

---

**opentext™**

# **W8300 Appliance**

Software Version: 24.2.3

## **Administrator's Guide to the W8300 Appliance**

# Legal Notices

Open Text Corporation  
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

# Copyright Notice

Copyright 2024 OpenText

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without 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: <a href="https://www.microfocus.com/en-us/contact-support/stackb">https://www.microfocus.com/en-us/contact-support/stackb</a>
Support Web Site	<a href="https://www.microfocus.com/en-us/support">https://www.microfocus.com/en-us/support</a>
ArcSight Product Documentation	<a href="https://www.microfocus.com/documentation/arcSight/#gsc.tab=0">https://www.microfocus.com/documentation/arcSight/#gsc.tab=0</a>

# Contents

About this Guide .....	4
Intended Audience .....	4
Additional Documentation .....	4
Contact Information .....	4
How the W8300 Appliance Works .....	5
NFS Server Not Included .....	5
High Availability Supported .....	5
Chapter 1: Setting Up a W8300 Appliance .....	6
Powering On the W8300 Appliance .....	6
Setting Up the Appliance for Remote Access .....	7
Changing the iDRAC password on your Appliance .....	7
Appliance Licenses .....	7
Features Included with the License .....	7
First Boot Initialization of the W8300 Appliance (Bootstrapping) .....	8
Regeneration of the First Login Token .....	11
Configuring a W8300 Appliance .....	11
Event Ingestion .....	11
Firewall .....	12
Deploying a W8300 Appliance .....	12
Restoring an Appliance to Factory Settings .....	14
Restoring an Appliance Using a USB Memory Stick .....	15
Image Burning .....	15
Restore Procedure: .....	15
Restoring an Appliance Using iDRAC Access .....	16
Restore Procedure: .....	17
Chapter 2: Managing the W8300 Appliance .....	19
Managing a Deployment .....	19
Adding a New Node .....	20
Updating a Node's Operating System .....	20
Restarting the Appliance .....	21
Publication Status .....	24
Send Documentation Feedback .....	25

# About this Guide

This installation guide provides instructions on how to install and initialize a standalone W8300 appliance.

For more information, see ["How the W8300 Appliance Works" on the next page](#).

## Intended Audience

This book provides information for admins who need to install, initialize, and restore W8300 appliances.

## Additional Documentation

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

### ArcSight Platform

- [ArcSight Platform 24.2.3 Release Notes](#), which provides information about the latest release.
- The Administrator's guide, which provides concepts, use cases, and guidance for installing, upgrade, managing, and maintaining the ArcSight Platform in your environment. See the guide corresponding to your deployment:
  - [Administrator's Guide for the ArcSight Platform 24.2.3 - Off-Cloud Deployment](#)
- [Technical Requirements for ArcSight Platform 24.2.3](#), which provides information about the hardware and software requirements for installing ArcSight Platform and the deployed capabilities in your environment.
- [ArcSight Platform Upgrade Paths](#), which provides information about the paths to upgrade to the latest release from your current release.
- [ArcSight Solutions and Compliance Insight Packages](#), which provide a complete set of compliance and audit related packages and documentation.
- [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](mailto:Documentation-Feedback@microfocus.com).

For specific product issues, contact [OpenText Customer Care](#).

## How the W8300 Appliance Works

The W8300 appliance enables you to install and run ArcSight Platform applications in a containerized stack powered by Kubernetes. Each W8300 comprises a Kubernetes master node and a worker node. Thus a production setup with 4 appliances would comprise 4 master nodes and 4 worker nodes. Each W8300 is a SLED appliance and can have a common power supply.

W8300 includes OpenText Recon and OpenText Transformation Hub by default, but additional capabilities may be added, such as OpenText SOAR and OpenText ESM.



OpenText Intelligence is not supported on W8300.

## NFS Server Not Included







The W8300 appliance does **not** include any default Network File System (NFS). You must supply and provide network access from the appliance to a third-party NFS for effective use of the appliance.

## High Availability Supported

To increase cluster availability, you can simply add more appliances. OpenText recommends that a production environment includes at least 3 appliances (that is, 3 master and 3 worker nodes). Note that any deployment of 3 or more appliances will require a virtual hostname, which is explained in the deployment section.

# Chapter 1: Setting Up a W8300 Appliance

This section describes how to rack mount your W8300 R8000 and R8100 Appliances. 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 W8300 appliances.

	Task	See
	1. Power on the W8300 Appliance	<a href="#">"Powering On the W8300 Appliance" below</a>
	2. Set up Remote Access	<a href="#">"Setting Up the Appliance for Remote Access" on the next page</a>
	3. Appliance Licenses	<a href="#">"Appliance Licenses" on the next page</a>
	4. First Boot of the Appliance	<a href="#">"First Boot Initialization of the W8300 Appliance (Bootstrapping)" on page 8</a>
	5. Appliance Configuration	<a href="#">"Configuring a W8300 Appliance" on page 11</a>
	6. Deploying a W8300 Appliance	<a href="#">"Deploying a W8300 Appliance" on page 12</a>

## Powering On the W8300 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 W8300 functionality.

### To power on the appliance:

1. Unpack the appliance and its accompanying accessories.



**Note:** Read carefully through the instructions, cautions, and warnings that are packed 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 to a suitable rack.
3. Make the front and rear panel connections.
4. Activate the power switch.

## 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](#).

## Appliance Licenses

Redeem your license on the [Software Entitlements Portal](#), then download the license file to a computer from which you can connect to W8300. For more information, refer to the software delivery confirmation email you received from OpenText.

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

[Installing Your License Key](#)

### Features Included with the License

For more information regarding what's included in your license refer to the following topics:

[Understanding the Types of Licenses](#)

[How Your License Affects Data Storage Policies](#)

## First Boot Initialization of the W8300 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.

Perform this operation on each appliance to initialize it on first boot.

1. Log into your appliance using iDRAC (see "[Setting Up the Appliance for Remote Access](#)" on the [previous page](#) 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 (arcsight) and password (change\_me).
5. You will be required to change the password for arcsight. Enter a new password and retype it to confirm.

```
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 display, with the **User must set 'root' password to proceed** message. You will be required to enter the arcsight user password you just reset to make the change to the root password:

```
password for arcsight
Changing password for user root.kill bi
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. 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
*****
Select one active connection to configure:
```

```
*****
1) enoxxxxnp0
#? 1
```

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

- Configure the network using a static IP address (FQDN) by providing this information:

```
*****
Configure the network connection enoxxxxnp0 for device enoxxxxnp0:
*****
Enter the hostname (FQDN) for this appliance: your_appliance_host_fqdn

Configure network using static IP address:
Enter static IPv4 address:
Enter IPv4 prefix (1-32):
Enter IPv4 gateway:
Enter IPv4 Primary DNS server:
Enter IPv4 Secondary DNS server (optional):
Enter spaced separated IPv4 DNS search domains: your_appliance_domain
```

- Next, the NTP server must be configured:

```
*****
NTP Server Configuration
*****
WARNING: You must specify an accessible NTP server

Enter the NPT server for this appliance:
```

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 configure network settings and NTP services using above
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...
```

To proceed, you will be asked for the root password again, as confirmation.

- 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>:6443 to install Recon product
IMPORTANT: You will need the token to login for the first time:
```

```
XXXXXXXXXX  
*****
```



The console will not allow you to copy the token, which you will need for your first login to the **Recon 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

In case there's a need to obtain a First Login Token again (other than with the preceding procedure), you can regenerate it by running the following command in the console:

```
# /var/opt/arcsight/appliance_scripts/generate_first_login_token.sh
```

You will be prompted for the arcsight password, and after providing it, the First Login Token will be generated again:

```
=====  
Go to https://<your_appliance_host_fqdn>:6443 to install Recon product  
IMPORTANT: You will need the token to login for the first time:  
XXXXXXXXXX  
=====
```

## Configuring a W8300 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 [User's Guide for ArcSight Platform CE 24.2.3](#).

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

If you have installed multiple W8300 appliances, connect to and configure each one separately.

## Event Ingestion

The W8300 appliance harnesses the Transformation Hub capabilities to receive events from SmartConnectors.

See [Producing Events with SmartConnectors](#) for more information.

## Firewall

The firewall for the W8300 appliance comes pre-configured, with the following ports open by default to facilitate the initial setup:

Port	Protocol	Description
22	HTTPS	Used by the appliance installer
6443	HTTPS	Used by the appliance installer

The rest of the ports required for the appliance's normal functions (such as for infrastructure, capabilities and supported components), are listed [here](#).

## Deploying a W8300 Appliance

This section will describe how to set up and deploy a W8300 appliance.

1. Log into the appliance using your ArcSight-supplied organizational credentials (username and password) and then click **Log in**.
2. On the **OpenText EULA** page, review the OpenText End User License Agreement. Select **I have read and agree with the end user license agreement** and then click **Next**.
3. On the **RedHat EULA** page, review the RedHat End User License Agreement. Select **I have read and agree with the end user license agreement** and then click **Next**.
4. On the **Deployment** page, ensure that the **External NFS** checkbox is selected, and then do the following:
  - a. In **NFS server**, enter the name of your third-party NFS server.
  - b. In **NFS path**, enter the network path to your NFS server.



The third-party NFS may **NOT** use RHEL 9.4 or Rocky Linux 9.4 hardened OS.

5. To add nodes to your cluster, under **Add Nodes**, click **Add Node**. The very first node you add will be the primary node.
6. On the **Add Node** dialog, in **Application Hostname/IP address**, enter the FQDN or the network path to the new node.
7. In **ArcSight OS user password**, enter the password to the node (your ArcSight password), then click **Save**. The node is added to your list of nodes.
8. On the list of nodes, select the newly-added node. In the **Node Type** column, click the down arrow in the column header, and then select a type for this node (master or worker).

9. In the **Label** column, click the down arrow in the column header and select a label. A label will indicate a capability you will run on the node. Examples of labels include *Core* and *Transformation Hub*. A node may have more than one label, which will indicate more than one capability will be processed on that node.
10. Repeat steps 6-9 until you have added and labeled all of your nodes.
11. (Conditional) If your cluster includes 3 or more nodes, in **Virtual Hostname**, enter the hostname of your cluster.
12. (Conditional) If you have labeled any nodes with the *Transformation Hub* label, on the **Transformation Hub** page, enter values for the following and then click **Next**:
  - a. **Retention in bytes for Avro topics**: Size in bytes of the retained data per partition for two Avro Kafka topics, th-arcsight-avro and mf-event-avro-enriched.
  - b. **Retention in bytes for CEF topics**: Size in bytes of the retained data per partition for non-Avro topics
  - c. **ArcMC generator ID range start**: Every event generated by an ArcSight component will have a unique Global Event ID. This is the start of the generator ID range.
  - d. **ArcMC generator ID range end**: End of the generator ID range.
  - e. **Replica count**: The number of CEF-to-Avro Stream Processor Instances to start. CEF-to-Avro Stream Processors convert incoming CEF events from th-cef topic to Avro format and route these events to th-arcsight-avro topic.
13. (Conditional) If you have labeled any nodes with the *Core* label, on the **Database** page, enter values for the following and then click **Next**. Database nodes are optional if Transformation Hub is the only capability in the cluster.
  - a. **Database administrator username**: Username for the DB administrator account.
  - b. **Set Password**: Set a password for the application administrator username.
  - c. **Confirm Password**: Retype password to confirm.
  - d. **S3 URL**: FQDN of the S3 database.
  - e. **S3 Access password**: Set S3 password.
  - f. **Confirm S3 Access password**: Retype password to confirm.
  - g. **Use SSL**: If selected, connections to the database node will be made over SSL. After enabling, click **Upload Certificate**. Then, on the **Upload Certificate** dialog, enter the certificate name. Click **Choose File** and browse to the certificate file location, and then click **Upload**.
14. (Conditional) To enable SOAR for your cluster, select **Enable SOAR**.
15. Click **Next**.

Node labels assigned in Step 9 will indicate to the wizard that the capability represented by the label will need to be configured. You will be presented only the steps below that correspond to

your own deployment. Labeling a node with *Nah*, will cause the wizard to prompt for configuration of the Database and Recon. See the *ArcSight Platform 24.2 Administrator's Guide* for more information on these settings.

16. (Conditional) If you have labeled any nodes with the *Recon* label, on the **Recon** page, enter values for the following and then click **Next**:
  - a. **Application administrator username**: ArcSight username.
  - b. **Set Password**: Set a password for the application administrator username.
  - c. **Confirm password**: Retype password to confirm.
  - d. **Enable Multitenancy**: If selected, the cluster will support multitenancy. See the *ArcSight Platform 24.2 Administrator's Guide* for more information.
17. On the **Review Summary** page, review and verify the summary information provided. If the summary is correct, click **Submit**. If not, click **Previous** to return to the previous page containing the incorrect information. Then correct the information, return to this page, and click **Submit**.
18. The appliance configuration proceeds and you will be informed about failure or success.
  - a. On a failure, the appliance displays an error message. Click **Retry** to submit the information. Alternatively, click **Exit** to exit the wizard and review the error logs, and then re-run the setup wizard (return to Step 1, above).
  - b. With success, the setup is confirmed and your cluster URL is displayed. Click **Copy URL** to copy the URL to your clipboard, then paste it into a browser to access the cluster.
19. Click **Exit Setup**.

To deploy a cluster of W8300 appliances, repeated Steps 1-18 for each individual appliance.

## 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 W8300 you are restoring. Find the name of the file in the **Downloading the ArcSight Platform Installation Files** section of the [ArcSight Platform 24.2.3 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" on the next page](#) method

- If you have only iDRAC access to the appliance, use the ["Restoring an Appliance Using iDRAC Access" on the next page](#) 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 7](#)
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 User Image RECON-R7615-R8X00-RH92-FIPS-STIG-XXXXXX.iso** option at the top to start right away.

Twice during this process you will receive a warning about all the data in the partition or hard disk being overwritten. You must enter Y to proceed both times:

```
Are you sure you want to continue? (y/n)
```

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 10 minutes. Once the restore process has reached this point:

```
realtime =none
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:

[Connecting to the W8300 Appliance](#)

## 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 7](#)

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 User Image RECON-R7615-R8X00-RH92-FIPS-STIG-XXXXXX.iso** option at the top to start right away.

Twice during this process you will receive a warning about all the data in the partition or hard disk being overwritten. You must enter Y to proceed both times:

```
Are you sure you want to continue? (y/n)
```

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 10 minutes. Once the restore process has reached this point:

```
realtime =none
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:

[Connecting to the W8300 Appliance](#)

# Chapter 2: Managing the W8300 Appliance

## Managing a Deployment

You can manage your deployment on the **Manage Deployment** page, viewing the details of nodes, adding new nodes, and updating a node's operating system.

### To view your nodes in detail:

In the navigation menu, click **Manage Deployment**. The page shows all nodes deployed in your cluster by name, type, labels assigned to the node, and status.

- **Name:** The name assigned to the node.
- **Type:** Shows Master or Worker.
- **Labels:** Shows one or more labels you assigned to the node, such as Recon or Transformation Hub.
- **Status:** Enables you to turn a node on or off.

### To manage or edit the settings for a node:

1. On the **Manage Deployment** page, select the node you wish to edit. You can edit the node type or the labels applied to a node.
2. Select a setting to edit by clicking the down arrow in the corresponding column header.
3. On the resulting dropdown, edit the settings as desired.
4. Click **Save**.

## Adding a New Node

### To add a new node:

1. On the **Manage Deployment** page, click **Add Node**.
2. On the **Add Node** dialog, enter the details of the new node:
  - **Application/Hostname IP:** Hostname or FQDN of the new node.
  - **ArcSight OS User Password:** The node's ArcSight account password.
3. Click **Save**.
4. Select the new node, then click the dropdown under **Type** and select a type for the new node.
5. Click the dropdown under **Label** and select one or more labels for the new node.

## Updating a Node's Operating System

### To update a node's OS:

1. Download the update file for the operating system to a secure network location.
2. On the **Manage Deployment** page, click **OS Update**.
3. Select a node to update.
4. On the **OS Update** dialog, browse to the location of the update file and click **Update**. The new OS version is applied to the selected node.

## Restarting the Appliance

The following steps are required to stop the appliance's processes, which would be required to perform maintenance, or when updating the OS.

The following commands must be executed as the root user.

1. Check that kubernetes is in running status:

```
kubect1 get pods -A
```

In the output, all pods must be in **Running** or **Completed** state.

2. Check the status of the ArcSight Database kafka scheduler:

```
cd /opt/arcsight-db-tools
```

```
./kafka_scheduler status
```

The scheduler must be in a running status, without exception.

3. (If Multi-Tenancy is enabled) Check the event flow for each tenant:

```
./kafka_scheduler events -t $tenant
```

The event flow must be running well.

4. Stop kubernetes with the following commands:

```
cd /opt/arcsight/kubernetes/bin
```

```
./kube-stop.sh
```

The operation must succeed without exception.

5. Stop the database with these commands:

```
cd /opt/arcsight-db-tools
```

```
scripts/watchdog.sh disable
```

The operation must succeed without exception.

```
./db_installer stop-db
```

The command should have the following output:

```
Database fusiondb stopped successfully
```

6. You can now perform the planned operation on the appliance.



If a reboot is needed, you can execute it at this point.

7. (Conditional) If the appliance has not been rebooted, execute these steps to resume operations:

```
cd /opt/arcsight/kubernetes/bin
```

```
./kube-start.sh
```

The operation must succeed without exception.

8. Check the kubernetes status:

```
kubectl get pods -A
```

In the output, all pods must be in **Running** or **Completed** state.

9. Start the ArcSight Database with these commands:

```
cd /opt/arcsight-db-tools
```

```
./db_installer start-db
```

The command should have the following output:

```
Database fusiondb: Startup Succeeded. All Nodes are UP
```

10. Start the scheduler with this command:

```
./kafka_scheduler start
```

The operation must succeed without exception.

11. Start the watchdog:

```
scripts/watchdog.sh enable
```

The operation must succeed without exception.

12. Check the status of the database kafka scheduler:

```
./kafka_scheduler status
```

The scheduler must be running without exception.

13. (If Multi-Tenancy is enabled) Check the event flow for each tenant:

```
./kafka_scheduler events -t $tenant
```

The event flow must be running well.

# Publication Status

**Released:** NOT RELEASED

**Updated:** Wednesday, November 13, 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 the W8300 Appliance (8000 Appliance 24.2.3)**

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](mailto:documentation-feedback@microfocus.com).

We appreciate your feedback!