx
================================================================
```

Configuring ESM

The first time you connect to the appliance, you will need to accept the end user license agreements, and provide basic setup information.

Follow these steps to configure your ESM appliance the first time:

> All through this process, you might see confirmation pop-ups, letting you know that the operation has concluded or started successfully.

1. Open a browser to access the following URL:

   ```
   https://<your_appliance_hostname>:7443
   ```

   > When you first access the URL, you might receive a message stating, "Your connection is not private." To proceed, please click **Advanced**, and then select **Continue to your_appliance_hostname**.

2. At the **Welcome** screen, set up your **Username** and **Password**, and provide your **Token** (which you obtained at the end of the "First Boot Initialization of the ESM Appliance (Bootstrapping)" on page 10 procedure), to begin the process.

   Click the Create User button to proceed.

3. On the next screen, provide your newly created **Username** and **Password**, and then click Log in.

4. The ESM Appliance Set up Wizard will guide you through the installation process. The first screen will display the **OpenText End User License Agreement**. You must scroll down to the end of the agreement and select I have read and agree with the end user license agreements for the Next button to allow you to proceed.

Every screen in this process will also have a Log out button on the right upper corner. Logging out will bring up the initial Login screen, but if you had already initiated a process (install or uninstall), the process will proceed behind the scenes even if you log out.

5. The second screen will display the **Red Hat End User License Agreement** for your perusal. You must scroll down to the end of the agreement, and select I have read and agree with the end user license agreements for the Next button to allow you to proceed.
6. Next, the Application Setup screen will prompt you for the following information:
   - Language to use in your environment.
   - Username for the ESM administrator.

     The ESM administrator username policy rules have the following requirements:
     - At least five characters.
     - No more than 15 characters.
     - Must not contain spaces.
     - Must not contain these characters: / ~ ` * % \ & |
   - Password for the ESM administrator. Confirm the password by re-entering it.

     The ESM administrator password policy rules have the following requirements:
     - At least six characters.
     - No more than 32 characters.
     - At least one number.
     - At least one lowercase character.
     - At least one uppercase character.
     - At least one special character including any of: _ ? ! % @ &
     - Must not contain white space.
   - Sender address, which is the email address to use to send email notifications.

     The following scenarios result in email notifications:
     - The subsystem status changes. The email includes information about the the change and who made it.
     - The report is successfully archived.
     - The account password is reset.
     - The archive report generation fails.
     - A destination receives too many notifications.
     - The event archive location reaches the cap space. The notification requests that you free up space by moving the event archives to another location.

- The user elects to email the ArcSight Console settings.
- The user sends a partition archival command.
- An archive fails because there is not enough space.
- The connection to the database fails.

- Recipient address, which is the email account that receives email notifications if the Manager becomes unavailable or encounters some other problem.
- Password for the CORR-Engine database. Confirm the password by re-entering it.

  The CORR-Engine database password policy rules have the following requirements:

  - At least six characters.
  - No more than 70 characters.
  - Must not contain the following characters: $ ' # ? " \
  - Must not contain white space.
- Storage Settings, which includes the following:
  - System storage size: number of gigabytes to set aside for storing resources.
  - Event storage size: number of gigabytes to set aside for storing events.
  - Online event archive size: maximum number of gigabytes of disk space for event archives.
  - Retention period: number of days to retain events before they are purged from the system.

  The sum of System Storage Size, Event Storage Size, and Online Event Archive Size, cannot exceed 18,883 GB.
- Packages are the additional optional packages you are licensed to use.

Click Next.

The next screen will present the information you just provided, for review. Click Submit if everything looks correct, or Previous for corrections.

7. The setup process will proceed without any more user intervention, and it will take around 20 minutes to complete. You can select for the setup to proceed with or without on-screen logs.

   If the installation fails, you will need to reboot the machine to restart the process. Follow these instructions in case of an installation failure.
8. Once the process is completed successfully, you will arrive at a screen with the following message: **You have successfully set up your appliance. Use the URL below to log into the ArcSight Command Center**.

Click Copy URL and paste the URL into your browser to start using your appliance.

9. The URL you obtained from the process will bring you to the Arcsight Command Center login screen, where you must provide the ESM administrator username and password specified previously in Step 6.

   Click the Login button to proceed.

ESM Configuration Failure

A configuration failure is highly unlikely, but if it should happen, follow this procedure to attempt it again.

1. If the configuration fails, you will land on a screen that shows the next message:

   ```
   The appliance setup was unsuccessful.  The logs below contain information
   about this failure.
   Please click the Uninstall button to revert the installation.
   ```

   Click the Uninstall button to proceed to the Uninstalling screen.

2. The uninstalling process can have two outcomes:

   - Success, which will take you to a screen with the following message:

     ```
     The uninstalling process has concluded successfully. Click the Reboot
     Appliance button to attempt the installation again (rebooting will take
     around 3 minutes)
     ```

     Clicking the Reboot Appliance button will take you to the Reboot in process… please hold! screen. Wait for around 5 minutes, and refresh your browser.

     Once the reboot is done, you will return to the Review Information screen, which has preserved all the configuration information you have provided.

     If the failure was caused by the information you provided, click Previous and make the necessary changes. Then click Next, review the updated information, and click Submit to try again. If the information was not the cause, simply review it and click Submit.

   - Failure, which will take you to a screen with the following message:

     ```
     The appliance setup was unsuccessful.  The logs below contain
     information about this failure.
     Please click the Retry Uninstall button to revert the installation.
     ```

     Clicking the Retry Uninstall button will repeat the procedure described in this page. The repeated process can have the same outcomes, success or failure.

     ```
     If the installation process continues to fail after multiple attempts,
     please contact OpenText tech support for assistance:
     https://www.microfocus.com/en-us/support/contact-support/
     ```

Appliance Licenses

While your appliance ships with its software already installed, you will require the ESM software license key (purchased separately).

Once the license has been installed, it will behave as a normal permanent license for ESM.

Obtaining Your License

Redeem your license on the Software Entitlements Portal, then download the license file to a computer from which you can connect to your appliance.

For more information, refer to the software delivery confirmation email you received from OpenText.

Chapter 3: Restore Procedures

OpenText recommends to perform backups of the information and configuration of an ESM appliance to ensure you can recover your data in case of loss.

Components should be backed up on a regular schedule, as well as before you upgrade your environment.

Restoring an Appliance to Factory Settings

You can restore appliances to their original factory settings by using the procedures detailed here. To perform a restore procedure, you will require:

- An `.iso` image file containing the factory settings for the version of ESM you are restoring. Find the name of the file in the **Downloading Your Factory Restore Image Files** section of the E8400 Appliance Release Notes.

  Once you have acquired the image file, please refer to the signature verification instructions, and perform the verification steps before starting the procedure below.

The restore procedure can be conducted in two ways:

- If you have physical access to the appliance, use the "Restoring an Appliance Using a USB Memory Stick" below method
- If you have only `iDRAC` access to the appliance, use the "Restoring an Appliance Using iDRAC Access" on page 20 method

Restoring an Appliance Using a USB Memory Stick

This method will require the following external hardware:

- A 32 GB or higher USB memory stick (the faster type available, but at least USB 2.0 or 3.x)
- A Linux machine to perform the burning of the .iso image into the USB memory stick

Image Burning

1. Connect the USB memory stick to one of the ports of the Linux machine.
2. From the command line, execute the following command to burn the `.iso` image into the USB memory stick:

```
dd if=<iso_image_file_name>.iso status=progress oflag=sync of=/dev/sdX
bs=1M
```

Where

- `<iso_image_file_name>` is the name of the image file downloaded here.
- /dev/sdX is the device name of your USB drive (e.g.,/dev/sdb).

And wait until the progress has reached 100%.

3. Turn your appliance off and connect the bootable USB stick you just created to one of its ports. Reboot the appliance.

Restore Procedure:

1. Access the remote console of the appliance through `iDRAC`.

   If you already used the remote access, use the password you setup the first time you connected. Otherwise, for instructions see:

   "Setting Up the Appliance for Remote Access" on page 8
2. From the `iDRAC` **Dashboard**, select the **Virtual Console** on the right lower corner.
3. Click the **BOOT** button on the upper right hand corner and select the **BIOS Boot Manager** option.

   A pop-up window will request to **Confirm Boot Action**, setting a new device to boot from. Select **Yes**.
4. The previous step will not initiate the reboot automatically. For that, you will need to click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.

   A pop-up window will request to **Confirm Power Action**. Select **Yes**.
5. The booting process will prompt a selection from the **Boot Manager**. Choose **One-shot UEFI Boot Menu**.
6. From the **Select UEFI Boot Option**, select your USB stick (its name will depend on brand and model, but it will start with **Disk connected to back USB**).
7. The appliance will boot from the selected USB stick.

   The restore process will start automatically if you allow it some time, or you can click on the **ArcSight** option at the top to start right away.
8. Different screens will follow each other, some of them with progress bars, indicating the restoring progress of a specific system portion. None of these require user intervention, and the whole process takes approximately 20 minutes. Once the restore process has reached this point:

   ```
   The next step: true
   Now run: true
   ```

   Your input will be required to reboot the appliance:

```
reboot
```

9. Once the reboot process is finished, follow the instructions listed in:

   "Initializing the ESM Appliance " on page 9

Restoring an Appliance Using iDRAC Access

When using the iDRAC Remote File Share feature to perform the restore procedure, make sure there is no USB drive connected to the appliance ports, since its presence may interfere with the restore process.

This method will require the following preparation:

- Store your `.iso` image in a location that is accessible to the iDRAC network. For more information, see the iDRAC documentation.
- Configure the iDRAC Remote File Share option in the Virtual Media tab using shared the `.iso` image downloaded here.

Restore Procedure:

1. Access the remote console of the appliance through iDRAC.

   If you already used the remote access, use the password you setup the first time you connected. Otherwise, for instructions see:

   "Setting Up the Appliance for Remote Access" on page 8
2. From the iDRAC **Dashboard**, select the **Virtual Console** on the right lower corner.
3. Click the **BOOT** button on the upper right hand corner and select the **BIOS Boot Manager** option.

   A pop-up window will request to **Confirm Boot Action**, setting a new device to boot from. Select **Yes**.
4. The previous step will not initiate the reboot automatically. For that, you will need to click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.

   A pop-up window will request to **Confirm Power Action**. Select **Yes**.
5. The booting process will prompt a selection from the **Boot Manager**. Choose **One-shot UEFI Boot Menu**.
6. From the **Select UEFI Boot Option**, select **Virtual Network File**.
7. The appliance will boot from the .iso image in the Remote File Share.

   The restore process will start automatically if you allow it some time, or you can click on the **ArcSight** option at the top to start right away.

8. Different screens will follow each other, some of them with progress bars, indicating the restoring progress of a specific system portion. None of these require user intervention, and the whole process takes approximately 20 minutes. Once the restore process has reached this point:

   ```
   The next step: true
   Now run: true
   ```

   Your input will be required to reboot the appliance:

   ```
   reboot
   ```

9. Once the reboot process is finished, follow the instructions listed in:

   "Initializing the ESM Appliance " on page 9

Publication Status

Released: Monday, September 30, 2024

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Administrator's Guide to Hardware Appliances for ArcSight ESM (8000 Appliance 24.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to documentation-feedback@microfocus.com.

We appreciate your feedback!