opentext™

CHA Appliance Model C8200

Software Version: 24.3

Administrator's Guide to Hardware Appliances for ArcMC

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 appliance:

- CHA C8200 (Connector Hosting Appliance)

Intended Audience

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

Additional Documentation

This documentation library includes the following resources, based on the product that you use.

- CHA Appliance 24.3 Release Notes, which provides information about the latest release.
- *Documentation* site for ArcSight Platform where you can discover documentation for multiple ArcSight products.

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

ArcSight Management Center (ArcMC) is a centralized security management center that manages deployments of ArcSight solutions such as Transformation Hub, Logger, SmartConnectors, etc., through a single interface.

ArcSight Management Center (ArcMC) automates log collection and log management, whether you have a large ArcSight deployment or a small one. ArcSight Management Center (ArcMC) helps you with:

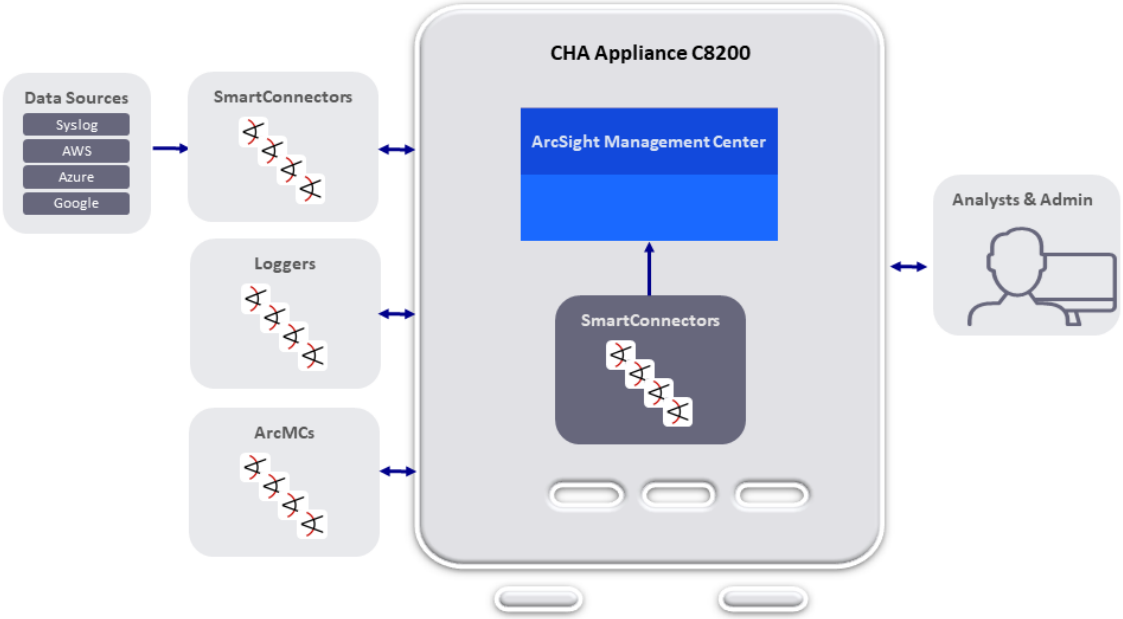
- The centralized management of ArcSight solutions.
- The automation of change management.
- The reduction of the resource requirement for security information and event management (SIEM).
- Easy management of large deployments, with reduction of administrative overhead and operational expenses.
- Efficient log traffic management.
- Bandwidth optimization for log collection.
- Support of IT operational analytics.

This appliance version of ArcSight Management Center (ArcMC) (CHA, or Connector Hosting Appliance) reinforces its known benefits, such as:

- Implementation of new and updated security policies in a quick and easy way.
- Configuration of managed nodes with an increased level of accuracy and error reduction.

How the CHA Appliance Works

Each appliance consists of a **single-node** version of ArcSight Management Center (ArcMC), configured to host and execute SmartConnectors, and to administrate and monitor CHA managed nodes (such as connector appliances, Loggers, other ArcSight Management Center (ArcMC)s, and Transformation Hub).


Data Sources
Syslog
AWS
Azure
Google
SmartConnectors
Loggers
ArcMCs
CHA Appliance C8200
ArcSight Management Center
SmartConnectors
Analysts & Admin

Chapter 2: Setting Up a CHA Appliance

You can verify the type of CHA you're using by going to System > LIcense & Upgrade in the menu, and looking at the Model value. Instructions in this page refer specifically to the C8200 model.

This section describes how to rack mount your CHA C8200. You do not need to run an installer when setting up your appliance; the software comes pre-installed on it. These basic steps enable you to start using your CHA appliances.

	Task	See
❑	1. Power on the Appliance	"Powering On the CHA Appliance" below
❑	2. Set up Remote Access	"Setting Up the Appliance for Remote Access" on the next page
❑	3. (Optional) Encryption of SEDs	"Encryption of SEDs" on page 10
❑	4. Appliance Initialization Procedures	"Setting Up the CHA C8200 Appliance " on page 10
❑	5. Appliance Configuration	"Configuring a CHA Appliance" on page 13

Powering On the CHA 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 CHA functionality.

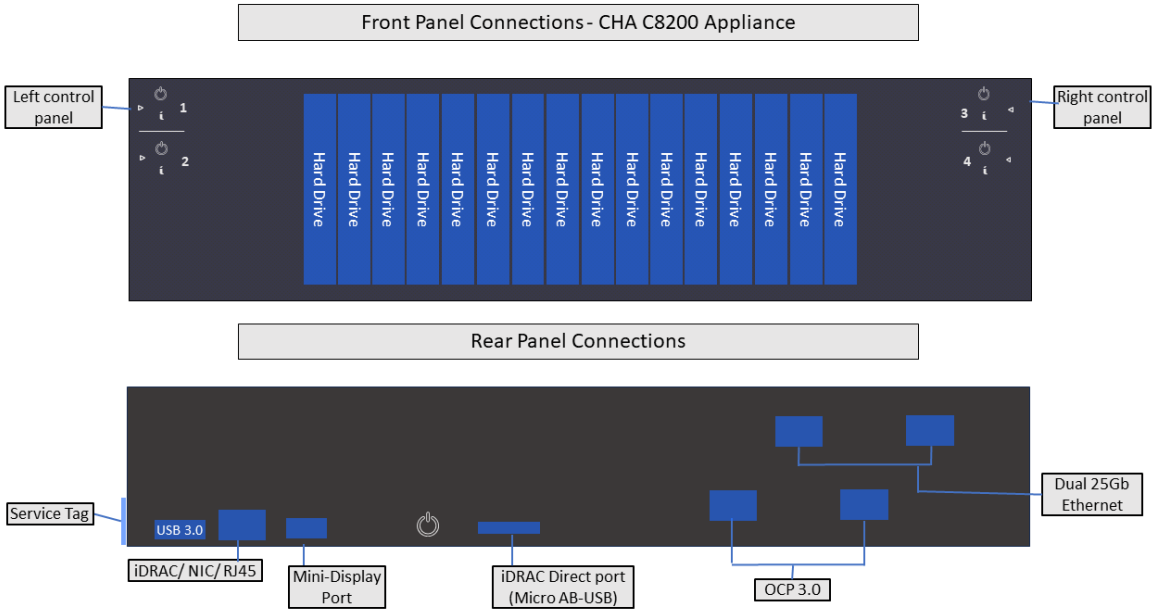
To install the appliance:

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.

Encryption of SEDs

The CHA 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.

Setting Up the CHA C8200 Appliance

The following instructions are intended to help you set up your CHA Appliance for its first use.

Configure a New IP Address

Use the appliance's Command Line Interface (CLI) to configure a new IP address, default gateway, hostname, and DNS and NTP servers. The CHA C8200 Appliance ships with the default IP address of `192.168.35.35 (subnet mask 255.255.255.0)` on `Eth0`.

Tip: You will need the following information available before proceeding:

- The new IP address, plus prefix or subnet mask.
- Your default gateway address.
- Your fully-qualified domain name.
- One or more name search domains and server addresses for DNS resolution.
- One or more NTP server addresses.

To configure a new IP address on the CLI:

1. On the CLI, connect to the appliance using these default credentials:

```
Login: admin
```

```
Password: password
```

2. Enter the new IP address with one of the following commands:

   ```
   set ip eth0 <ip>/<prefix>
   ```

   Where <ip>and <prefix> are your new IP address and prefix.

   Or:

   ```
   set ip eth0 <ip> <subnetmask>
   ```

   Where <ip>and <subnetmask> are your new IP address and subnet mask.

3. Execute the following command to set the default gateway:

   ```
   set defaultgw <address>
   ```

   Where <address> is your default gateway IP address.

4. Execute the following command to set the hostname:

   ```
   set hostname <FQDN>
   ```

   Where <FQDN> is the fully-qualified domain name of the host.

5. Execute the following command to set up DNS and nameservers:

   ```
   set dns <search_domain_1>, <search_domain_2>...<search_domain_N>
   <nameserver1> <nameserver2>...<nameserver_N>
   ```

   Where each <search_domain_N> must be replaced with a search domain, and each <nameserver_N> must be replaced with the IP address of a nameserver you wish to use for DNS.

6. Execute the following command to set up NTP servers:

   ```
   set <ntp_server_1> <ntp_server_2>...<ntp_server_N>
   ```

   Where each <ntp_server_N> must be replaced with the IP address of an NTP server you wish to use to set the Appliance time.

7. Execute the following command to review your settings:

   ```
   show config
   ```

   If any part of the information returned is incorrect, correct it using the same set commands as described above.

Accept the End User License Agreement

Upon first connecting to the appliance, you are prompted to accept the End User License Agreement (EULA).

1. Open a browser and connect to the CHA appliance at:

   ```
   https://<IP>
   ```

   Where <IP> is the newly configured IP address.
2. Review the terms of the license.
3. Select the I accept the terms of the License Agreement checkbox, and then click Accept.
4. Log in as an administrator using the default credentials.

   ```
   Login: admin
   ```

   ```
   Password: password
   ```

Appliance Licenses

While your appliance ships with its software already installed, you will require the ArcSight Management Center (ArcMC) per-instance software license key (purchased separately) to be able to get your appliance up and running.

Once the license has been installed, it will behave as a normal permanent license for ArcSight Management Center (ArcMC).

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 CHA.

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

Initialize the C8200 Appliance

The Appliance is initialized by uploading its license file. Optionally, you can also set the date and time, and change the admin login credentials to non-default values.

1. On the CHA Appliance menu, go to System > License & Update, click the Browse... button to look for your license file.
2. Click Upload Update and wait for the update to finish. An Update In Progress page displays the update progress.

   After the update has completed, the Update Results page displays the update result (success/failure).
3. A reboot is required after installing or updating a license.
4. Configure your date and time settings for the appliance.

5. Change the `admin` login credentials from their default values. For instructions, see Change Password.

For instructions on how to install your license key, see:

License & Update

Configuring a CHA Appliance

The links provided for each feature are meant as a starting point, and not meant to be exhaustive. You will find more in depth information in the ArcSight Management Center (ArcMC) Guide. Please be aware that CHA appliances are referred to as ArcMC appliances in that guide.

The installation and initialization process sets up your appliance with an initial, basic configuration. You can perform additional configuration on the appliance to adapt to your environment needs.

If you have installed multiple CHA appliances, connect to and configure each one separately.

Event Ingestion

The CHA appliance harnesses the Transformation Hub capabilities to receive events from SmartConnectors.

For more information see:

- Configuring ArcSight Management Center (ArcMC) to Manage a Transformation Hub
- Producing Events with SmartConnectors
- Pushing JKS files from ArcSight Management Center (ArcMC)

Configuring the Firewall on a CHA Appliance

Your CHA Appliance includes a script that you can use to configure the firewall. This script looks at your current CHA configuration and decides what ports to keep open. Alternatively, you can configure the firewall on your appliance as you would on any server, by editing `iptables-config` and white-listing the appropriate ports.

When called without arguments, the `/usr/sbin/arcfirewall` script previews and displays the ports that it will keep open, but takes no action to alter the firewall configuration. To alter firewall configuration, use the `-set` option.

To preview the list of ports the script will open:

1. Log into the appliance as root.
2. Run the following command:

   ```
   /usr/sbin/arcfirewall
   ```

   The script displays the ports that it would open, as shown in the following example.

   ```
   [root@myserver ~]# /usr/sbin/arcfirewall
   PREVIEW MODE - NO FIREWALL CHANGES...
   List of ports that firewall would allow inbound from any IP address:
   21/tcp
   22/tcp
   443/tcp
   9001/tcp
   9002/tcp
   9003/tcp
   9004/tcp
   9005/tcp
   9006/tcp
   9007/tcp
   9008/tcp
   123/udp
   ```

To configure the firewall:

1. Log into the appliance as root.
2. Run the following command:

   ```
   [root@myserver ~]# /usr/sbin/arcfirewall --set
   ```

   The script configures the firewall leaving the previewed ports open.

   If you configure a CHA appliance local container, assign it a network port, then run `arcfirewall`, the script will detect that the new port should be opened and list it in the preview of ports. You can then run `arcfirewall` with the `--set` option, as described above, to actually open the port.

   If `arcfirewall` is not run, and the port not opened, the connector will not receive any events.

SNMP

SNMP (Simple Network Management Protocol) can be used to monitor the health of your appliance. C8200 appliances support version 3 of SNMP.

The instructions in this page differ from the ones in the ArcSight Management Center (ArcMC) guide. Please use these instructions for the SNMP configuration of a C8200 appliance.

SNMP Configuration

You can configure SNMP polling and notifications. If SNMP polling is configured, a manager station can query the SNMP agent residing on the appliance. The information retrieved provides detailed information at the hardware and operating system level.

To configure SNMP polling:

1. In the main menu bar, click **Administration > Setup> System Admin**
2. In the navigation tree, under **System**, click **SNMP**.
3. On the **SNMPPoll Configuration** tab, ensure **Enabled** is selected.
   - For **Port**, the default is *161* but can be any available port. Ensure the specified port is open on your firewall.
   - For **SNMP version**, select *V3* and specify:
     - Username (alphanumeric lower-case string of 4-16 characters, which must begin with an alphabetic characters and may include underscores).
     - Authentication protocol: MD5 or SHA
     - Authentication passphrase (4 to 256 characters)
     - Privacy protocol: AES128
     - Privacy passphrase (4 to 256 characters).
4. Click **Save**.

If an SNMP destination is configured, the appliance can send notifications for a limited set of events (see "Viewing SNMP System Information" on the next page).

SNMP notifications differ from those sent by connectors, which are for a generic ArcSight event. The notifications listed here are specific to a single event, making them easier for understanding by a network management system.

To configure the destination for SNMP notifications:

1. In the main menu bar, click **Administration > System Admin**
2. In the navigation tree, under **System**, click **SNMP**.
3. On the **SNMP Destination** tab, ensure **Enabled** is selected. Then, specify values for the other parameters that match your existing NMS SNMP settings.

- For Port, specify *162*.

  Specifying a non-default port may cause a brief delay. Give the process time to complete.

- For SNMP version, select *V3* and then specify values for the prompted settings.
- Authentication Protocol: MD5 or SHA
- Privacy Protocol: AES128

4. Click **Save**

Viewing SNMP System Information

SNMP notifications are viewable in any MIB browser. The following SNMP notifications are supported:

- **Application**
  - Login attempt failed
  - Password change attempt failed
  - User account locked
  - Reboot command launched
  - Manual backup failed
  - Enable FIPS mode successful
  - Disable FIPS mode successful
  - Enable FIPS mode failed
  - Disable FIPS mode failed
- **Platform**
  - CPU Usage
  - Memory Usage
  - Disk Almost Full
  - Fan Failure
  - Power Supply Failure
  - Temperature Out of Range
  - Ethernet Link Down

To view system notifications in an MIB browser on your appliance:

You can download the ArcSight MIB file and other standard Net-SNMP MIB files using the following URLs:

```
https://<system_name_or_ip>/platform-service/ARCSIGHT-EVENT-MIB.txt
```

```
https://<system_name_or_ip>/platform-service/DISMAN-EVENT-MIB.txt
```

```
https://<system_name_or_ip>/platform-service/HOST-RESOURCES-MIB.txt
```

```
https://<system_name_or_ip>/platform-service/IF-MIB.txt
```

```
https://<system_name_or_ip>/platform-service/UCD-SNMP-MIB.txt
```

MIB Contents

Notifications are written to the following modules of the MIB file:

Module	Notification Types
HOST-RESOURCES-MIB	Standard hardware parameters.
IF-MIB	Objects for network interfaces.
IP-MIB	IP and ICMP implementations.
DISMAN-EVENT-MIB	Event triggers and actions for standard network management.

SSH, FTP, Diagnostic Tools and Audit Forwarding

SSH Access to the Appliance

By default, SSH access to the appliance is disabled. If required, follow this procedure to enable, disable and use SSH access to your appliance:

Although the instructions in the procedure linked below call for logging in as a root user, for C8200 appliances you must use the otadmin user and the change_me password.

After the initial login, you can switch back to the root user as needed.

Enabling or Disabling SSH Access

FTP Protocol

For an appliance to use FTP protocol, it must be enabled with a maximum accumulated files directory size. Follow the procedure below to configure it:

Enabling FTP

Diagnostic Tools

The appliance Diagnostic tools are available for set up, management, and troubleshooting tasks. For more information see:

Diagnostic Tools

Configuring Audit Forwarding

For Audit Forwarding, you will require a single `syslog` connector installed in your appliance. Follow the procedure below to configure it:

To configure audit forwarding for ArcMC Appliance

Chapter 3: Navigating the User Interface

The links provided for each feature are meant as a starting point, and not meant to be exhaustive. You will find more in depth information in the ArcSight Management Center (ArcMC) Guide. Please be aware that CHA appliances are referred to as ArcMC appliances in that guide.

The CHA browser-based user interface consists of a menu bar at the top, which provides access to the main functional components of CHA.

The menu bar options are:

- Dashboard
- Node Management
- Configuration Management
- User Management
- Administration
- Job Manager 
- Admin: which includes the following options
  - Help: to access the product help
  - About: to see your CHA version information
  - Logout: to close your session
- Stats
- Site Map

Chapter 4: Backup and Restore Procedures

OpenText recommends to perform backups of the information and configuration of a CHA 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 verify the type of CHA you're using by going to System > LIcense & Upgrade in the menu, and looking at the Model value. Instructions in this page refer specifically to the C8200 model.

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 CHA you are restoring. Find the name of the file in the **Downloading Your Factory Restore Image Files** section of the CHA Appliance 24.3 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 22 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/sdb
   bs=1M
   ```

   Where `<iso_image_file_name>` is the name of the image file downloaded here.

   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 9
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** ARCMC-C6615-C8200-RH92-FIPS-STIG-CIS2-xx.x.x-x.iso 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:

   "Setting Up the CHA C8200 Appliance " on page 10

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 9

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 Optical Drive**.
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** ARCMC-C6615-C8200-RH92-FIPS-STIG-CIS2-xx.x.x-x.iso 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:

   "Setting Up the CHA C8200 Appliance " on page 10

Managing Backups and Restoring from them

The links provided for each feature are meant as a starting point, and not meant to be exhaustive. You will find more in depth information in the ArcSight Management Center (ArcMC) Guide. Please be aware that CHA appliances are referred to as ArcMC appliances in that guide.

The Backup and Restore menu options enable you to back up and restore your CHA configuration. A complete backup includes: all data on managed nodes, configurations, system administration, and connector data (in `agentdata` folders), as well as all repository files.

You can also choose to include a selection of the data in a given backup file, to make your backup file smaller and more manageable.

For more information, see:

- Backup
- Restore

Publication Status

Released: Monday, September 30, 2024

Updated: 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 ArcMC (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!