

ZENworks

System Updates Reference

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/en-us/legal>.

© Copyright 2008 - 2023 Open Text

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.

About This Guide

This *ZENworks System Updates Reference* explains how to obtain updates to ZENworks software on a timely basis and how to schedule automatic downloads of the updates. The guide includes the following sections:

- ♦ [Chapter 1, “Pre-deployment Settings,” on page 7](#)
- ♦ [Chapter 2, “Managing Update Downloads,” on page 23](#)
- ♦ [Chapter 3, “Deploying Updates,” on page 35](#)
- ♦ [Chapter 4, “Deleting Updates,” on page 57](#)
- ♦ [Chapter 5, “Reviewing the Content of an Update,” on page 59](#)
- ♦ [Chapter 6, “Update Statuses,” on page 63](#)
- ♦ [Chapter 7, “Configuring the System Update Behavior of the ZENworks Agent,” on page 67](#)
- ♦ [Chapter 8, “Troubleshooting System Updates,” on page 75](#)

Audience

This guide is intended for ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the **comment on this topic** feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks documentation website](#).

Contents

About This Guide	3
1 Pre-deployment Settings	7
1.1 System Update Settings	7
1.1.1 System Update Entitlement	7
1.1.2 Check for Updates Schedule	8
1.1.3 Download Schedule	10
1.1.4 Email Notification	11
1.1.5 Proxy Server Settings	12
1.1.6 Dedicated Server Settings	12
1.1.7 Stage Timeout Settings	13
1.1.8 Reboot Behavior	14
1.2 Creating Deployment Stages	15
1.2.1 Understanding Stages	15
1.2.2 Creating and Populating a Deployment Stage	17
1.2.3 Modifying the Stage Timeout	18
1.2.4 Modifying Staging Behavior	19
1.2.5 Modifying Reboot Behavior	20
1.2.6 Modifying the Membership of a Deployment Stage	20
1.2.7 Renaming a Deployment Stage	21
1.2.8 Deleting a Deployment Stage	21
1.2.9 Rearranging the Staging Order	21
2 Managing Update Downloads	23
2.1 Understanding Available Updates	23
2.2 Downloading Updates	24
2.2.1 Scheduling Update Downloads	24
2.2.2 Manually Checking for Updates	25
2.2.3 Manually Download Updates	25
2.2.4 Manually Importing Updates to Servers without Internet Connectivity	27
2.3 Downloading and Installing the PRU	27
2.4 PRU Schedule	28
2.4.1 PRU Availability Check Schedule	28
2.4.2 PRU Download Schedule	29
2.4.3 PRU Deployment Schedule	30
2.4.4 Email Notification	30
2.5 Canceling or Deleting a System Update	31
2.6 Preparing an Update	31
2.7 Retry Prepare Update	32
2.8 Authorizing an Update	33
2.9 Configuring an Update	33
3 Deploying Updates	35
3.1 Update Prerequisites	35

3.2	Understanding Deploying Updates	37
3.3	Deploying Updates	41
3.3.1	Upgrading the Agent in VDI environment	45
3.4	Starting a Pending Stage	46
3.5	Rescheduling a Deployment	46
3.5.1	Rescheduling a Deployment for the All Stages Status	46
3.5.2	Rescheduling a Deployment for the Other Statuses	46
3.6	Bypassing Staging	47
3.7	Canceling a Deployment	47
3.8	Clearing an Error to Retry a Deployment	48
3.9	System Update Fails on the Device with an Error Code	48
3.10	Viewing Status by Device	48
3.10.1	Understanding Device Statuses	48
3.10.2	Viewing a Device Properties	49
3.10.3	Viewing Information of a Device Status	49
3.10.4	Viewing Status by Device - Advanced	49
3.10.5	Toggling Ignored Devices	51
3.10.6	Redeploying Updates to Devices	52
3.10.7	Refreshing Devices	52
3.10.8	Searching - Status by Device	52
3.11	Viewing the System Update Deployment Status	53
3.12	Standalone Agent Updater	54
3.12.1	Creating the Standalone Agent Updater executable	54
3.12.2	Executing the Standalone Agent Updater	55
3.12.3	Viewing the Standalone Agent Updater log files	55
3.13	Superseded Files	56
3.14	Limitations of System Update	56
3.14.1	System Update on Windows 10 devices connected through RDP	56
4	Deleting Updates	57
5	Reviewing the Content of an Update	59
5.1	Viewing the Release Details Page	59
5.2	Update Release Details	59
5.3	Deployment History	60
5.3.1	Understanding Deployment History Details	61
5.3.2	Performing Deployment History Tasks	62
6	Update Statuses	63
7	Configuring the System Update Behavior of the ZENworks Agent	67
7.1	ZENworks Updater Service	71
7.1.1	Refresh Interval	71
7.1.2	Configuring ZEUS to Communicate Using a Non-Standard Port	72
8	Troubleshooting System Updates	75

1 Pre-deployment Settings

Perform the following tasks to configure your update process:

- [Section 1.1, “System Update Settings,” on page 7](#)
- [Section 1.2, “Creating Deployment Stages,” on page 15](#)

1.1 System Update Settings

You should configure System Update settings before attempting to use it. Following are the settings that you can configure:

- [Section 1.1.1, “System Update Entitlement,” on page 7](#)
- [Section 1.1.2, “Check for Updates Schedule,” on page 8](#)
- [Section 1.1.3, “Download Schedule,” on page 10](#)
- [Section 1.1.4, “Email Notification,” on page 11](#)
- [Section 1.1.5, “Proxy Server Settings,” on page 12](#)
- [Section 1.1.6, “Dedicated Server Settings,” on page 12](#)
- [Section 1.1.7, “Stage Timeout Settings,” on page 13](#)
- [Section 1.1.8, “Reboot Behavior,” on page 14](#)

1.1.1 System Update Entitlement

In ZENworks 2017 or later, you need to activate the System Update entitlement to obtain updates to the ZENworks 2017 software on a timely basis. Before activating the entitlement, ensure that the Primary Server you want to use to activate the entitlement can communicate with the [NCC server \(https://secure-www.novell.com\)](https://secure-www.novell.com).

The System Update Entitlement panel displays the System Update entitlement status and allows you to activate the System Update entitlement for the ZENworks 2017 in the Management Zone to receive the latest version of ZENworks System Updates and Product Recognition Updates (PRUs) from the Novell Customer Center (NCC) server.

To activate the entitlement:

- 1 In ZENworks Control Center (ZCC), click **Configuration**, in the left pane.
- 2 In the **Configuration** page, click **Infrastructure Management > System Update Settings**.
- 3 Configure the following settings:
 - **Email Address:** Specify a valid email address to be used for communication from Micro Focus. We recommended that you specify the email address used to purchase the System Update Entitlement.

- ♦ **Activation Code:** Specify the System Update entitlement activation code. You can access the System Update entitlement activation code by visiting the Micro Focus Customer Center. The activation code to activate the Entitlement is available below the **Software** tab. For the current version of ZENworks, use the related valid activation code that has **ZENworks Configuration Management Activation Code** in the description.

To purchase the System Update Maintenance Entitlement, contact an authorized Micro Focus Sales representative or a Certified Micro Focus Partner.

4 Click **Activate**.

The specified information is validated with the NCC server, and subsequently the entitlement is created for the Management Zone in the NCC server.

Retry System Update Entitlement

During [Step 4](#) in [Section 1.1.1, “System Update Entitlement,” on page 7](#), if validation with the NCC server fails due to connectivity issues, you will be prompted to retry the system update activation process in the background. If you click Yes, the system update activation will be initiated in the background.

The `SUEntitlementConf.properties` file has the following settings, which are used for the System Update Entitlement configuration. The values for these settings are initiated based on the values you enter in the `SUEntitlementConf.properties` file:

- ♦ **connection-timeout:** This is the connection timeout value in seconds for establishing a connection with the NCC server.
- ♦ **retryCount-Activation:** This is the maximum number of retries allowed in the background when configuring the System Update entitlement.
- ♦ **sleepInterval-Activation:** This is the sleep interval allowed between retries for the system update activation in the background.

To change the default value of these settings in the `SUEntitlementConf.properties` file, go to the following path:

Linux: `/etc/opt/novell/zenworks/SUEntitlementConf.properties`

Windows: `%zenworks_home%/conf/SUEntitlementConf.properties`

If you click the **Configure** link when the SU-Entitlement activation is in progress in the background, the system displays a warning message.

1.1.2 Check for Updates Schedule

The default is to not schedule update checking (**No Schedule** is displayed in the **Schedule Type** field). With this scheduling option selected, the only way you can check for software updates is to do so manually in the **Available System Updates** panel on the **System Updates** tab.

You can specify how often you want to check for updates. When you specify the schedule, information on available updates is automatically downloaded from Micro Focus to the **Available System Updates** panel on the **System Updates** tab when the schedule starts. This does not download the update content itself. Downloading can be scheduled in the **Download Schedule** panel (see [“Download Schedule” on page 10](#)).

To schedule checking for the ZENworks software updates:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **Configuration** tab.
- 2 Click **Management Zone Settings** to expand its options, click **Infrastructure Management** to expand its options, and then select **System Update Settings**.

In the **Check for Updates** panel, there are two scheduling options for updates:

- ♦ **No Schedule:** The default is to not schedule update checking. With this scheduling option selected, the only way you can check for software updates is to do so manually in the **Available System Updates** panel on the **System Updates** tab. To specify the **No Schedule** option, continue with [Step 3](#).
 - ♦ **Recurring:** Lets you specify how often you want to check for updates. When you set this option, information on available updates is automatically downloaded from Micro Focus to the **Available System Updates** panel on the **System Updates** tab when the schedule starts. This does not download the update content itself. To set a recurring schedule, skip to [Step 4](#).
- 3 (Conditional) To exclude scheduled checking for software updates (the default), click the down-arrow in the **Schedule Type** field, select **No Schedule**, click **Apply** to save the schedule change, then skip to [Step 6](#).

With this option selected, you must check for updates manually. For more information, see [“Downloading Updates” on page 24](#).

- 4 (Conditional) To set a recurring schedule for checking for updates to your ZENworks software, click the down-arrow in the **Schedule Type** field, then select **Recurring**.
- 5 Fill in the fields:
 - 5a Select one or more check boxes for the days of the week.
 - 5b To set the time of day for checking to occur, use the **Start Time** box to specify the time.
 - 5c (Optional) For additional scheduling options, click **More Options**, then select the following options as necessary:

- ♦ **Process Immediately if Device Unable to Execute on Schedule:** Checks for updates to occur as soon as possible, if the checking cannot be done according to schedule. For example, if a server is down at the scheduled time, checking for updates occurs immediately after the server is available.
- ♦ **Use Coordinated Universal Time:** Schedules to interpret the times you specify as UTC instead of local time.
- ♦ **Start at a Random Time Between Start and End Times:** Allows checking for updates to occur at a random time between the specified time and the time specified in [Step 5b](#). Fill in the **End Time** fields.
- ♦ **Restrict Schedule Execution to the Following Date Range:** In addition to the other options, you can specify a date range when the checking should occur.

- 5d When you have finished configuring the recurring schedule, click **Apply** to save the schedule change.
- 6 To exit this page, click **OK** when you are finished configuring the schedule.

Click **OK** to save and apply your changes. Click **Cancel** to close the page, but your unapplied changes will be discarded.

1.1.3 Download Schedule

The default is to not schedule downloading of updates (**No Schedule** is displayed in the **Schedule Type** field). With this scheduling option selected, the only way you can download updates is to do so manually in the **Available System Updates** panel on the **System Updates** tab.

If you do specify how often you want to download updates, you should set this schedule in conjunction with the schedule to check for updates (see [“Check for Updates Schedule” on page 8](#)).

After an update has been checked, the information is displayed in the **Available System Updates** panel on the **System Updates** tab, you can schedule the download from Micro Focus to automatically occur when the schedule starts.

To schedule ZENworks software updates:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, and then click the **Configuration** tab.
- 2 Click **Management Zone Settings** to expand its options, click **Infrastructure Management** to expand its options, and then select **System Update Settings**.

In the **Download Schedule** panel, there are two scheduling options for downloading updates:

- ♦ **No Schedule:** By default, **No Schedule** is displayed in the **Scheduled Type** field. When schedule is not set, then you have to download the updates manually in the **Available System Updates** panel on the **System Updates** tab. To specify the **No Schedule** option, continue with [Step 3](#).
 - ♦ **Recurring:** You can specify how often you want to download updates. After an update is checked, the information displayed in the **Available System Updates** panel on the **System Updates** tab, you can schedule the download from Micro Focus to automatically occur when the schedule starts. To set a recurring schedule, skip to [Step 4](#).
- 3 (Conditional) To exclude scheduled downloading of software updates, click the down-arrow in the **Schedule Type** field, select **No Schedule**, click **Apply** to save the schedule change, and then skip to [Step 6](#).

If you select this option, then you must download updates manually. For more information, see [Section 2.2, “Downloading Updates,” on page 24](#).
 - 4 (Conditional) To set a recurring schedule for downloading updates to your ZENworks software, click the down-arrow in the **Schedule Type** field, and then select **Recurring**.
 - 5 Fill in the fields:
 - 5a Select one or more check boxes for the days of the week.
 - 5b To set the time of day for downloading to occur, use the **Start Time** field to specify the time.
 - 5c (Optional) For additional scheduling options, click **More Options**, then select the following options as necessary:
 - ♦ **Process Immediately if Device Unable to Execute on Schedule:** Checks for updates to occur as soon as possible if the checking cannot be done according to schedule. For example, if a server is down at the scheduled time, checking for updates occurs immediately after the server comes back online.
 - ♦ **Use Coordinated Universal Time:** Schedules to interpret the times you specify as UTC instead of local time.

- ♦ **Start at a Random Time Between Start and End Times:** Allows downloading of updates to occur at a random time between the time you specify here and the time you specified in [Step 5b](#). Fill in the **End Time** fields.
- ♦ **Restrict Schedule Execution to the Following Date Range:** In addition to the other options, you can specify the days when downloading should occur.

5d When you have finished configuring the recurring schedule, click **Apply** to save the schedule change.

6 To exit this page, click **OK** when you are finished configuring the schedule.

Click **OK** to save and apply your changes. Click **Cancel** to close the page, but your unapplied changes will be discarded.

1.1.4 Email Notification

In conjunction with [using stages](#), you can set up email notifications to indicate when each stage has completed. When you deploy an update, you can specify to use the email notifications.

- 1** In ZENworks Control Center, click **Configuration** in the left pane, and then click the **Configuration** tab.
- 2** Click **Management Zone Settings** to expand its options, click **Event and Messaging**, then select **Notification Servers** to display the **Email Notification** panel.

Staging must be used to receive notifications, and the stage behavior must be set to one of the following:

- ♦ **Advance Through Stage Automatically With Notification**
- ♦ **Advance To Next Stage and Notify When Complete**

SMTP must be configured in order for the staging email configuration to work.

3 (Conditional) If you do not have SMTP configured:

3a To access the SMTP Settings page, click **Configuration** in the left pane, click the arrows in the **Management Zone Settings** heading to expand its options, click **Event and Messaging**, and then select **Notification Servers**.

3b In the **email Notification** section, fill in the fields:

SMTP Server Address: Specify the DNS name or IP address of the SMTP server.

SMTP Port: Specify the SMTP server's communication port.

SMTP Server Requires Authentication: If authentication is required, select this check box, then specify the **User** and **Password**.

3c Click **OK** to save the changes.

3d Click **Management Zone Settings** to expand its options, click **Infrastructure Management**, and then select **System Update Settings** to display the **Email Notification** panel.

4 Fill in the fields:

From: Either specify your administrator email address, or type something descriptive, such as `System-Update-Stage-Notice`. Do not use spaces between words.

To: Specify your administrator email address. You can specify multiple email addresses separated by a comma (,).

This is the person you want to be notified when the stage ends.

- 5 Click **Apply** to make the changes effective.
- 6 Either click **OK** to close the page, or continue with [another configuration task](#).
Click **OK** to save and apply your changes. Click **Cancel** to close the page, but your unapplied changes will be discarded.

1.1.5 Proxy Server Settings

This option is useful for restrictive environments where you do not want all of your production servers to have Internet access. This is used in conjunction with the [Dedicated Server Settings](#) panel.

To specify a proxy server:

- 1 In ZENworks Control Center, click **Configuration** in the left pane.
- 2 On the **Configuration** tab, expand the **Management Zone Settings** section (if necessary), click **Infrastructure Management**, then click **System Update Settings** to display the **Proxy Server Settings** panel.
- 3 Fill in the fields:
Proxy Server Address: Specify the DNS name or IP address of the proxy server.
Proxy Server Port: Specify the proxy server's communication port.
Proxy Server Requires Authentication: When you select this check box, the **User** and **Password** fields become editable. If authentication is required, select this check box and specify the username and password for accessing the proxy server.
- 4 Click **Apply** to make the changes effective.
- 5 Either click **OK** to close the page, or continue with [another configuration task](#).
Click **OK** to save and apply your changes. Click **Cancel** to close the page, but your unapplied changes will be discarded.

1.1.6 Dedicated Server Settings

By default, any available Primary Server in the Management Zone can be used randomly to download the updates. However, you can specify one ZENworks Server to be dedicated to handling your update downloads. The server that you select should have access to the Internet, directly or through a [proxy server](#). The zone-wide pre-install actions will run on the dedicated system update server.

The following sections contain more information:

- ♦ [“Specifying a Dedicated Update Server” on page 12](#)
- ♦ [“Clearing a Dedicated Update Server” on page 13](#)

Specifying a Dedicated Update Server

- 1 In ZENworks Control Center, click **Configuration** in the left pane.
- 2 On the **Configuration** tab, expand the **Management Zone Settings** section (if necessary), click **Infrastructure Management**, then click **System Update Settings** to display the Dedicated Server Settings panel.
- 3 Browse for and select a ZENworks Primary Server.

The server's identification is displayed in the **Dedicated System Update Server** field.


This ZENworks Server must be a member of the Management Zone.

- 4 Click **Apply** to make the changes effective.
- 5 Either click **OK** to close the page, or continue with [another configuration task](#).

If you did not click **Apply** to make your changes effective, clicking **OK** does so. Clicking **Cancel** also closes the page, but loses your unapplied changes.

Clearing a Dedicated Update Server

Clearing a dedicated update server causes your updates to be retrieved randomly from any Primary Server in the Management Zone.

- 1 In ZENworks Control Center, click **Configuration** in the left pane.
- 2 On the **Configuration** tab, expand the **Management Zone Settings** section (if necessary), click **Infrastructure Management**, then click **System Update Settings** to display the Dedicated Server Settings panel.
- 3 Click  to remove the dedicated server from the **Dedicated System Update Server** field.
- 4 (Conditional) If you need to revert to the last saved dedicated server setting, click **Reset**.
This resets the dedicated server to the last saved setting, such as when you last clicked **Apply** or **OK**.
- 5 Click **Apply** to make the change effective.

IMPORTANT: Previous settings cannot be restored after you click **Apply**.

1.1.7 Stage Timeout Settings

Deployment stages are optional; however, stages allow you to deploy an update one step at a time, such as to a test group first, then to your managed devices. If a failure occurs during the update process, the process is halted. [Email notifications](#) can let you know when each stage has completed.

The global default timeout setting is 3 days. This provides the same timeout length for each stage. For information about setting the timeout for individual stages, see [“Modifying the Stage Timeout” on page 18](#).

Set this value to be long enough to accommodate updating all of the devices you plan to update.

When the timeout value is reached, the stage's deployment stops and an email message is sent, if email notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).

You can use [email notification](#) to know when a stage has completed.

To configure global stage timeout settings:

- 1 In ZENworks Control Center, click **Configuration** in the left pane.
- 2 On the **Configuration** tab, expand the **Management Zone Settings** panel (if necessary), click **Infrastructure Management**, then click **System Update Settings** to display the Stage Timeout Settings panel.
- 3 Select the **Stage Timeout** check box, then specify the days, hours, and minutes desired.
- 4 Click **Apply** to make the changes effective.
- 5 Either click **OK** to close the page, or continue with [another configuration task](#).

If you did not click **Apply** to make your changes effective, clicking **OK** does so. Clicking **Cancel** also closes the page, but loses your unapplied changes.

1.1.8 Reboot Behavior

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

To configure the reboot behavior:

- 1 In ZENworks Control Center, click **Configuration** in the left pane.
- 2 On the **Configuration** tab, expand the **Management Zone Settings** panel (if necessary), click **Infrastructure Management**, then click **System Update Settings** to display the Reboot Behavior panel:
- 3 Select one of the following options:
 - ♦ **Prompt User to Reboot When Update Finishes Applying:** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.
 - ♦ **Reboot device when no user is logged into the system:** Select this option to reboot the device even if no user has logged into the system.
 - ♦ **Reboot device when the device is locked (only on Windows 8.1 and earlier):** Select this option to reboot the device if the device is locked. Prompt will not be displayed before rebooting the device.

The above options are applicable on agents only when they are upgraded to ZENworks Update 2 or later version.

- ♦ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.
 - ♦ **Start ZENworks Agent with limited functionality:** Select this option to start ZENworks services incase reboot is suppressed while deploying the update to the device. It is not applicable for Primary Servers. For information about Reboot-less Agent, see [section Reboot-less Agent](#) in the *ZENworks Discovery, Deployment, and Retirement Reference*.
 - ♦ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention if a reboot is required by the update.
- 4 Click **Apply** to make the changes effective.

- 5 Either click **OK** to close the page, or continue with [another configuration task](#).

If you did not click **Apply** to make some of your changes effective, clicking **OK** does so. Clicking **Cancel** also closes the page, but loses your unapplied changes.

1.2 Creating Deployment Stages

Deployment stages are optional; however, stages allow you to deploy an update one step at a time, such as to a test group first, then to your managed devices. [If a failure occurs during the update process, the process is halted. Email notifications](#) can let you know when each stage has completed.

The following sections contain more information:

- ♦ [Section 1.2.1, “Understanding Stages,” on page 15](#)
- ♦ [Section 1.2.2, “Creating and Populating a Deployment Stage,” on page 17](#)
- ♦ [Section 1.2.3, “Modifying the Stage Timeout,” on page 18](#)
- ♦ [Section 1.2.4, “Modifying Staging Behavior,” on page 19](#)
- ♦ [Section 1.2.5, “Modifying Reboot Behavior,” on page 20](#)
- ♦ [Section 1.2.6, “Modifying the Membership of a Deployment Stage,” on page 20](#)
- ♦ [Section 1.2.7, “Renaming a Deployment Stage,” on page 21](#)
- ♦ [Section 1.2.8, “Deleting a Deployment Stage,” on page 21](#)
- ♦ [Section 1.2.9, “Rearranging the Staging Order,” on page 21](#)

1.2.1 Understanding Stages

You can do the following with stages:

- ♦ Set them up for different devices or groups, such as for a test group, specific devices or device groups, or all managed devices in the zone.
- ♦ Modify an existing stage’s membership.
- ♦ Change the order in which the stages run.
- ♦ Rename and delete stages.
- ♦ Specify the default timeout for a stage. When the timeout value is reached, the stage’s deployment stops and an email message is sent, if email notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).
- ♦ Specify the reboot behavior when devices complete the update: prompt a reboot, force a reboot, or suppress rebooting.
- ♦ Specify how the update process is to advance through the stages:
 - ♦ Automatically, with or without notification
 - ♦ One stage at a time with notification when each stage is completed
 - ♦ Bypass the configured stages and immediately apply the update to all devices

There are many reasons for creating deployment stages:

- ♦ Testing the update on certain devices before deploying it to your production environment
- ♦ Including all Primary Servers in one stage so they can be updated at the same time.
- ♦ Grouping your servers in several stages so that the update process isn't too intensive for the Primary Server being used to perform the updates.
- ♦ Grouping the workstations in several stages so that the update process isn't too intensive for the Primary Server being used to perform the updates.

Any managed devices that are not part of a stage are automatically updated after the last deployment stage has been processed.

You cannot configure stages when an update is in progress.

NOTE: Actions on this page are available only to administrators with the following rights:

- ♦ Deploy Update rights
 - ♦ View Leaf rights
-

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Table 1-1 *Deployment Stages column descriptions.*

Column Heading	Explanation
Ordinal	<p>Displays the order in which the stages run. You can rearrange the staging order by using the Move Up and Move Down options. For more information, see “Rearranging the Staging Order” on page 21.</p> <p>The first stage listed always displays ordinal 1, the second, ordinal 2, and so on. Therefore, you do not need to include a sequence number in your stage names.</p>
Stage Name	<p>Name of the stage, which you specify when creating the stage by using the Action > Add Stage option.</p> <p>Make this name descriptive enough to indicate its purpose.</p>
Stage Members	<p>This column contains the View/Modify Members option, which opens the Modify Stage Members dialog box that lists all of the members of the stage. You can use the dialog box to add or remove members from the stage.</p> <p>Stage membership can include individual devices and groups that contain devices.</p> <p>For more information, see “Modifying the Membership of a Deployment Stage” on page 20.</p>
Staging Behavior	<p>Displays the current behavior for each stage, which you can change by using the Action > Modify Staging Behavior option. For more information, see “Modifying Staging Behavior” on page 19.</p>

Column Heading	Explanation
Reboot Behavior	<p>Displays the reboot behavior of devices after the update is deployed.</p> <p>Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.</p> <p>You have the following reboot options:</p> <ul style="list-style-type: none"> ♦ Prompt User to Reboot When Update Finishes Applying: After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted. <ul style="list-style-type: none"> ♦ Reboot device when no user is logged into the system: Select this option to reboot the device even if no user has logged into the system. ♦ Reboot device when the device is locked (only on Windows 8.1 and earlier): Select this option to reboot the device if the device is locked. Prompt will not be displayed before rebooting the device. <p>The above options are applicable on agents only when they are upgraded to ZENworks Update 2 or later version.</p> <ul style="list-style-type: none"> ♦ Do Not Reboot Device: The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted. <ul style="list-style-type: none"> ♦ Start ZENworks Agent with limited functionality: Select this option to start ZENworks services incase reboot is suppressed while deploying the update to the device. It is not applicable for Primary Servers. For information about Reboot-less Agent, see section “Reboot-less Agent” in the ZENworks Discovery, Deployment, and Retirement Reference. ♦ Force Device to Reboot: After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update. <p>For more information, see “Modifying Reboot Behavior” on page 20.</p>
Stage Timeout	<p>Displays the stage timeout, which you can change by using the Action > Modify Stage Timeout option. The default is 3 days, 0 hours, and 0 minutes, which is the global timeout value that can be changed in “Stage Timeout Settings” on page 13. Changing the value here only changes it for the selected deployment stage.</p> <p>When the timeout value is reached, the stage’s deployment stops and an email message is sent, if email notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).</p> <p>For more information, see “Modifying the Stage Timeout” on page 18.</p>

1.2.2 Creating and Populating a Deployment Stage

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deployment Stages panel, click **Action**, then select **Add Stage**.

You cannot add a stage while a deployment is in process.

- 3 Specify a deployment stage name, then click **OK**.

Deployment stages appear as device folders on the **Devices** tab, so you should specify names that help you to know a folder's purpose.

You might want to include something like "Deployment Stage" at the beginning of the name to sort the groups in the devices listing in ZENworks Control Center.

For information about naming in ZENworks Control Center, see "[Naming Conventions in ZENworks Control Center](#)" in the *ZENworks Control Center Reference*.

A newly created stage does not have any members. You must modify the stage's membership to add them.

- 4 Add devices to a deployment stage:

- 4a In the **Stage Members** column, click **View/Modify Members** for the stage for which you want to add members.

- 4b Click **Add**, browse for and select the devices, then click **OK**.

You can add individual devices or device groups, or any combination of them.

You can have both managed servers and workstations in the same deployment stage or in different stages, or you can split your servers and workstations into separate deployment stages.

IMPORTANT: Some of your network servers will be Primary Servers for use in ZENworks management, while other servers on your network might only be managed devices with the ZENworks Agent installed on them.

You must update your Primary Servers before updating any of the other managed servers and especially before updating any managed workstations.

- 4c Repeat [Step 4b](#) until you are finished adding members to the stage.

- 4d To add members to another stage, repeat [Step 4a](#) through [Step 4c](#).

- 5 Repeat [Step 2](#) through [Step 4](#) until you have created all of your deployment stages.

- 6 If you need to reorder the sequence of the deployment stages, select a stage, then click **Move Up** or **Move Down**.

If you are using one of the stages for test purposes, make sure that it is first in the listing.

1.2.3 Modifying the Stage Timeout

A stage timeout sets the length of time before a stage terminates. The default timeout is 3 days. You set the value for individual stage timeouts by using the procedure in this section. The global stage timeout value is established by following the steps in "[Stage Timeout Settings](#)" on page 13.

You cannot modify a stage if an update is in progress.

To set the timeout value for a selected stage:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deployment Stages panel, select the check box for a stage, click **Action**, then select **Modify Stage Timeout**.

- 3 Specify the timeout value.

This change in timeout value only applies to the selected stage. If you specify a timeout value for this stage, set its value to be long enough to accommodate updating all of the devices in the stage.

When the timeout value is reached, the stage's deployment stops and an email message is sent, if email notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).

- 4 (Optional) Select the **Use Global Stage Timeout Setting for All Stages** check box to specify using the global timeout value (default of 3 days, 0 hours, and 0 minutes).

For more information, see ["Stage Timeout Settings" on page 13](#).

- 5 Click **OK**.

1.2.4 Modifying Staging Behavior

The default stage behavior is to automatically advance through the configured stages. You can change this default behavior. If you change the staging behavior for one stage, the change becomes effective for all stages.

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deployment Stages panel, select the check box next to any stage, click **Action**, then select **Modify Stage Behavior**.
- 3 Select one of the following stage behaviors:

Advance Through Stages Automatically: As soon as one stage has completed its updates, the next stage begins. This is the default behavior (its check box is enabled).

After the last stage has completed, all applicable devices that are not members of a stage are then processed.

Advance Through Stages Automatically with Notification: Starts the first stage, sends an email notification when it has completed, then automatically starts the next stage, and so on.

To use this option, a notification method must be set up on the [System Update Download Settings page](#) in the **email Notification** section.

Advance to Next Stage Manually and Notify When Complete: Use this method for user action between the stages, such as reviewing the results of an update to a test group.

This option automatically starts the first stage. After any stage has completed, email notification is sent, then the system waits for you to manually start the next stage.

To use this option, a notification method must be set up on the [System Update Download Settings page](#) in the **email Notification** section.

- 4 Click **OK**.

1.2.5 Modifying Reboot Behavior

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

To modify the reboot behavior:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deployment Stages panel, select the check box for one or more the deployment stages, click **Action**, then click **Modify Reboot Behavior**.
- 3 Select one of the following options:
 - ♦ **Prompt User to Reboot When Update Finishes Applying:** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.
 - ♦ **Reboot device when no user is logged into the system:** Select this option to reboot the device even if no user has logged into the system.
 - ♦ **Reboot device when the device is locked (only on Windows 8.1 and earlier):** Select this option to reboot the device if the device is locked. Prompt will not be displayed before rebooting the device.
 - The above options are applicable on agents only when they are upgraded to ZENworks Update 2 or later version.
 - ♦ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.
 - ♦ **Start ZENworks Agent with limited functionality:** Select this option to start ZENworks services incase reboot is suppressed while deploying the update to the device. It is not applicable for Primary Servers. For information about Reboot-less Agent, see section “[Reboot-less Agent](#)” in the *[ZENworks Discovery, Deployment, and Retirement Reference](#)*.
 - ♦ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.
- 4 Click **OK**.

1.2.6 Modifying the Membership of a Deployment Stage

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 (Optional) Add devices to a deployment stage:
 - 2a In the **Stage Members** column, click **View/Modify Members** for the stage for which you want to add members.
 - 2b Click **Add**, browse for and select the devices, then click **OK**.

You can add individual devices or device groups, or any combination of them.

You can have both managed servers and workstations in the same deployment stage or in different stages, or you can split your servers and workstations into separate deployment stages.

IMPORTANT: Some of your network servers will be Primary Servers for use in ZENworks management, while other servers on your network might only be managed devices with the ZENworks Agent installed on them.

You must update your Primary Servers before updating any of the other managed servers and especially before updating any managed workstations.

- 2c Repeat [Step 2b](#) until you are finished adding members to the stage.
- 2d To add members to another stage, repeat [Step 2a](#) through [Step 2c](#).
- 3 (Optional) Remove devices from a deployment stage:
 - 3a In the **Stage Members** column, click **View/Modify Members** for the stage for which you want to remove members.
 - 3b Select the check box next one or more devices that you want to remove, then click **Remove**.
- 4 Click **OK** when you have finished configuring the stage's membership.

1.2.7 Renaming a Deployment Stage

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deployment Stages panel, click the check box for the deployment stage to be renamed.
- 3 Click **Rename**.
- 4 In the Rename dialog box, specify the new name, then click **OK**.

For information about naming in ZENworks Control Center, see "[Naming Conventions in ZENworks Control Center](#)" in the *ZENworks Control Center Reference*.

1.2.8 Deleting a Deployment Stage

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deployment Stages panel, click the check box for one or more of the deployment stages to be deleted.
- 3 Click **Delete**.

Deleted stages cannot be recovered.

1.2.9 Rearranging the Staging Order

All updates that use stages deploy to the devices that are members of the stages according to the currently listed staging order.

To rearrange the staging order:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deployment Stages panel, click the check box for the deployment stage to be moved.

- 3 Click **Move Up** or **Move Down** as necessary to rearrange the staging order.
- 4 Repeat [Step 2](#) and [Step 3](#) as necessary for each stage.

2 Managing Update Downloads

The Available System Updates panel on the System Updates page displays the updates that are available after you have checked for them. This includes the Product Recognition Update (PRU), which Micro Focus provides to update your knowledge base so that ZENworks Inventory can recognize newer software. The display refreshed according to the schedule you set in [“Check for Updates Schedule” on page 8](#).

The following sections contain more information:

- [Section 2.1, “Understanding Available Updates,” on page 23](#)
- [Section 2.2, “Downloading Updates,” on page 24](#)
- [Section 2.3, “Downloading and Installing the PRU,” on page 27](#)
- [Section 2.4, “PRU Schedule,” on page 28](#)
- [Section 2.5, “Canceling or Deleting a System Update,” on page 31](#)
- [Section 2.6, “Preparing an Update,” on page 31](#)
- [Section 2.7, “Retry Prepare Update,” on page 32](#)
- [Section 2.8, “Authorizing an Update,” on page 33](#)
- [Section 2.9, “Configuring an Update,” on page 33](#)

2.1 Understanding Available Updates

The following table explains the column information and the **Auto Refresh** drop-down list (on the right side of the panel, above **Target Type**). For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Table 2-1 Available System Updates column descriptions.

Column Heading or List	Explanation
Update Name	Displays the name of the update, which is created by Micro Focus. Click the name to access the Release Details page. For more information, see Chapter 5, “Reviewing the Content of an Update,” on page 59 .
Release Date	Displays the date that Micro Focus created the update.
Download Date	Displays the date that you downloaded the update.
Applied Date	Displays the date that you first applied the update.

Column Heading or List	Explanation
Status	Displays the current status of the update, which is automatically updated every 15 seconds. For more information on the individual statuses, see Chapter 6, “Update Statuses,” on page 63.
Importance	Displays the relative importance of the update’s content to your ZENworks installation. Some possible entries include: OPTIONAL: Not required for normal operation of ZENworks. MANDATORY: A required update that must be applied.
Target Type	Displays the type of update, such as: ZENworks Servers: The update applies only to ZENworks Servers. All Devices: The update applies to all managed devices, including ZENworks Servers.
Auto Refresh	Click Auto Refresh (the menu item on the right side of the panel, above Target Type), then select one of the following: <ul style="list-style-type: none"> ◆ No Auto Refresh ◆ 15-second Refresh ◆ 30-second Refresh ◆ 60-second Refresh <p>By default the panel view is not automatically refreshed. However, you can manually refresh the view by clicking the System Updates tab.</p>
View Status	Click View Status to view the system update progress of this server.

2.2 Downloading Updates

You can schedule the downloads, or download them manually:

- ◆ [Section 2.2.1, “Scheduling Update Downloads,”](#) on page 24
- ◆ [Section 2.2.2, “Manually Checking for Updates,”](#) on page 25
- ◆ [Section 2.2.3, “Manually Download Updates,”](#) on page 25
- ◆ [Section 2.2.4, “Manually Importing Updates to Servers without Internet Connectivity,”](#) on page 27

2.2.1 Scheduling Update Downloads

You can schedule both checking for updates and downloading them:

- ◆ [“Check for Updates Schedule”](#) on page 8
- ◆ [“Download Schedule”](#) on page 10

2.2.2 Manually Checking for Updates

If the most recent updates are not being displayed in the Available System Updates panel on the System Updates page, you can manually refresh the display.

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Available System Updates panel, click **Action > Check for Updates**.
Any available updates are displayed with a status of **Available**.
- 3 To re-sort the listed updates, click the heading for any of the columns in the Available System Updates panel.
Click the heading a second time to reverse the sorting order.

2.2.3 Manually Download Updates

Download system update files in one of the following ways:

- ♦ “From Software and Licenses Download (SLD)” on page 25
- ♦ “From ZENworks Control Center” on page 26

From Software and Licenses Download (SLD)

Log in to the [Micro Focus Customer Portal](#) site to download the files for update. From the **Downloads** screen, select the **Product**, **Product Name** (entitlement) and **Version** to view the files. Click the **Media Version** column and select the **ZENworks 23.4** release option, and then click **Download Selected**.

Software Downloads

Account Name:

Product:

ZENworks Configuration Management (ZCM) ▼

Product Name:

ZENworks Configuration Management per Department Workstation Academic Sub SW E-LTU ▼

Version:

23.4 ▼

Export Media Report

Download Selected

☐ Show Superseded Patches

Get Licenses

i By downloading the software below, you agree, on behalf of or as the licensee of such software, that you have read and hereby accept that, unless otherwise agreed in writing by OpenText, the End User License Agreement and any associated Additional License Authorizations located [here](#), for such software shall apply and supersede different license terms that may be embedded within such software.

<input type="checkbox"/>	Description	Category	Platform	Language	File Type	Media Version	Created Date	Action
<input type="checkbox"/>	ZENworksDiagnosticCenter_23.4.zip	ZENworks 23.4	All	English	Software	23.4	2023-11-07	More Details <input type="button" value="Q"/> Download
<input type="checkbox"/>	ZENworks_23.4_Update.zip	ZENworks 23.4			Software	23.4	2023-11-07	More Details <input type="button" value="Q"/> Download
<input type="checkbox"/>	ZENworks2020_Update2.iso	ZENworks 23.4	Software	23.4	2023-11-07	More Details <input type="button" value="Q"/> Download
<input type="checkbox"/>	ZENworks2020_Update2_Appliance-x86_64.vhdx.zip	ZENworks 23.4	Software	23.4	2023-11-07	More Details <input type="button" value="Q"/> Download

Downloads

Select the following files and click **Download Selected**.

File Type	File Name
System update ZIP file	ZENworks_23.4_Update.zip
ZENworks Diagnostic Center for validity	ZENworksDiagnosticCenter23.4.zip

Perform MD5 checksum on all downloaded files for data integrity.

After downloading the System update ZIP file, perform the following steps:

1. (Optional) Create a temporary directory on Windows and Linux. On Linux, create the directory in `/var/tmp` or `/var/opt/microfocus/zenworks/common/tmp`.
2. Copy the System update ZIP file to the temporary directory.
3. Run the following command:

```
zman sui <Path of the system update zip file>
```
4. When prompted, specify the administrator credentials.

The system update will be imported to the zone. To track the status in ZCC, go to Configuration > System Updates.

Next, follow the update deployment steps. For information on deploying the update, see [step 6 in Deploying Updates](#).
5. In ZCC, after the system update is downloaded completely, the System update ZIP file can be deleted from the temporary directory.

ZENworks 23.4 Licensing

You need to enable/ activate System update entitlement in ZCC before able to view 23.4 in ZCC. For more information, see [“System Update Entitlement” on page 7](#).

You can manually download the updated SU zip from SLD. For more information, see [Section 2.2, “Downloading Updates,” on page 24](#).

NOTE: You need not have to fetch or activate new product licenses if already activated at 20.2 version.

If not licensed for ZENworks 2020 Suite, then all individual ZENworks component licenses will need to be entered separately during update.

From ZENworks Control Center

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Available System Updates panel, select the check box next to ZENworks 23.4, click **Action**, then click **Download Update**.

The update is downloaded to the zone and preparing of the update is performed.

Depending on the size of the update, the downloading process can take some time.

- 3 To refresh the view of the download progress (**Status** column), click the **System Updates** tab or use the **Auto Refresh** option.

After the system update is downloaded, the Preparing stage will be automatically initiated.

For more information, see [“Preparing an Update” on page 31](#)

2.2.4 Manually Importing Updates to Servers without Internet Connectivity

If you have servers in your environment that do not have Internet access, you can obtain the update or Product Recognition Update (PRU) files from the [Micro Focus Downloads page](#), copy the files onto a CD or other media, and then use the CD to import the files to a ZENworks Primary Server by using the `zman system-update-import` command. For more information, see [“System Update/Product Recognition Update Commands”](#) in the [ZENworks Command Line Utilities](#).

After the system update is downloaded, the Preparing stage will be automatically initiated. For more information on Preparing stage, see [“Preparing an Update” on page 31](#)

After the files are on a ZENworks Primary Server, the update or PRU displays in the Available System Updates panel on the **System Updates** tab in ZENworks Control Center (**Configuration > System Updates**). You can then follow the instructions in [Chapter 3, “Deploying Updates,” on page 35](#) to deploy the update to managed devices.

2.3 Downloading and Installing the PRU

ZENworks provides a Product Recognition Update (PRU) to update your knowledge-base so that ZENworks Inventory can recognize newer software.

This action deploys the PRU to your database and sets its deployment to your managed devices to be scheduled. Deployment is then done by the ZENworks Agent on the devices.

If the PRU is not up-to-date, Inventory might return some software as unrecognized. However, you can use the [Local Software Products](#) utility to take a fingerprint of the unrecognized software to update your knowledgebase.

To download and install the PRU:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 If a PRU is not displayed in the Available System Updates panel, click **Action > Check for Updates**. Information for the latest PRU is displayed, if it is available.
- 3 To download a listed PRU, go to the Available System Updates panel, select the check box for a listed PRU, then click **Action > Download Update**.
- 4 To install a downloaded PRU, go to the Available System Updates panel, then click **Action > Deploy PRU Now**.

The PRU is now listed in the panel, where its progress is displayed.

After the system update is downloaded, the Preparing stage will be automatically initiated. For more information on Preparing stage, see [“Preparing an Update” on page 31](#).

You can automate the PRU process (Availability check, Download and Deployment) by scheduling the PRU. For more information, see [PRU Schedule](#).

NOTE: The PRU content is replicated only on Primary Servers. Hence, Content Replication status is not displayed for Satellite Servers.

2.4 PRU Schedule

This page enables you to configure a schedule to check for PRU availability, PRU download and PRU deployment. You can also configure email notifications to inform other users or administrators about the PRU status.

All the PRU schedule tasks will be performed on the dedicated System Update server. If the dedicated System Update server is not configured, then the tasks will be performed on the first Primary Server.

To configure PRU schedule:

1. In ZCC, click **Configuration**.
2. In **Management Zone Settings**, click **Inventory**.
3. In the **Inventory** panel, click **PRU Schedule** and configure any of the following PRU schedules:
 - ♦ [Section 2.4.1, “PRU Availability Check Schedule,” on page 28](#)
 - ♦ [Section 2.4.2, “PRU Download Schedule,” on page 29](#)
 - ♦ [Section 2.4.3, “PRU Deployment Schedule,” on page 30](#)
 - ♦ [Section 2.4.4, “Email Notification,” on page 30](#)

2.4.1 PRU Availability Check Schedule

In this section, you can configure a schedule to perform PRU availability check. A mail will be sent to the recipients whenever a new PRU is available. To configure the email notifications, see [Email Notifications](#).

1. Select a schedule type:
 - a. **No Schedule:** To perform the availability check manually.
 - b. **Recurring:** To perform the PRU availability check on a certain day of the month, last day of the month or at a fixed day of the month. The following options are displayed:
 - i. Specify the day on which the PRU check should be performed by using one of the following options:
 - ♦ **Day of the month:** To select a particular day of the month in numeric format. For example, specify 1 for the first day of the month.
 - ♦ **Last day of the month:** To schedule PRU availability check on the last day of the month.

- ♦ **Configurable field:** To select a particular instance of a specific day in the month. For example, First Friday of the month. To add additional dates, click “+”.
 - ii. Specify the Start Time for the PRU availability check.
 - iii. Click More Options.
 - iv. Select the additional options based on your requirements:
 - ♦ To immediately run the PRU Availability check when the device fails to execute it as per the defined schedule, select Process immediately if device unable to execute on schedule.
 - ♦ To define a standard time, select Use Coordinated Universal Time (UTC).
 - ♦ To perform the check at any time between the start and end times, select Start at a random time between Start Time and End Time, and specify the End Time.
 - ♦ To run the check between a particular date ranges, select Restrict schedule execution to the following date range, and specify the start and end dates.
2. Click Apply or OK.

2.4.2 PRU Download Schedule

In this section, you can configure a schedule to download the available PRU. A mail will be sent to the recipients whenever the PRU is downloaded.

1. Select a schedule type:
 - a. **No Schedule:** To manually download the PRU.
 - b. **Recurring :** To download the PRU on a certain day of the month, last day of the month or at a fixed day of the month. The following options are displayed:
 - i. Specify the day on which the PRU should be downloaded by using one of the following options:
 - ♦ **Day of the month:** To select a particular day of the month in numeric format. For example, specify 1 for the first day of the month.
 - ♦ **Last day of the month:** To download PRU on the last day of the month.
 - ♦ **Configurable field:** To select a particular instance of a specific day in the month. For example, First Friday of the month. To add additional dates, click “+”.
 - ii. Specify the Start Time to download the PRU.
 - iii. Click **More Options**.
 - iv. Select the additional options based on your requirements:
 - ♦ To immediately download the PRU when the device fails to execute it as per the defined schedule, select Process immediately if device unable to execute on schedule.
 - ♦ To define a standard time, select Use Coordinated Universal Time (UTC).
 - ♦ To download PRU at any time between the start and end times, select Start at a random time between Start Time and End Time, and specify the End Time.
 - ♦ To download the PRU between a particular date ranges, select Restrict schedule execution to the following date range, and specify the start and end dates.
2. Click **Apply** or **OK**.

2.4.3 PRU Deployment Schedule

In this section, you can configure a schedule to deploy the PRU. A mail will be sent to the recipients whenever the PRU is deployed.

1. Select a schedule type:
 - a. **No Schedule:** To manually deploy the PRU.
 - b. **Recurring:** To deploy the PRU on a certain day of the month, last day of the month or at a fixed day of the month. The following options are displayed:
 - i. Specify the day on which the PRU should be deployed by using one of the following options:
 - ♦ **Day of the month:** To select a particular day of the month in numeric format. For example, specify 1 for the first day of the month.
 - ♦ **Last day of the month:** To deploy PRU on the last day of the month.
 - ♦ **Configurable field:** To select a particular instance of a specific day in the month. For example, First Friday of the month. To add additional dates, click “+”.
 - ii. Specify the Start Time to deploy the PRU.
 - iii. Click **More Options**.
 - iv. Select the additional options based on your requirements:
 - ♦ To immediately deploy the PRU when the device fails to execute it as per the defined schedule, select Process immediately if device unable to execute on schedule.
 - ♦ To define a standard time, select Use Coordinated Universal Time (UTC).
 - ♦ To deploy PRU at any time between the start and end times, select Start at a random time between Start Time and End Time, and specify the End Time.
 - ♦ To deploy the PRU between a particular date ranges, select Restrict schedule execution to the following date range, and specify the start and end dates.
2. Click **Apply** or **OK**.

2.4.4 Email Notification

In this section, you can enable administrators to receive email notifications when a new PRU is available, downloaded or deployed. Before configuring the email notification settings, ensure that an SMTP server is configured to send and receive emails.

To enable the email notification:

- 1 Specify the email ID From which the email should be sent.
- 2 Specify the email IDs To whom the notifications should be sent when a new PRU is available, downloaded or deployed.
- 3 Select the events for which email notifications should be sent:
 - ♦ PRU availability check completed

- ♦ PRU downloaded
 - ♦ PRU deployed
- 4 Click **OK** or **Apply**

2.5 Canceling or Deleting a System Update

You can cancel the downloading of an update, or you can delete the update from the Available System Updates list.

To cancel an update:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 Select the check box for a system update that is being downloaded, then click **Action > Cancel Download**.

Cancelling an update cancels the downloading of an update. Files that are already downloaded are not automatically removed, but if you delete the update, any downloaded files are removed.

You can resume the download by clicking **Download Update**. The download will resume from where it was canceled.

If a server's connection to the ZENworks database is lost while downloading an update, the download does not resume after reconnecting. Attempting to use the **Cancel Download** action results in the update hanging in the Cancel state. Use the `zman sudo --force` command to delete the update.

To delete an update:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 Select the check box for the system update that you want to delete, then click **Action > Delete Update**.

Deleting an update removes it from the list and all downloaded files are removed. However, if the deleted update is still available on the update server the next time that you check for updates, it is displayed in the list again for possible downloading.
- 3 Click **OK** to confirm the deletion.

2.6 Preparing an Update

In the preparing stage, the prerequisites check and system update preparation is performed on all the Primary Servers. Click the **Preparing** link to view the preparation status.

The preparing includes following stages:

- ♦ **Replicating Content:** In this stage, latest System Update files are replicated to the local content repository.
- ♦ **Deploying Web Applications:** In this stage, each update is embedded with web applications, which assist administrators in configuring and monitoring the update.

- ♦ **Upgrading ZENworks Updater Service:** In this stage, the ZENworks Updater Service on all the primary Servers will be replaced with the new package that is included in the update.
- ♦ **Persisting Update Commands:** This stage saves further information on each update, such as dependencies and identifiers in the local file system, and it updates the updates-prepared file with the latest GUID information.
- ♦ **Finalizing Preparation:** In this stage, list of update commands that are executed on each Primary Servers are fetched from the database and saved in the local file system.

NOTE: If an error occurs during any stage, the system will retry preparing after a few minutes.

If any server fails during preparing stage, you can ignore that server and continue with the system update. To ignore a server, select the server and click **Ignore Device**. It is recommended to resolve the issue, and then continue with the system update.

If you want to deploy the system update, you should authorize and configure the update, and only then you will be able to deploy the updates.

You can deploy the system update through deployment stages or by select the devices. For more information, see [Chapter 3, “Deploying Updates,” on page 35](#).

If the download of the system update does not complete successfully, click the **Error** link and perform the required steps based on the displayed message. Files that are already downloaded are not automatically removed. The download will resume from where it went into the **Error** state.

2.7 Retry Prepare Update

If the prepare update stage has failed on any server, then you can retry the prepare update.

To retry prepare update:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 Select the check box for the system update that you to perform retry prepare update.
- 3 Click **Action > Retry Prepare Update**.

NOTE: During retry prepare update, the previously ignored servers will also be considered for preparing the update.

2.8 Authorizing an Update

You can authorize any downloaded update before configuring it. The deploy options are available only if the updates are configured and authorized.

To authorize an update:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 Select the check box for the system update that you want to authorize.
- 3 Click **Action > Authorize Update**.

2.9 Configuring an Update

After the system update is prepared, it should be configured before deploying. During configuring the system update, ZENworks collects information that is required for the update.

To enhance the system security, from ZENworks Update 3 onwards, the ZENworks Server service is split into two separate instances, ZENworks Client Management, and ZENworks Administration Management.

The new ZENworks Administration Management instance will host all the administrative services including the ZENworks Control Center. For this, a new port (default port 7443) should be configured before deploying the system update. The specified port will be used to run all the administrative services across all the primary servers. This port will be opened in the server firewall when the system update is deployed on a primary server. The ZENworks Client Management services will continue to run on the existing port to ensure the continuity of managed device communication. The default port here is 443.

To configure a system update:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Available System Updates panel, select the check box next to an update, click **Action**, and then click **Download Updates**. For more information, see [Downloading Updates](#).
- 3 Select the check box next to an update, click **Action**, then click **Authorize Update**.
- 4 Select the check box next to the same update, click **Action**, then click **Configure Update**.
After clicking **Configure Update**, the System Update Configuration page is displayed.
- 5 On the System Update Configuration page, click **Next**.
- 6 Click **Finish**.

NOTE: It is recommended that you login to the ZCC using the host name.

IMPORTANT: While configuring the update, the following warning messages might be displayed:

- ♦ **Warning: The zone contains one or more SLES 12 or SLES 15 non-Appliance Primary Servers. For this system update, ensure that the 'libseccomp2' package is at 2.4.1-11.3.2 or later version.**

In this scenario, check the libseccomp2 package version on all the SLES 12.x and SLES 15.x Primary Servers in the zone and then perform the following:

- ♦ If the version is 2.4.1-11.3.2 or higher, then you can ignore the warning and deploy the update.
- ♦ If the version is lesser than 2.4.1-11.3.2, then ensure that you update the version to 2.4.1-11.3.2 or higher before deploying the system update.
- ♦ ***Warning: The zone contains managed devices running on operating systems that do not support strong ciphers for secure communication with ZENworks servers. By registering managed devices running on an operating system that requires weak and vulnerable ciphers to communicate with ZENworks servers, you are reducing the security provided by default, thereby exposing the system to increased security risks. By proceeding, you understand and agree to assume all associated risks and hold Open Text harmless for the same. The capability is provided "as is". For more information, see the [online documentation](#).***

This message is displayed because the zone contains legacy Windows devices as mentioned below, that require weak ciphers to be enabled to communicate with the ZENworks Primary Servers. To restore the strong ciphers configured by default, all such devices need to be deleted from the zone.

Following are the legacy Windows devices that are supported in backward compatibility mode:

- ♦ Windows 7 (all variants, including SP1)
- ♦ Windows Server 2012 (all variants, including R2)

NOTE: If weak ciphers are enabled in the zone, it does not block the system update. However, it is recommended that you disable the weak ciphers immediately after the system update. For more information, see [Disabling Weak Ciphers](#).

3 Deploying Updates

- ♦ [Section 3.1, “Update Prerequisites,” on page 35](#)
- ♦ [Section 3.2, “Understanding Deploying Updates,” on page 37](#)
- ♦ [Section 3.3, “Deploying Updates,” on page 41](#)
- ♦ [Section 3.4, “Starting a Pending Stage,” on page 46](#)
- ♦ [Section 3.5, “Rescheduling a Deployment,” on page 46](#)
- ♦ [Section 3.6, “Bypassing Staging,” on page 47](#)
- ♦ [Section 3.7, “Canceling a Deployment,” on page 47](#)
- ♦ [Section 3.8, “Clearing an Error to Retry a Deployment,” on page 48](#)
- ♦ [Section 3.9, “System Update Fails on the Device with an Error Code,” on page 48](#)
- ♦ [Section 3.10, “Viewing Status by Device,” on page 48](#)
- ♦ [Section 3.11, “Viewing the System Update Deployment Status,” on page 53](#)
- ♦ [Section 3.12, “Standalone Agent Updater,” on page 54](#)
- ♦ [Section 3.13, “Superseded Files,” on page 56](#)
- ♦ [Section 3.14, “Limitations of System Update,” on page 56](#)

3.1 Update Prerequisites

All the Primary Servers should be updated before you update the agents and the Satellite Servers in the zone. To ensure the proper functioning of ZENworks, it is recommended that all Primary Servers are updated in as short a time as possible - ideally, immediately after the first Primary Server is updated.

The administrator can always choose to update one of the Primary Servers and then the remaining Primary Servers. The Primary Server that is chosen to be updated first should be the server with the embedded database.

NOTE:

- ♦ The ZENworks Updater Service should be running to initiate an update on Primary Servers and Windows Agents.
 - ♦ The ZENworks Agent Service should be running to initiate an update on Linux Agents.
 - ♦ If the zone contains an embedded database, the server that is running in the database should be updated first.
 - ♦ Before updating the ZENworks Agent on managed devices, ensure that any reboots required from applying a policy are completed.
 - ♦ If the zone contains one or more SLES 12 or SLES 15 non-appliance primary servers, for the ZENworks 23.4 system update, ensure that the ‘libseccomp2’ package is at 2.4.1-11.3.2 or later version.
-

Vertica Prerequisite When updating a Vertica enabled zone to ZENworks 23.4, a new pre-requisite check is introduced to verify the Vertica version in the zone. If the version is lower than Vertica 23.3, then you need to upgrade to the latest version by using the Vertica Upgrade tool. For more information on the tool and how to run the tool, see [Upgrading Vertica](#) in the [ZENworks Vertica Guide](#).

Windows 10 Prerequisite: When updating the ZENworks Agent to ZENworks 2017 Update 1 on a Windows 10 device, you need to disable Client Self Defense and reboot the device before running the update. Self Defense can be re-enabled after the update. This prerequisite is not applicable when updating the ZENworks Agent from ZENworks 2017 Update 1 to a later version. For information about the Self Defense setting, see “[Configuring the Agent Security](#)” in the [ZENworks Discovery, Deployment, and Retirement Reference](#).

Full Disk Encryption Agent prerequisites: For information about Full Disk Encryption update prerequisites and other considerations for doing a system update on managed devices using Full Disk Encryption, see the [ZENworks - Full Disk Encryption Update Reference](#).

IMPORTANT: If you have enabled the ZENworks Patch Management in your zone, then ensure that you perform the following steps before updating to ZENworks 23.4:

1. Run the following query to identify the Patch policies that have DaysToRebuild set to 0:

```
SELECT * FROM zbundle
WHERE zuid IN (
  SELECT zuid
  FROM zzenobject
  WHERE path LIKE '%ZPM/Policy%'
  AND primarytype = 'Bundle'
  AND subtype LIKE '%Patch Bundle%'
  AND serversidedata LIKE '%xmlns:ns2="http://novell.com/zenworks/
datamodel/objects/settings">DaysToRebuild</ns2:Name><ns2:Value
xmlns="http://novell.com/zenworks/datamodel/objects/settings"
xmlns:ns2="http://novell.com/zenworks/datamodel/objects/settings">0</
ns2:Value></Variables><Variables><ns2:Name xmlns="http://novell.com/
zenworks/datamodel/objects/settings"% '
)
```

2. Run the following update query to set the DaysToRebuild from 0 to the desired value:

```
UPDATE zbundle SET serversidedata = replace(serversidedata,
'xmlns:ns2="http://novell.com/zenworks/datamodel/objects/
settings">DaysToRebuild</ns2:Name><ns2:Value xmlns="http://novell.com/
zenworks/datamodel/objects/settings" xmlns:ns2="http://novell.com/
zenworks/datamodel/objects/settings">0</ns2:Value></
Variables><Variables><ns2:Name xmlns="http://novell.com/zenworks/
datamodel/objects/settings" ', 'xmlns:ns2="http://novell.com/zenworks/
datamodel/objects/settings">DaysToRebuild</ns2:Name><ns2:Value
xmlns="http://novell.com/zenworks/datamodel/objects/settings"
xmlns:ns2="http://novell.com/zenworks/datamodel/objects/
settings">120</ns2:Value></Variables><Variables><ns2:Name xmlns="http://
novell.com/zenworks/datamodel/objects/settings" ')
```

```
WHERE zuid IN (
SELECT zuid
FROM zzenobject
WHERE path LIKE '%ZPM/Policy%'
AND primarytype = 'Bundle'
AND subtype LIKE '%Patch Bundle%'
AND serversidedata LIKE '%xmlns:ns2="http://novell.com/zenworks/
datamodel/objects/settings">DaysToRebuild</ns2:Name><ns2:Value
xmlns="http://novell.com/zenworks/datamodel/objects/settings"
xmlns:ns2="http://novell.com/zenworks/datamodel/objects/settings">0</
ns2:Value></Variables><Variables><ns2:Name xmlns="http://novell.com/
zenworks/datamodel/objects/settings"% '
)
```

NOTE: In the above query, as an example 120 is used. However, the number can be increased if you do not want the Patch Policy to be rebuilt soon. The number 120 represents the days to rebuild the patch policy.

For additional information, see [Troubleshooting System Updates](#).

3.2 Understanding Deploying Updates

You have the following options for deploying an update:

- Deploy the update to all devices without using deployment stages.
- Deploy the update by using deployment stages where one stage automatically starts after the previous one has completed, unless you have configured stages to pause the deployment and send email notifications to the administrator.
- Deploy the update by using deployment stages with e-mail notification to allow manual control for starting the next stage. You can use this option to test the update before deploying it to all devices in your production environment.
- Deploy the update to specific devices (selected individually and by device groups) without using deployment stages. You can use this option to test the update before deploying it to all devices in your production environment.

When you retire a device in ZENworks Control Center the device gets into the retired state only after the ZENworks Agent is refreshed on the device. You can either wait for the default device refresh to complete (the default device refresh interval is set to 12 hours) or you can manually refresh the

agent. After the agent is refreshed and the device has moved to the retired state, you can deploy the update to the remaining devices in the zone. If you deploy the update before the agent is refreshed, the update is applied to the retired device as well.

Although the retired device will show the system update assignment on the device details page in ZCC, the agent update service will not apply the assignment as long as the device is retired.

The Deploying System Updates panel displays the progress and results of deploying an update.

Updates are removed from this panel when the entire update process completes. You can view the Deployment History panel on the Release Details page for information on deployed updates.

NOTE: Actions on this page are available only to administrators with the following rights:

- ♦ Deploy Update rights
 - ♦ View Leaf rights
-

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Table 3-1 Deploying System Updates column descriptions

Column Heading	Explanation
Update Name/ Stage Name	<p>Displays the name of the system update, or name of the stage in which the System Update was deployed.</p> <p>Following are the various stage names:</p> <ul style="list-style-type: none">♦ stage_name: The update is being deployed to the managed devices that are members of the current stage that is listed.♦ Selected Devices Stage: The update is being deployed to selected managed devices without the use of stages.♦ All Devices Stage: The update is being deployed to all managed devices in the Management Zone without the use of stages. <p>After the system update is deployed to all devices in the Deployment Stages, the update will be deployed to the remaining devices (devices that are not a part of any deployment stage) in the zone. While deploying the update to the remaining devices, the Update Name /Stage Name will be All Devices Stage.</p> <p>If stages are being used, then click a stage name to view the device status for each stage member.</p> <p>All Devices Stage is displayed after the last stage has completed, which means any devices left in the Management Zone that were not part of a completed stage are then receiving the update. In other words, managed devices are not allowed to skip a system update.</p>
Start Schedule	<p>Displays the current schedule, if any has been set. Use the Reschedule Deployment action to reschedule the update. For more information, see Section 3.5, “Rescheduling a Deployment,” on page 46.</p> <p>Each device can have its own schedule.</p>

Column Heading	Explanation
Reboot Behavior	<p>Displays the reboot behavior of devices after the update is deployed.</p> <p>Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.</p> <p>You have the following reboot options:</p> <ul style="list-style-type: none"> ♦ Prompt User to Reboot When Update Finishes Applying: After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted. This is the default. <ul style="list-style-type: none"> ♦ Reboot device when no user is logged into the system: Select this option to reboot the device even if no user has logged into the system. ♦ Reboot device when the device is locked (only on Windows 8.1 and earlier): Select this option to reboot the device if the device is locked. Prompt will not be displayed before rebooting the device. <p>The above options are applicable on agents only when they are upgraded to ZENworks Update 2 or later version.</p> <ul style="list-style-type: none"> ♦ Do Not Reboot Device: The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted. <ul style="list-style-type: none"> ♦ Start ZENworks Agent with limited functionality: Select this option to start ZENworks services incase reboot is suppressed while deploying the update to the device. It is not applicable for Primary Servers. For information about Reboot-less Agent, see section “Reboot-less Agent” in the ZENworks Discovery, Deployment, and Retirement Reference. ♦ Force Device to Reboot: After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.

Column Heading	Explanation
Stage	<p>Indicates the deployment state. The possible entries are:</p> <p>stage_name: The update is being deployed to the managed devices that are members of the current stage that is listed.</p> <p>Selected Devices Stage: The update is being deployed to selected managed devices without the use of stages.</p> <p>All Devices Stage: The update is being deployed to all managed devices in the Management Zone without the use of stages.</p> <p>All Devices Stage is displayed after the last stage has completed, which means any devices left in the Management Zone that were not part of a completed stage are then receiving the update. In other words, managed devices cannot skip an update.</p> <p>If stages are being used, click a stage name to view the device status for each stage member. For more information, see Section 3.10, "Viewing Status by Device," on page 48.</p>
Status	<p>Indicates the status of the update being deployed (for the current stage, if stages are being used). For information on the possible statuses, see Chapter 6, "Update Statuses," on page 63.</p> <p>Click an item in the Status column to view a message explaining the current status.</p> <p>When the status for an update reaches either the APPLIED or BASELINE status, the update deployment item is no longer displayed in this panel, but is displayed in the Deployment History panel. For more information, see Section 3.10, "Viewing Status by Device," on page 48.</p>
Pending	<p>Displays the number of devices for which the update deployment process is pending. A device can be pending if it is a member of a stage when stages are not automatically started after another stage completes.</p> <p>Click the number to view the Status by Device page, which displays the devices that have a pending deployment of the update. For more information, see Section 3.10, "Viewing Status by Device," on page 48.</p>
Successful	<p>Displays the number of devices for which the update deployment process is complete.</p> <p>Click the number to view the Status by Device page, which displays the devices that successfully received the update. For more information, see Section 3.10, "Viewing Status by Device," on page 48.</p>
Failed	<p>Number of devices for which the update deployment process has failed.</p> <p>Click the number to view the Status by Device page, which displays the devices that failed to receive the update. For more information, see Section 3.10, "Viewing Status by Device," on page 48.</p> <p>For failed deployments, you have the option of ignoring the error and continuing, or you can redeploy the update if the error has been resolved.</p>

3.3 Deploying Updates

NOTE: If you have downloaded the system update via SLD, go to [step 6](#)

- 1 (Optional) Before deploying the updates, ensure that the health of the Primary Servers and the database in the Management zone is conducive for the deployment by performing diagnostic tests on the Primary Server using the ZENworks Diagnostic Center tool.

For detailed information about the ZENworks Diagnostic Center tool, see “[ZENworks Diagnostic Center](#)” in the *[ZENworks Command Line Utilities Reference](#)*.

- 2 (Optional) If you want to use deployment stages, set them up if you have not previously done so.

For more information, see [Section 1.2, “Creating Deployment Stages,”](#) on page 15.

NOTE: If you are using profiling or monitoring tools during the System Update, ensure that you use the Java Development Kit (JDK) binaries (`jvisualvm.exe`) from the custom installation of JDK, and not the binary files installed by ZENworks. If you use the ZENworks binaries, during the update, when JDK gets upgraded, it will fail to update any in-use binary file(s), causing the System Update to fail.

- 3 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab to display the Available System Updates panel.

- 4 (Conditional) If new updates are not being displayed, click **Action > Check for Updates**.

- 5 (Optional) To view the content of an available update, click the name of the update (in the **Update Name** column) to display the Release Details page:

For more information, see [Chapter 5, “Reviewing the Content of an Update,”](#) on page 59.

- 6 To download an update, select the check box, click **Action**, and then click **Download Updates**.

After an update is downloaded, the status automatically changes to **Downloaded**. The time taken to download an update depends on its size and system hardware configuration.

You can download multiple updates at a time, but you can deploy only one. Because these steps are repeated for each update, you only need to download the update that you plan to deploy.

After downloading the system update from ZENworks Control Center or manually importing from `zman sui` the system update is automatically prepared.

For more information, see “[Preparing an Update](#)” on page 31

- 7 To deploy an update, you should authorize the update. To authorize an update, select the check box for the system update that you want to authorize, click **Action**, and then select **Authorize Update**.

For more information, see “[Authorizing an Update](#)” on page 33

- 8 After preparing the update, the update should be configured. To configure an update, select the check box for the system update that you want to configure, click **Action**, and then select **Configure Update**.

For more information, see “[Configuring an Update](#)” on page 33.

- 9 To deploy an update, select the check box for the update that you want to deploy, click **Action > Deploy Update to Devices**.

You can deploy only one update at a time.

If you want to review the content of the update that you downloaded, see [Chapter 5](#), “[Reviewing the Content of an Update](#),” on page 59.

If you want to download a different update for deployment, return to [Step 5](#).

This starts the Create System Update Deployment Wizard for deploying the update to all applicable devices. If deployment stages are enabled, they can be used.

The Deployment Wizard provides you with many options, including scheduling the deployment.

10 In the Deployment Wizard, complete the following steps:

- 10a** On the Choose the System Update and Deployment Option page, select a deployment option (all of them can be scheduled in a subsequent wizard page).

NOTE: As a best practice, we recommend that you deploy the update to a Primary Server (in the case of a zone with embedded database, see step 2 below) before deploying the update to other Primary Servers and to the Managed Devices that contact those servers.

We recommend that you perform the following actions in order:

1. Designate a ZENworks Primary Server to download the system update.
2. Designate a ZENworks Primary Server to be the first server to update in the zone. In the case of a zone with embedded database, it must be the Primary Server that hosts the database.
3. After the system update is in the **Downloaded** state, assign the update to only the designated Primary Server chosen in Step 2 above.
4. Refresh the ZENworks Updater Service, and allow the system update to complete. After the system update is completed, reboot the system.

The refresh can be performed by using the `zac zeus-ref` command. By default, it will be performed as per the schedule.
5. After the Server is restarted and running, update the other Primary Servers in the zone, followed by Satellite Servers and Managed Devices.

In a production environment, we recommend that you use the **Deploy System Update to selected devices in the Management Zone** option to update the designated Primary Server chosen in Step 2 above, remaining Primary Servers, Satellite Servers and Managed Devices. Or you should use the **Deploy System Update to devices using Stages in the Management Zone** option to deploy the update to a stage containing the designated Primary Server chosen in Step 2 above before deploying it to other stages containing the remaining Primary Servers and managed devices.

-
- ♦ **Deploy System Update to selected devices in the Management Zone:** Deploys the selected update to only the devices that you select in [Step 10c](#). Stages are not used. If you choose this option, the next page of the wizard lets you select the reboot behavior for the devices included in the deployment.
 - ♦ **Deploy System Update to all devices in the Management Zone:** Deploys the selected update to all devices in the Management Zone. Stages are not used. If you choose this option, the next page of the wizard lets you select the reboot behavior for the devices included in the deployment.

NOTE: This option is available to administrators only if they have Deploy Update rights and View Leaf rights to all devices in the zone.

This option does not guarantee that ZENworks Servers are updated before managed devices. In a large ZENworks system or in a production environment, we recommend that you use one of the other options.

- ♦ **Deploy System Update to devices using Stages in the Management Zone:** The selected update is deployed to only the devices that have membership in one of the stages. The stages are executed one after the other; that is, a stage does not start until the previous stage completes. After all stages complete, the **All Devices** stage is run. If you choose this option, and because the reboot behavior is set per stage, the next page of the wizard lets you select the reboot behavior for the **All Devices Stage**, which runs automatically after all other stages.

NOTE: This option is available to administrators only if they have Deploy Update rights and View Leaf rights to all devices in the zone.

For more information on stages, see the [Section 1.2, “Creating Deployment Stages,” on page 15](#).

10b Click **Next** and select one of the following options, and then click **Next**:

- ♦ **Prompt User to Reboot When Update Finishes Applying:** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted. This is the default.
 - ♦ **Reboot device when no user is logged into the system:** Select this option to reboot the device even if no user has logged into the system.
 - ♦ **Reboot device when the device is locked (only on Windows 8.1 and earlier):**
Select this option to reboot the device if the device is locked. Prompt will not be displayed before rebooting the device.

The above options are applicable on agents only when they are upgraded to ZENworks Update 2 or later version.

- ♦ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.
 - ♦ **Start ZENworks Agent with limited functionality:** (Optional) Select this option to start ZENworks Agent with limited functionality without rebooting the device. For more information, see [Reboot-less Agent](#) in the [ZENworks Discovery, Deployment, and Retirement Reference](#) guide.
- ♦ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

10c (Conditional) If you selected **Deploy System Updates to Selected Devices** in the Management Zone in [Step 10a](#), the following wizard page displays:

10d To add devices or groups to the deployment configuration, click **Add**, browse for and select the devices or device groups to include in the update deployment, then click **OK**.

10e Click **Next** to display the Choose the Deployment Schedule page.

10f Fill in the fields:

Schedule Type: Select one of the schedule options:

- ♦ **Now:** Immediately deploys the update when you finish the wizard.
- ♦ **Date Specific:** Deploys the update according to the schedule that you set. The following options are displayed for the **Date Specific** option:

Fill in the fields:

- ♦ **Start Date:** Select the deployment date from the calendar.
- ♦ **Run Event Every Year:** Select this option to deploy the update every year on the start date.
- ♦ **Process Immediately if Device Unable to Execute on Schedule:** Do not use this option for updates. It does not apply to updates.
- ♦ **Start Immediately at Start Time:** Lets you deploy updates at the start time you specify.
- ♦ **Start at a Random Time Between Start and End Times:** Lets you deploy updates at a random time between the times you specify. Fill in the **End Time** fields.

10g Click **Next** to display the Review Deployment Options page, and review the information. Click **Back** to make changes.

11 Click **Finish** to start the deployment.

WARNING: While updating ZENworks to 11.4.2 or later versions on a Windows 10 device, before the System Update begins, a pop-up window is displayed with the **Windows Explorer will be restarted before ZENworks System Update** message if **Show System Update Progress** is enabled in the device, folder or zone settings.


After restarting Windows Explorer:

- ♦ All unsaved changes will be lost.
 - ♦ All opened applications will be restarted.
 - ♦ All opened folders will be closed.
-

12 In the **Status Link** window, click the URL to view the deployment status.

For more information, see [“Viewing the System Update Deployment Status” on page 53](#).

13 (Conditional) If you chose the deployment schedule type as **Now** in [Step 10f](#), the update is deployed only during the next device refresh schedule. However, if you want to immediately apply the update to the device, you must manually refresh the managed device in one of the following ways:

- ♦ Click the **Devices** tab > the **Managed** tab > **Servers** or **Workstations**, then select the check box next to the devices you want to refresh, click **Quick Tasks** > **Refresh Device**.
- ♦ On the managed device, right-click the  icon, then click **Refresh**.
- ♦ On the Linux unmanaged device, open a terminal, change your current working directory to `/opt/novell/zenworks/bin/`, and execute `./zac ref` for managed devices and `./zac zeus-ref` for Primary Servers.

- 14 To observe the progress of the update deployment, do any of the following:
 - ♦ In ZENworks Control Center, observe the panels on the System Updates page:
 - ♦ The Available System Updates panel automatically displays **Baselined** in the **Status** column when the deployment has completed.
 - ♦ The Deployed System Updates panel displays the update in its listing when the deployment has completed.
- 15 To verify that the update was successfully deployed:
 - 15a To verify that the MSIs or RPMs have been installed and the update process is complete, review the following log files:

Windows: %zenworks_home%\logs\system-update\<SU_GUID>\system-update.log

Linux: /var/opt/novell/log/zenworks/system-update/<SU_GUID>/system-update.log
 - 15b Test the ZENworks software on the device to ensure that it is working properly.
 - 15c To ensure that the update has been deployed, do one of the following to determine whether the version number has been incremented (for example, the first update for ZENworks should change the value from 10.0.x to 10.0.2):
 - ♦ Open the Windows Registry and browse to the following:

HKEY_LOCAL_MACHINE/Software/Novell

For the **ZCM** key, the update process should have incremented the **version** value.
 - ♦ On a Windows device, review the following file:

Installation_path\Novell\ZENworks\version.txt
 - ♦ On a Linux device, review the following file:

/etc/opt/novell/zenworks/version.txt
 - 15d Repeat [Step 15a](#) through [Step 15c](#) for each test device.
- 16 (Conditional) If you are receiving email notifications at the completion of the deployment stages and are ready to begin the next stage, go to the Deployed System Updates panel, then click **Action > Advance to Next Stage**.
- 17 To deploy another update, repeat from [Step 5](#).

3.3.1 Upgrading the Agent in VDI environment

Perform the following steps to upgrade Master image:

- 1 Switch on the master image and deploy the SU to master image.
- 2 Backup the `initial-web-service` file from the %ZENworks_Home%\conf location.
- 3 If you want to add a registration key, you can add in the `initial-web-service` file.
The first line of the `initial-web-service` file contains the list of IP addresses and host names of the server to which this device has registered. Add the registration key in the second line.
- 4 Unregister the device by using the `zac unr` command.

- 5 Clear the Workstation GUID by using `zac fsg -d` command.
- 6 At the command prompt, go to `%ZENworks_Home%\bin\preboot` folder, then run the `ZISWIN.exe -w` command to clear Image-safe Data.
- 7 Clear the cache by using the `zac cc` command.
- 8 Copy the backed up `initial-web-service` file to `%ZENworks_Home%\conf` location.

Shutdown the master image, take the snapshot, and use the snapshot for recomposing the desktop pools. For more information about updating master image, see [Update Linked-Clone Desktops \(VMware\)](#).

3.4 Starting a Pending Stage

The default stage behavior is to automatically advance through the configured stages. However, you can configure stage behavior for individual stages or for all stages.

The **Start Pending Stage** option is only available if you used the **Advance to Next Stage Manually and Notify When Complete** option to stop each stage for manual input before continuing, instead of having the stages complete automatically.

To start a pending stage:

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deploying System Updates panel, select the check boxes for an update.
- 3 Click **Action > Start Pending Stage**.

3.5 Rescheduling a Deployment

You cannot reschedule a deployment after it starts:

- [Section 3.5.1, “Rescheduling a Deployment for the All Stages Status,” on page 46](#)
- [Section 3.5.2, “Rescheduling a Deployment for the Other Statuses,” on page 46](#)

3.5.1 Rescheduling a Deployment for the All Stages Status

- 1 Select the check box for an update.
Because all devices do not need to have the update deployed at the same time, you can set individual deployment schedules for the devices.
- 2 Click **Action > Reschedule Deployment** to open the Redeployment Schedule dialog box.
- 3 Either click **OK** to accept the default schedule of **Now**, or select **Date Specific** in the **Schedule Type** field, specify the new date, then click **OK**.

3.5.2 Rescheduling a Deployment for the Other Statuses

- 1 Select the check box for an update.
- 2 Click **Action > Reschedule Deployment**.

- 3 In the Status by Device page, select the check box for an update, then click **Reschedule Deployment**.
- 4 On the Status by Device page, select one or more devices that are listed in the **Device** column.
- 5 Click **Reschedule Devices** to open the Redeployment Schedule dialog box.
- 6 Either click **OK** to accept the default schedule of **Now**, or select **Date Specific** in the **Schedule Type** field and specify the new date, then click **OK**.

3.6 Bypassing Staging

You can bypass the stages at any time and immediately deploy the update to all managed devices in the Management Zone.

- 1 Select the check box for an update.
- 2 Click **Action > Bypass Stages and Apply to All Devices**.

3.7 Canceling a Deployment

This option is mainly for canceling a deployment that has not yet started.

If you select to apply the update only through stages, and if you cancel the update deployment, the status in the Available System Updates panel is changed to **Aborted**.

However, for an update, you can select to deploy to individual devices, as well as through stages for the other devices. Therefore, the status in the Available System Updates panel is changed to:

- ♦ **Ready** if you cancel only the staged deployment.
- ♦ **Aborted** if you cancel both the staged deployment and the deployment for individually selected devices.

To cancel a deployment:

- 1 Select the check box for an update.
- 2 Click **Action > Cancel Deployment**.

WARNING: If you cancel a deployment that is currently running (not just scheduled), all deployment actions performed up to that point cannot be reversed. There currently is no rollback option.

- 3 Click **OK** to confirm canceling the deployment.

3.8 Clearing an Error to Retry a Deployment

To continue with the deployment after determining that an error is not serious enough to stop the deployment:

- 1 Click **Action** > **Clear Error and Continue**.

3.9 System Update Fails on the Device with an Error Code

When you deploy an update on the managed device, the system update checks for the availability of the Windows installer service, before making any change to the device.

If installation of other MSIs, not related to ZENworks, is in progress and the system update installation begins, the update of subsequent ZENworks MSIs fails. The Windows installer displays the following error with the error code 1618:

ERROR_INSTALL_ALREADY_RUNNING

You need to redeploy the update on the managed device to successfully update the ZENworks MSIs.

3.10 Viewing Status by Device

The following sections contain more information:

- [Section 3.10.1, “Understanding Device Statuses,” on page 48](#)
- [Section 3.10.2, “Viewing a Device Properties,” on page 49](#)
- [Section 3.10.3, “Viewing Information of a Device Status,” on page 49](#)
- [Section 3.10.4, “Viewing Status by Device - Advanced,” on page 49](#)
- [Section 3.10.5, “Toggling Ignored Devices,” on page 51](#)
- [Section 3.10.6, “Redeploying Updates to Devices,” on page 52](#)
- [Section 3.10.7, “Refreshing Devices,” on page 52](#)
- [Section 3.10.8, “Searching - Status by Device,” on page 52](#)

3.10.1 Understanding Device Statuses

In the Deploying System Updates panel, you can click any of the underlined links to display the corresponding status of devices. For example, if you click the link in the **Pending** column, you see the status of devices on which the deployment is pending.

The possible statuses that can be viewed on this page are:

Pending Devices: Lists only the devices where the selected update is pending.

Successful Devices: Lists all of the devices where the selected update has been successfully deployed.

Failed Devices: Lists only the devices where the selected update failed.

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order. This page refreshes automatically to allow you to work with devices as the update is applied on them.

Column Heading	Explanation
Device	The device name. Click the device name to display the property of the device.
Status	<p>The current update deployment status for the device. Click the status item to view information about the status.</p> <p>For more information on the individual statuses, see Chapter 6, “Update Statuses,” on page 63.</p>
Device Type	Whether the device is a server or workstation.
In Folder	The folder where the device object resides in the ZENworks Control Center.

3.10.2 Viewing a Device Properties

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deploying System Updates panel, click an underlined link in the **Update Name, Stage, Pending, Successful, or Failed** column to display the appropriate Status by Device page.
For example, if you click the link in the **Pending** column, you see the status of devices on which the deployment is pending.
- 3 Click the underlined link in the **Device** column to display the device’s properties.

3.10.3 Viewing Information of a Device Status

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Deploying System Updates panel, click an underlined link in the **Update Name, Stage, Pending, Successful, or Failed** column to display the appropriate Status by Device page.
- 3 Click the underlined link in the **Status** column to display status information about the device.

3.10.4 Viewing Status by Device - Advanced

This page displays the status of devices in the Advanced view based on your selection in the Deploying System Updates panel. To view Status by Device Advanced page:

1. In **ZENworks Control Center**, click **Configuration**, and then click **System Updates** tab.
2. In the **Deploying System Updates** panel, click any device status link.
3. In the Status by Device page, click the **Advanced** button.

Status by Device Advanced page is displayed. Depending on your selection in the Deploying System Update panel, the displayed column might vary.

Table 3-2 Status by Device - Advanced view column information

Column Heading	Description
Ignored	Displays a check mark next to ignored devices.
Device	Displays the device name. Click the name to display the properties of the device.
Reboot Behavior	<p>Displays the reboot behavior of devices after the update is deployed.</p> <p>Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.</p> <p>You have the following reboot options:</p> <ul style="list-style-type: none"> ♦ Prompt User to Reboot When Update Finishes Applying: After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted. <ul style="list-style-type: none"> ♦ Reboot device when no user is logged into the system: Select this option to reboot the device even if no user has logged into the system. ♦ Reboot device when the device is locked (only on Windows 8.1 and earlier): <p>Select this option to reboot the device if the device is locked. Prompt will not be displayed before rebooting the device.</p> <p>The above options are applicable on agents only when they are upgraded to ZENworks Update 2 or later version.</p> ♦ Do Not Reboot Device: The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted. ♦ Start ZENworks Agent with limited functionality: Select this option to start ZENworks services in case reboot is suppressed while deploying the update to the device. <p>For more information, see Reboot-less Agent in the ZENworks Discovery, Deployment, and Retirement Reference guide.</p> ♦ Force Device to Reboot: After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.

Column Heading	Description
Status	<p>Displays the current system update deployment status for the device. To view status information, click the status item.</p> <p>For more information on Status, see “Update Statuses” on page 63.</p>
Device Type	Displays whether the device is a server or a workstation.
Source	Displays the name of the source through which the system update was assigned to the device. System update source can be assigned directly, or through a group or folder.
Applied Date	<p>Displays the date when the system update was applied on the device.</p> <p>This column is displayed only for devices on which the system update is successfully applied.</p>
In Folder	Displays the ZENworks Control Center folder where the device object resides.
Auto Refresh	<p>To define the interval at which the information should be refreshed, click Auto Refresh and select the required option:</p> <ul style="list-style-type: none"> ◆ No Auto Refresh ◆ 15-Second Refresh ◆ 30-Second Refresh ◆ 60-Second Refresh

3.10.5 Toggling Ignored Devices

Ignoring a device is helpful if an update fails on a device and you want to continue with the deployment without resolving the error. For example, if a device is offline, you might want to ignore that device so that the deployment can continue.

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the **Deploying System Updates** panel, click an underlined link in the **Update Name, Stage, Pending, Successful, or Failed** column to display the appropriate Status by Device page.
- 3 Select the check box next to one or more devices.
- 4 Click **Action > Toggle Ignored Devices**.

The options available in the **Action** menu varies, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

3.10.6 Redeploying Updates to Devices

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the **Deploying System Updates** panel, click an underlined link in the **Update Name**, **Stage**, **Pending**, **Successful**, or **Failed** column to display the appropriate Status by Device page.
- 3 Select the check box next to one or more devices.
- 4 Click **Action > Redeploy Update to Devices**.

The options available from the **Action** menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

3.10.7 Refreshing Devices

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the **Deploying System Updates** panel, click an underlined link in the **Update Name**, **Stage**, **Pending**, **Successful**, or **Failed** column to display the appropriate Status by Device page.
- 3 Select the check box next to one or more devices.
- 4 Click **Action > Refresh Device**.

The options available from the **Action** menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

3.10.8 Searching - Status by Device

The search panel in the Status by Device page enables you to narrow the number of devices displayed. Based on your selection in the Deploying System Update panel, the fields displayed in the search panel might vary.

Table 3-3 Status by Device - Search panel information

Field	Description
Device Name	Specify the device name.
Status	Select the type of request you want to include in the search result. Depending on your selection in the Deploying System Update panel, the displayed status fields might vary.
Device Type	Select the type of device you want to include in the search result.
In Folder	Specify the name of the folder in which the device object resides in the ZENworks Control Center.

Field	Description
Include Ignored Device	<p>Select this option to include ignored devices in your search results.</p> <p>This field is displayed only for devices with Pending and Failed status.</p>

3.11 Viewing the System Update Deployment Status

After deploying a system update to devices, you can view the deployment status. To view the deployment status perform the following:

1. In the ZENworks Control Center, click Configuration in the left pane, then click the System Update tab.
2. In the Available System Updates panel, click View Status button.
You will be navigated to a new tab. In this tab, you can view update status of Primary Servers.

Note: You can also view the deployment status by using following URL format:

`https://<host_name>:7444/systemupdate/sustatus`

In the System Update Status page, you can view update status by clicking the filter buttons. By default, update status of all Primary Servers are displayed.

The filter options are:

- ♦ **Total:** Lists all the servers on which the system update is assigned.
- ♦ **Failed:** Lists all the servers on which the system update has failed.
- ♦ **Not Started:** Lists all the servers on which the system update has not started.
- ♦ **In Progress:** Lists all the servers on which the system update is in progress.
- ♦ **Completed:** Lists all the servers on which the system update is completed.

If you have deployed more than one system update in the zone, then use the drop-down button to narrow your search results.

Following are some of the tasks that you can perform in the System Update Status page.

Table 3-4 System Update Status

Tasks	Description	Additional Information
Rerun the schema update	<p>To rerun the schema update:</p> <p>Click the Rerun button.</p> <p>Enter the zone administrator credentials, and then click the Submit button.</p>	<ul style="list-style-type: none"> ♦ You can rerun the schema update only from the server on which the schema update has failed.

Tasks	Description	Additional Information
Rerun the Package update	To rerun the package update, click the Rerun button.	You can rerun the package update only from the server on which the update has failed.

3.12 Standalone Agent Updater

The Standalone Agent Updater is an independent executable to update Windows managed devices and Windows Satellite Servers. Even if the device is unable to connect to the server, the Standalone Agent Updater can update the device to the latest version of the agent. The executable can be generated on any ZENworks Primary Server in the zone by using the `zman system-update-create-package (sucp)` command for the update that is imported into the zone.

IMPORTANT: ♦ .NET 4.5 full framework must be installed on your device to execute Standalone Agent Updater.

- ♦ Only a system user with administrative privileges can execute this tool.
 - ♦ If the device is not registered to any zone, then it will automatically register with the zone from where the standalone updater executable has been created.
 - ♦ Using Standalone Agent Updater, you cannot update the managed devices which are registered to a different zone.
 - ♦ The ZENworks agent or service does not have to be in a working state for the update to be applied through the Standalone Agent Updater.
 - ♦ ZENworks supports updating only Windows platform through the Standalone Agent Updater (both 32 bit and 64 bit platforms).
 - ♦ If the zone CA or server certificates have undergone change, then the existing Standalone Agent Updater executables need to be created again.
-

The Standalone Agent Updater contains the following sections:

- ♦ [Section 3.12.1, “Creating the Standalone Agent Updater executable,” on page 54](#)
- ♦ [Section 3.12.2, “Executing the Standalone Agent Updater,” on page 55](#)
- ♦ [Section 3.12.3, “Viewing the Standalone Agent Updater log files,” on page 55](#)

During certificate update, if you ignore any device, then after successful activation of certificates, the ignored devices will not be able to communicate with zone. After the certificate update is baselined, the certificate updater tool will be removed from the download location (<https://<server-address>/zenworks-setup>). To overcome the communication issue on ignored devices, all devices should be updated with the certificate update using certificate updater tool. Hence, we recommend to back up the relevant certificate updater tool from the download location before ignoring any device.

3.12.1 Creating the Standalone Agent Updater executable

Standalone updater package is created by using the `zman sucp` command.

To create a system update package for a specific device:

- 1 Run the following `zman` command:

```
zman sucup <System_Update_Name or SystemUpdate GUID> <device path  
relative to /Devices or Device GUID> [-n|--package-name=Standalone  
update package name]
```

For example, `zman sucup 5011030000fc50000000002013052716 /Devices/Workstations/managed-device1` for generating package for the managed-device1 workstation.

- 2 (Conditional) If the package-name (or -n) is not specified with a Standalone Agent Updater Package name, then the package is created as <deviceName>[<deviceGUID>].exe and stored.

To create a system update package for a platform:

- 1 Run the following `zman` command:

```
zman sucup <System_Update_Name or SystemUpdate GUID> -p=<OS Platform> -  
a=<Architecture>
```

-p, --platform=<OS Platform>: OS platform for the standalone update package. Valid value is Windows.

-a, --arch=<Architecture>: Device architecture for the standalone update package. Valid values are "32" and "64".

The created standalone updater package is stored in the following path:

- **For Linux:** /opt/microfocus/zenworks/install/downloads/system-update/
- **For Windows:** %ZENSERVER_HOME%\install\downloads\system-update

3.12.2 Executing the Standalone Agent Updater

To execute the Standalone Agent Updater:

- 1 Copy the EXE file to the agent device.
- 2 Log into the managed device as an administrator.
- 3 Double click the EXE file to start the upgrade. Running the EXE from a command prompt with -v provides verbose output while upgrading or if any errors occur.

3.12.3 Viewing the Standalone Agent Updater log files

While creating the standalone update package on the Primary Server by using the `zman sucup` command, if any error displays, then see `zman.log` and `loader-messages.log` files.

While executing the standalone agent updater on the managed device, if any error displays, then see %zenworks_home%\logs\system-update\<SU_GUID>\system-update.log file.

3.13 Superseded Files

When you install the newer version of ZENworks, the older version file or package will be retained. The retained file or package names will have superseded as suffix. These superseded files allow you to enable the older version components that are disabled after updating.

Superseded files are in the following location:

- ♦ **Windows:** %ZENWORKS_HOME%\install\downloads
- ♦ **Linux:** /opt/novell/zenworks/install/downloads

These files might not be deleted even after deleting the update from the zone. Before deleting the superseded files manually, refer to the TID [7012095 \(https://support.microfocus.com/kb/doc.php?id=7012095#\)](https://support.microfocus.com/kb/doc.php?id=7012095#).

NOTE: To allow clean-up of superseded files on all the Primary Servers, ensure that all the Primary Servers in the zone are active before attempting to baseline any existing System Update.

3.14 Limitations of System Update

3.14.1 System Update on Windows 10 devices connected through RDP

- ♦ On Windows 10 1809 or earlier versions, due to Windows limitations, the device will reboot even without a System Update prompt.
- ♦ On Windows 10 20H2 or later versions, the prompt will not be displayed, and the device will not reboot. The reboot prompt will be suppressed and if the prompt is displayed, the reboot will not be honoured. You must reboot the device manually.
- ♦ The system update reboot prompt is not applicable for devices that are connected through the RDP session for non-console users and terminal server environments, even if the update prompt is configured.

4 Deleting Updates

You can clear an update that fails to download, or an update that you do not want to deploy.

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Available System Updates panel, select the check boxes for one or more updates.
- 3 Click **Action > Delete Update**.

The update is deleted from the list and all downloaded files are removed. However, if the deleted update is still available on the update server, it is displayed in the list again for possible downloading the next time that you check for updates.

5 Reviewing the Content of an Update

You might want to review the content of an update for the following reasons:

- ♦ To determine whether to download the update
- ♦ To determine whether to deploy a downloaded update
- ♦ To review what was deployed by the update
- ♦ To review the history of the update

This section contains the following information:

- ♦ [Section 5.1, “Viewing the Release Details Page,” on page 59](#)
- ♦ [Section 5.2, “Update Release Details,” on page 59](#)
- ♦ [Section 5.3, “Deployment History,” on page 60](#)

5.1 Viewing the Release Details Page

- 1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **System Updates** tab.
- 2 In the Available System Updates panel, click an update name in the **Update Name** column to display the Release Details page:.

5.2 Update Release Details

Table 5-1 Information from the System Update Release Details Panel

Column Heading	Explanation
Update Name	The name of the update, which is created by Micro Focus.
Update GUID	The update’s GUID.
Release Date	The date the update was released by Micro Focus.
Download Date	The date you downloaded the content of the update, including all files necessary to install the update.
Priority Level	The relative importance of the update’s content to your ZENworks installation. Some possible entries: OPTIONAL: Not required for normal operation of ZENworks. MANDATORY: A required update that must be applied.
Description	Brief information about the purpose of the update and its content.

Column Heading	Explanation
Targets	Indicates whether the target devices are Primary Servers only, all managed devices, or servers with ZENworks roles.
Product Version	The version of ZENworks in this update.
Prerequisite Updates	Any updates that are required for this update.
Superseded Updates	Any updates that the current update supersedes.
Update Notes	Brief information about important issues related to the update.
Update Readme	Information pertinent to deploying the update, such as last-minute instructions. Click this entry to open the Readme.
Updated Files	Lists all of the files contained in the update that will be applied to update your ZENworks software.
Content Replication Status	Displays the content replication status of the current update on Primary Servers and Content Satellite Servers. It is advisable to deploy the update to managed devices only after all the servers have 100% replication.

5.3 Deployment History

This Deployment History panel displays a current snapshot of the history for the selected update. It does not automatically refresh its content.

The following sections contain more information:

- ♦ [Section 5.3.1, “Understanding Deployment History Details,” on page 61](#)
- ♦ [Section 5.3.2, “Performing Deployment History Tasks,” on page 62](#)

5.3.1 Understanding Deployment History Details

Table 5-2 Columns for the Deployment History Details Panel

Column Heading	Explanation
Stage	<p>Indicates the deployment method used. The possible entries are:</p> <p>stage_name: The update was deployed to the managed devices that are members of the stage that is listed.</p> <p>Selected Devices Stage: The update was deployed to selected managed devices in the Management Zone that are not members of a stage.</p> <p>All Devices Stage: The update was deployed to all managed devices in the Management Zone that are not members of a stage.</p>
Status	<p>Indicates the status of the update that was successfully deployed, such as Applied or Baselined.</p> <p>In Process: The update is currently being deployed to the members of the stage.</p> <p>For more information on the individual statuses, see Chapter 6, “Update Statuses,” on page 63.</p>
Pending	<p>Displays the number of devices for which the update deployment process is pending. A device can be pending if it is a member of a stage when stages are not automatically started after another stage completes.</p> <p>Click the number to view the Status by Device page, which displays the devices that have the deployment of the update pending.</p>
Successful	<p>Displays the number of devices for which the update deployment process has completed.</p> <p>Click the number to view the Status by Device page, with the devices displayed that successfully received the update.</p>
Failed	<p>Displays the number of devices for which the update deployment process has failed.</p> <p>Click the number to view the Status by Device page, which displays the devices that failed to receive the update.</p> <p>For failed deployments, you have the option of ignoring the error and continuing, or you can redeploy the update if the error has been resolved.</p>

5.3.2 Performing Deployment History Tasks

Table 5-3 Tasks for Evaluating an Update's Deployment History

Task	Steps	Additional Details
View which devices have their deployment pending	<ol style="list-style-type: none">1. In the Deployment Stages panel, click the number in the Pending column.2. On the Status by Device page, review the information.	Displays devices where the deployment of the update is pending.
View the devices where deployment was successful	<ol style="list-style-type: none">1. In the Deployment Stages panel, click the number in the Successful column.2. On the Status by Device page, review the information.	Displays devices that have had the selected update successfully applied.
View which devices had the deployment fail	<ol style="list-style-type: none">1. In the Deployment Stages panel, click the number in the Failed column.2. On the Status by Device page, review the information.	<p>Displays devices where the update deployment failed.</p> <p>In order to consider a deployment successfully finished when there are failed devices, the failed devices should either be ignored, or the error should be fixed before you redeploy the update to those failed devices.</p>

6 Update Statuses

The following update statuses can be displayed in the **Status** column of several System Update panels in ZENworks Control Center:

Aborted: The deployment of the update was stopped, such as by selecting **Action > Cancel Deployment**.

Applied: The update was successfully applied to the managed devices.

Available: Updates with this status have downloaded the information about the update, which you can view by clicking the update name in the **Update ID** column.

Awaiting Reboot: The device is waiting for you to manually reboot after the update has been applied.

Rebuilding Deployment Packages: From ZENworks 2020 Update 3 onwards, the Network (.NET required) and Standalone (.NET required) packages for Windows and Network (JRE required) for Linux are no longer supported.

An administrator user can download the ZENworks Agent package (web-installer.exe) from the ZENworks Server.

You can now download a lightweight network installer .zip file from the ZENworks setup page and then execute it to install the full ZENworks agent. The Network installer .zip file contains Micro Focus signed web installer file and a config file containing the ZENworks server URLs and Zone CA certificate.

NOTE: Only All Architecture is supported for the network packages. During the system update, ZENworks uses the configuration of all architecture or x86_64 (64-bit) or x86 (32-bit) to rebuild an All Architecture version, and the existing x86 (32-bit) and x86_64 (64-bit) will be removed for custom packages. Precedence for choosing the existing custom package for rebuilding will be in the order of all architecture, x86_64 (64-bit) and then x86 (32-bit).

Only the Standalone (.NET included) package is available. During the system update, ZENworks uses the configuration of either Standalone (.NET included) or Standalone (.NET required) to rebuild the Standalone (.NET included) package. Standalone (.NET included) takes higher precedence for rebuilding. The existing Standalone (.NET required) package will be removed.

Baselined: The update has been assigned to the `/Devices` folder, meaning that all new devices added to the Management Zone automatically get the update, unless they are already at that update level. When an update is baselined, any packages (MSIs and RPMs) that were updated by the system update have been deleted and replaced with the new packages. A baselined update is considered complete; although, individual devices could have been ignored.

Canceled: Displays after you select **Action > Cancel Download** and the download or deployment was successfully canceled.

Canceling: Temporarily displays after you select **Action > Cancel Download**.

Deploying: The update is currently being deployed. See [Chapter 3, “Deploying Updates,” on page 35](#) for further deployment information and for actions that you can take on an update that is being deployed.

Downloaded: You have downloaded the update’s content and it is ready for deployment. See [Chapter 3, “Deploying Updates,” on page 35](#) for further deployment information and for actions that you can take on an update that has been deployed.

Downloading: Displays a percentage of completion during the downloading process. This status changes to **Downloaded** when the download is complete.

Error: The stage failed to complete because of an error with one or more of the devices being updated. You can select to ignore the error and continue, or to fix the error before continuing. This status can also indicate an error in downloading the update.

In Process: That the current stage is active.

Preparing: Indicates that the system update is in the Preparing stage.

During this stage, prerequisites are checked, and then preparation of the system update starts on all the Primary Servers. For more information, see [“Preparing an Update” on page 31](#).

Awaiting Authorization: Indicates that the System Update should be authorized by the administrator.

Awaiting Configuration: Indicates that the system update is ready to be configured.

Administrators with Configure System Update rights can configure the system update.

Installing Update: The update is currently being installed on the device.

Ready: The current stage is ready to start.

Reboot in Process: Rebooting the device is in process.

Reboot Process Canceled: Rebooting the device after the update was applied was canceled.

Rebuilding System Packages: The agent packages will be rebuilt in this stage. For more information, see [Managing Deployment Packages](#).

Scheduled: The update has a schedule defined for it. See [Chapter 3, “Deploying Updates,” on page 35](#) when creating the deployment in the Create System Update Deployment Wizard. You can alter the update’s schedule by using the **Action > Reschedule Deployment** option.

Stage Complete: The stage has completed.

Status Unknown: The status of updates for the device is unknown.

Superseded: Indicates that the update has been replaced by another update listed in the Available System Updates section. You should see this status only if you are in the process of deploying this update and there are pending devices. You can delete a superseded update, but you cannot deploy it.

Update Aborted: The update was canceled for the device.

Update Completed: Installation of the update has been completed on the device.

Update Completed with Errors: Installation of the update has been completed on the device, but there were errors. Check the update log for details.

Update Assigned: The update has been assigned to the device.

Zone Pre-Update Actions: Actions for the Management Zone are taking place before the server update begins.

Zone Post-Update Actions: Actions for the Management Zone are taking place after the server upgrade finishes.

7 Configuring the System Update Behavior of the ZENworks Agent

You can configure System Update behavior on the ZENworks Agent that resides on managed devices.

- 1 In ZENworks Control Center, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click **Device Management**, then click **System Update Agent**.
- 3 Fill in the fields:

Show Permission Prompt: Select **On** to display a dialog box on the managed device when a System Update is ready to begin. If this setting is set to **On**, the user can cancel, postpone, or allow the update to begin.

By default, this setting is set to **Off**, which does not give the user the ability to cancel or postpone the update, and the update begins immediately without the user being prompted.

Permission Prompt Max Postpone This setting specifies how many times the user can postpone the update. If you select **On** for the **Show Permission Prompt** setting, the user is prompted before a System Update begins. The user can then postpone the update. Select **Unlimited** to let the user postpone the update an unlimited number of times. Or, Select **Limit**, then specify a number to let the user postpone the update the specified number of times. By default, the user can postpone the update five times.

Permission Prompt Timeout When the user is prompted for permission to apply the update, you can specify how long you want to wait for an answer before the update begins. To display the permission prompt until the user responds, select **No Timeout**. Or, select **Timeout after _ mins** and specify the number of minutes you want an unanswered prompt to remain on the user's screen before the update starts. By default, the user has five minutes to respond to the prompt.

Specify this value in minutes.

Permission Prompt Nag Time When the user chooses to postpone the start of the update, this setting specifies how often the prompt appears to let the user know that an update is waiting to start. By default, this prompt displays every 15 minutes.

Specify this value in minutes.

Permission Prompt Max Wait Time To prevent the user from continuing to postpone the update without any feedback being given to the ZENworks system, this setting specifies the maximum number of minutes that an update waits for permission before giving up and reporting the update as canceled by the user.

Specify this value in minutes. The default is 120 minutes.

Reboot Prompt Nag Dialog If this setting is set to **On**, a dialog box is displayed on the managed device to remind the user that a reboot is required to complete the update. By default, the setting is set to **On**, and the dialog box displays every 15 minutes.

Reboot Prompt Max Postpone This setting specifies how many times the user can postpone the reboot if one is required for the update. If you select **On** for the **Reboot Prompt Nag Dialog** setting, the user is prompted before a reboot occurs. The user can then postpone the reboot. Select **Unlimited** to let the user postpone the reboot an unlimited number of times. Or, select **Limit**, then specify a number to let the user postpone the reboot the specified number of times. To postpone a reboot n times, you need to specify the **Limit** as $n-1$. For example, if you want to postpone the reboot 3 times, then you need to specify the **Limit** as 2. By default, the user can postpone the reboot five times.

Reboot Prompt Timeout When an update is assigned with the **Prompt User for Reboot** option, the default behavior is to wait five minutes for a response from the user and, in the absence of a response, automatically initiate the reboot. Select **No Timeout** to display the dialog box until the user responds, without initiating the reboot. Or, select **Timeout after _ mins**, then specify the number of minutes to wait for the reboot response before initiating the reboot.

Reboot Prompt Nag Time When an update assigned with the **Suppress Reboot** option, or if a user chooses to cancel a required reboot, a dialog box displays to remind the user that a reboot is required to complete the update. By default, the dialog box displays every 15 minutes. This setting lets the administrator define how often the prompt is presented to users.

Specify this value in minutes.

Show System Update Progress Select **On**, to enable the user to view the system update progress. A notification message is displayed in the Windows system tray.

By default, this setting is set to On. If this setting is set to Off, user will not see the system update progress.

Update Watcher Icon You can specify a different icon that displays on the managed device's notification area of the system tray. The path to the file must resolve on the managed device. If the file does not exist, or if the file is not a valid `.ico` file, the default icon displays.

Agent Message Overrides You can provide custom text for Agent System Update messages that display in dialog boxes during the update. Click **Add** to display the Edit Agent System Update Message dialog box. Select a Message Key from the drop-down list, type the desired text, then click **OK**.

You can also remove and edit custom messages that you have created.

The following table lists the available message keys with their description:

Message Key	Description
AWAITING_PERMISSION	A ZENworks update is available.
AWAITING_REBOOT	A system reboot is required to complete the ZENworks Update.
DEBUG	DEBUG: {0}
ERROR_CHECKING_PREREQUISITE	The update was canceled because one or more prerequisites were not met.
ERROR_DELETING_FILE	{0} could not be deleted. Try deleting the file or directory manually and restarting the ZENworks Update.
ERROR_DURING_INSTALL	An unknown error occurred during the ZENworks Update. Please see the system update log for details.
ERROR_MOVING_FILE	{0} could not be renamed. Try renaming the specified file to {0}.bak and restarting the ZENworks Update.
ERROR_MSI_UNAVAILABLE	It appears that another installation is taking place. When it is complete, restart the ZENworks Update.
ERROR_STARTING_PROCESS	{0} could not be started. Try starting the process manually and restarting the ZENworks Update.
ERROR_STARTING_SERVICE	The {0} service could not be started. Try manually starting the service manually and restarting the ZENworks Update.
ERROR_STOPPING_PROCESS	The {0} process could not be stopped. Try exiting all instances of the process and restarting the ZENworks Update.
ERROR_STOPPING_SERVICE	The {0} service could not be stopped. Try stopping the service manually and restarting the ZENworks Update.
ERROR_ZENWORKS_HOME_NOT_DEFINED	The ZENWORKS_HOME variable is not set on the device. This can result in an undesired behavior. Set the environment variable on this device and retry the update.
EXIT	Exit
FINISHED	The ZENworks Update has completed successfully.
FINISHED_WITH_ERROR	The ZENworks Update has completed; however, some errors were encountered during the update. Contact your ZENworks Administrator to resolve this issue.
INSTALLING_PERCENTAGE	{0}% Complete

Message Key	Description
MSI_INSTALL_ERROR	An error occurred while installing {0}. msisec returned {1}.
NO_STATUS_REPORTED	No status has been reported.
PERMISSION_MSG	Select OK to allow the update to start; select Cancel to postpone the update. Note: If no selection is made, the update will begin automatically in {1} minutes.
PERMISSION_MSG_NO_POSTPONES_REMAINING	Select OK to allow the update to start. Note: If no selection is made, the update will begin automatically in {1} minutes.
PERMISSION_MSG_NO_POSTPONES_REMAINING_NO_TIMEOUT	Select OK to allow the update to start.
PERMISSION_MSG_NO_TIMEOUT	Select OK to allow the update to start, or select Cancel to postpone the update.
PERMISSION_MSG_POSTPONES_ONE_REMAINING	You will be allowed {0} more opportunities to postpone the update, then the update will be started.
PERMISSION_TITLE	ZENworks Update Available
REBOOT_CANCELLED	One or more logged on users have canceled the needed reboot. To complete the ZENworks Update, manually restart your system.
REBOOT_MSG	Select OK to allow the reboot now, or select Cancel to abort the reboot. Note: If no selection is made, the reboot will occur automatically in {1} minutes.
REBOOT_MSG_NO_POSTPONES_REMAINING	Select OK to allow the reboot to start. Note: If no selection is made, the update will begin automatically in {1} minutes.
REBOOT_MSG_NO_POSTPONES_REMAINING_NO_TIMEOUT	Select OK to allow the reboot to start.
REBOOT_MSG_NO_TIMEOUT	Select OK to allow the reboot now, or select Cancel to abort the reboot.
REBOOT_MSG_POSTPONES_ONE_REMAINING	You will be allowed {0} more opportunities to postpone the reboot, then the reboot will be started automatically.
REBOOT_MSG_POSTPONES_REMAINING	You will be allowed {0} more opportunities to postpone the reboot, then the reboot will be started automatically.
REBOOT_TITLE	Restart Required

Message Key	Description
RESUME_UPDATE_LATER	If an update is postponed, the update might resume later from the Tray icon. .
SHOW_STATUS	Show Status
SHUTDOWN_ADJUST_FAILED	Unable to get permission to initiate a reboot (error code {0}). Manually restart your system.
SHUTDOWN_INIT_FAILED	A reboot could not be initiated (error code {0}). Restart your system manually.
SHUTDOWN_LUID_FAILED	Unable to get permission to initiate a reboot (error code {0}). Restart your system manually.
SHUTDOWN_MSG	A reboot has been initiated to complete the ZENworks Update.
SHUTDOWN_TOKEN_FAILED	Unable to get permission to initiate a reboot (error code {0}). Restart your system manually.
STATUS_TITLE	ZENworks Update
UNKNOWN	An unknown error occurred during the ZENworks Update. See the system update log for details.
UNKNOWN_STATUS	An unknown status was reported '{0}'
UPDATE_NOT_RUNNING	The ZENworks Update is not running. Contact your ZENworks Administrator to resolve this issue.
WATCHER_ICON_TOOLTIP	ZENworks Update Status

4 Click **OK**.

7.1 ZENworks Updater Service

The ZENworks Updater Service allows you to set a refresh interval to pull down system updates from the Primary Server at a scheduled interval.

7.1.1 Refresh Interval

This setting specifies the interval at which ZENworks Updater Service (ZeUS) gets refreshed. The default refresh interval is set to 6 hours.

You can set a new interval by entering the number of days and hours in the respective fields. The value is limited to 9 days and 23 hours. On refresh, ZeUS pulls down the system updates from the Primary Servers.

The new refresh interval will be effective after ZeUS is refreshed. For example, if you set the interval to 9 hours, ZeUS will refresh after 6 hours according to the existing default interval. However, the next refresh happens after 9 hours according to the new refresh interval. If the refresh interval is set to zero, the default value is considered.

7.1.2 Configuring ZEUS to Communicate Using a Non-Standard Port

ZENworks Updater Service uses port number 80 to communicate with Primary Servers. If a Primary Server has been configured to use a non-standard port, then perform the following steps for ZEUS to communicate using a non-standard port.

This workaround is applicable only for ZENworks 2017 and earlier versions, from ZENworks 2017 Update 1 onwards, a non-standard port is automatically updated to communicate with the agent.

Upgrade Scenario	Action
Upgrading from 11.4.x to 2017	Change the port manually for ZEUS to communicate using a non-standard port. You have to configure the non-standard ports on both servers and agents.
Upgrading from 2017 to 2017 Update 1	Change the port manually for ZEUS to communicate using a non-standard port. You have to configure the non-standard ports on both servers and agents.
Upgrading from Update 1 or later	Non-standard ports are automatically updated to communicate with the agent.

On Servers:

- 1 Back up the `web.xml` file located in the `/opt/novell/zenworks/share/tomcat/webapps/zenworks-ping/WEB-INF/` folder.
- 2 Back up the `zeus.conf` file located in the `ZENWORKS_HOME%\ZeUS\conf` folder.
- 3 In the `zeus.conf` file modify the `#task-notifier-port=80` line.
For example:
`task-notifier-port=88` (if the non-standard port is 88)
- 4 Modify the following content in the `web.xml` file to match that in the `zeus.conf`:

```
<init-param>  
<param-name>com.novell.zenworks.zeus.worktodo.nioport</param-name>  
<param-value>88</param-value>  
</init-param>
```
- 5 After configuring the ports, restart the ZENworksUpdaterService and the ZENworks server.

On Agents:

- 1 Back up the `zeus.conf` file located in the `ZENWORKS_HOME%\ZeUS\conf\zeus.conf` folder.
- 2 Modify the `#task-notifier-port=80` line.
For example:

`task-notifier-port=88` (if the non-standard port is 88)

- 3 Restart the ZENworksUpdaterService, or reboot the agent.

8 Troubleshooting System Updates

The following sections provide solutions to the problems you might encounter while performing a system update:

- ♦ [“ZENworks System Update fails if Oracle DataGuard is Configured” on page 76](#)
- ♦ [“ZENworks Update fails During the Prepare state” on page 76](#)
- ♦ [“An error is Displayed while Logging into the ZENworks Control Center” on page 77](#)
- ♦ [“System Update prepare fails while updating to ZENworks 23.3” on page 77](#)
- ♦ [“An error message is displayed when trying to log in to ZCC after updating to ZENworks 23.3” on page 78](#)
- ♦ [“System Update Fails in an Embedded Postgres Zone” on page 79](#)
- ♦ [“The ZENworks Update Watcher Tooltip Notification is Displayed Even After the System Update is Completed” on page 79](#)
- ♦ [“Deployment of Antimalware Bundle Fails on Windows 11 Pro Device” on page 79](#)
- ♦ [“Update Fails on a Newly Added Server” on page 80](#)
- ♦ [“Agent Update Fails during FDE Package Update” on page 80](#)
- ♦ [“Unable to Update to ZENworks 2020 Update 3, as the System Update Does not Progress” on page 80](#)
- ♦ [“System Update Fails During Prepare-Update” on page 82](#)
- ♦ [“If the update is already configured, the application uses the previously configured port after reimporting the system update” on page 82](#)
- ♦ [“System update fails on a Windows 7 agent” on page 82](#)
- ♦ [“After deploying the PRU, the Device status indicates that the Update has completed even for devices that are switched off, or deleted from the zone.” on page 83](#)
- ♦ [“System update fails on the device” on page 83](#)
- ♦ [“System update hangs” on page 83](#)
- ♦ [“System update of a Windows device fails because the ZENUdater.exe executable crashes” on page 84](#)
- ♦ [“An administrator with System Update Deploy right and device level View Leaf right is unable to create the first stage” on page 84](#)
- ♦ [“Two ZENworks icons are displayed after System update is completed on a Mac Agent” on page 84](#)
- ♦ [“Unable to get updates when you perform the Check For Updates action” on page 85](#)
- ♦ [“http-nio CLOSE_WAIT clear connection default value is set to 1 hour” on page 85](#)
- ♦ [“Permission prompt not getting displayed on Embedded win 7 device” on page 85](#)
- ♦ [“ZeUS service does not working properly when a Satellite Server is demoted and then the device is updated without a reboot” on page 86](#)

- ♦ “The ZENworks services are not restarted on SLES servers after the system update is completed” on page 86
- ♦ “System update fails due to the lack of sufficient disk space” on page 86
- ♦ “Connection fails when the QuickTask was triggered on the 20.2 agent from the 23.x primary server” on page 87
- ♦ “The ZENworks system update fails if JDBC URL does not contain the ‘encrypt’ entry” on page 87

ZENworks System Update fails if Oracle DataGuard is Configured

Source: ZENworks 23.3 and later versions

Explanation: If you are using the Oracle database and configured Oracle DataGuard, while upgrading ZENworks to ZENworks 23.3 or later versions, the system update fails.

Action:

The workaround should be performed only in the following scenarios:

- ♦ When you have configured Oracle DataGuard
- ♦ When you are planning to upgrade to ZENworks 23.3 or later versions
- ♦ When the System Update fails

For the ZENworks database, add the following key “Jdbc_Url” entry in the zdm.xml file:

```
<entry key="Jdbc_Url">JDBC URL HERE</entry>
```

- ♦ On Windows: %ZENSERVER_HOME%/conf/datamodel/zdm.xml
- ♦ On Linux: /etc/opt/microfocus/zenworks/datamodel/zdm.xml

For the Audit database, add the following entry in the zenaudit.xml file:

```
<entry key="Jdbc_Url">JDBC URL HERE</entry>
```

- ♦ On Windows: %ZENSERVER_HOME%/conf/datamodel/zenaudit.xml
- ♦ On Linux: /etc/opt/microfocus/zenworks/datamodel/zenaudit.xml

NOTE: Replace the JDBC URL HERE with the actual JDBC URL. The URL can be copied from the existing JdbcUrl key if configured.

After performing the above steps, restart all the ZENworks services by running the `microfocus-zenworks-configure -c Start` command.

ZENworks Update fails During the Prepare state

Source: ZENworks 23.3 and ZENworks 23.4

Explanation: If you are using an SQL Server database with dynamic ports enabled and have both Port and Named Instance configured in ZENworks, then during or after the upgrade connection to the database might fail.

Action:

Perform the following steps:

1. Remove the <Port> key entry from `zdm.xml` and `zenaudit.xml` files.

- ♦ On Windows: `%ZENSERVER_HOME%\conf\datamodel`
- ♦ On Linux: `/etc/opt/microfocus/zenworks/datamodel`

2. If this key exists, remove the port from `jdbc_url`.

Example: `<Jdbc_Url> jdbc:sqlserver://sk-drdb01.epm.blr.novell.com:1433;databaseName=zenworksconfig;encrypt=false;instanceName=FTPDB</Jdbc_Url>`

After performing the above steps, restart all the ZENworks services using `microfocus-zenworks-configure -c Start`.

An error is Displayed while Logging into the ZENworks Control Center

Source: ZENworks 23.3

Explanation: While logging into the ZENworks Control Center, the following error is displayed:

500 Error Internal server error occurred. For error messages and additional information refer to API Gateway logs.

The following error is logged in the `api-gateway-spring-framework.log` file:

java.security.cert.CertificateException: No subject alternative DNS name matching found.

at sun.security.util.HostnameChecker.matchDNS(HostnameChecker.java:212) ~[?:?]

at sun.security.util.HostnameChecker.match(HostnameChecker.java:103) ~[?:?]

The `api-gateway-spring-framework.log` file is available in the following location:

- ♦ On Linux: `/var/opt/microfocus/log/zenworks/api-gateway`
- ♦ On Windows: `%ZENSERVER_HOME%\logs\api-gateway`

Possible Cause: This error might be logged when the hostname that is being used to connect does not match with the SAN (Subject Alternative Name) in the certificate.

Action: Remint the server certificate to include the hostname in the SAN.

System Update prepare fails while updating to ZENworks 23.3

Source: ZENworks 23.3

Explanation: While updating to ZENworks 23.3, the prepare stage might fail. Check the prepare-update.log file and the following message is logged:

```
"/opt/microfocus/zenworks/bin/run_preglobal_update:: OUT: Caused by:
org.springframework.web.client.HttpClientErrorException$UnsupportedMediaT
ype: 415 Unsupported Media Type: ({'timestamp':'2023-10-
02T16:46:47.915+00:00','status':415,'error':'Unsupported Media
Type','message':'','path':'/rest/get-zeus-version'}) [] [] [SystemUpdate]"
```

NOTE: The following workaround is applicable only if prepare fails with the above message logged in the prepare-update.log file.

Action: Manually upgrade the ZeUS RPM by running the following command as a root user and can be performed from anywhere on the server. Ensure that you run this command on all the servers where prepare fails with the above-mentioned error log message.

```
rpm -Uvh /var/opt/microfocus/zenworks/content-repo/system-
update/5023030000fc50000000002023072812/rpm/novell-
zenworks-updater-service-server-23.3.0-333.noarch.rpm
```

After running the command, restart ZeUS by running `systemctl restart novell-zenworks-updater-service`.

The Prepare stage runs every 20 minutes. Hence, after running this command, within 20 minutes the Prepare System Update stage will be re-initiated automatically.

An error message is displayed when trying to log in to ZCC after updating to ZENworks 23.3

Explanation: After updating to ZENworks 23.3, the ZCC login page might display the following error:

This page contains the following errors:

error on line 1 at column 1: Document is empty

Below is a rendering of the page up to the first error.

Possible Cause: This issue occurs when the Primary Server has multiple NICs (multiple IP addresses) and one of them is down and the ZENworks API Gateway service resolves the hostname to the IP address or NIC that is down and results in a 503 SERVICE_UNAVAILABLE error.

The below error is displayed in the log file:

```
[DEBUG] [2023-06-20 10:23:42] [reactor-http-epoll-6] [7]
[Api-Gateway] [39] [AbstractErrorWebExceptionHandler]
[[a61378b8-146] Resolved [AnnotatedConnectException:
finishConnect(..) failed: No route to host: <IP address>]
for HTTP POST /zenworks-location/]
```

```
[DEBUG] [2023-06-20 10:23:42] [reactor-http-epoll-6] [7]
[Api-Gateway] [39] [CharSequenceEncoder] [[a61378b8-146]
Writing "finishConnect(..) failed: No route to host: <IP
address>" ]
```

The log file is available in the following location:

- ♦ **Windows:** %ZENSERVER_HOME%\log\zenworks\api-gateway\api-gateway-spring-framework.log
- ♦ **Linux:** /var/opt/microfocus/log/zenworks/api-gateway/api-gateway-spring-framework.log

Action: Ensure the hostname resolves to a valid IP address and restart the ZENworks API Gateway service.

System Update Fails in an Embedded Postgres Zone

Source: ZENworks 2020 Update 3

Explanation: When an administrator deploys the system update to all Primary Servers at same time for an embedded Postgres zone, the system update fails on the other servers that do not have database.

Action: For an embedded Postgres zone, first update the Primary Server that has the database. Once the Primary Server with the database is updated, then update the other servers.

The ZENworks Update Watcher Tooltip Notification is Displayed Even After the System Update is Completed

Source: ZENworks 23.3

Explanation: While updating ZENworks 23.3 System Update on Windows Server 2019, the ZENworks Restart Required prompt is displayed even when the ZENworks Update Watcher tooltip notification displays that the system update is in progress.

Action: If the reboot prompt is displayed, ignore the progress displayed in the Update Watcher tooltip notification as the update is completed and proceed with the reboot.

Deployment of Antimalware Bundle Fails on Windows 11 Pro Device

Source: ZENworks 23.3

Explanation: The deployment of Antimalware bundle fails on the Windows 11 Pro device as the OS version mapping information was missing on the Primary Servers in the zone.

Action: Add the missing entries in `windowsVersionMapping.properties` on the Primary Server, and then run the following configure action:

```
microfocus-zenworks-configure -c SettingsConfigureAction -
Dtype=CustomOSTarget -Dadd
```

To add the missing entries, see [Adding an entry in the windowsVersionMapping](#)

Update Fails on a Newly Added Server

Source: ZENworks 2020 Update 2 and ZENworks 2020 Update 3

Explanation: When you add a new Primary Server that is on ZENworks 2020 Update 2 to a ZENworks 2020 Update 3 baselined zone, the update fails on the newly added server, and the following message is logged in the system-update.log file:

Failed to download content.Content download failed for content guid

Action: Reassign the update.

Agent Update Fails during FDE Package Update

Source: ZENworks Agent, ZENworks 2020 Update 3

Possible Cause: While updating to ZENworks 2020 Update 3 on agents, if FDE and BitLocker are enabled, then the agent update fails.

Action: If FDE is enabled or the product license is active, then the BitLocker should be disabled, else the system update fails.

Unable to Update to ZENworks 2020 Update 3, as the System Update Does not Progress

Explanation: If you have enabled ZENworks Patch Management and updating to ZENworks 2020 Update 3, the update does not progress as some of the Patch Policies have DaysToRebuild set to 0.

Action: Perform the following steps:

1. Kill the processes that are executing the configure actions and ensure that the system update is in the failed state:

On Linux Primary Server:

- a. Open the terminal and run the following commands:
- b. `ps -aux | grep 'ConfigureLoader'`
After running the command, note down the Process ID (PID)
- c. `kill <PID>`

On Windows Primary Server: Open the Task Manager, check and end all the running java.exe processes.

2. After the System Update is in the failure state, run the following query to update the database:


```

UPDATE zbundle SET serversidedata =
replace(serversidedata, '<Variables><ns2:Name
xmlns="http://novell.com/zenworks/datamodel/objects/
settings" xmlns:ns2="http://novell.com/zenworks/
datamodel/objects/settings">RebuildSchedule</
ns2:Name><ns2:Value xmlns="http://novell.com/zenworks/
datamodel/objects/settings" xmlns:ns2="http://
novell.com/zenworks/datamodel/objects/
settings">&lt;Schedule xmlns=&quot;http://
www.novell.com/ZENworks/v1.0&quot;
xmlns:xsi=&quot;http://www.w3.org/2001/XMLSchema-
instance&quot; xsi:schemaLocation=&quot;http://
www.novell.com/ZENworks/
v1.0&quot;&gt;&lt;IntervalSchedule&gt;&lt;RepeatFrequen
cy Months=&quot;0&quot; Weeks=&quot;0&quot;
Days=&quot;0&quot; Hours=&quot;0&quot;
Minutes=&quot;0&quot; Seconds=&quot;0&quot;','
'<Variables><ns2:Name xmlns="http://novell.com/
zenworks/datamodel/objects/settings" xmlns:ns2="http://
novell.com/zenworks/datamodel/objects/
settings">RebuildSchedule</ns2:Name><ns2:Value
xmlns="http://novell.com/zenworks/datamodel/objects/
settings" xmlns:ns2="http://novell.com/zenworks/
datamodel/objects/settings">&lt;Schedule
xmlns=&quot;http://www.novell.com/ZENworks/v1.0&quot;
xmlns:xsi=&quot;http://www.w3.org/2001/XMLSchema-
instance&quot; xsi:schemaLocation=&quot;http://
www.novell.com/ZENworks/
v1.0&quot;&gt;&lt;IntervalSchedule&gt;&lt;RepeatFrequen
cy Months=&quot;0&quot; Weeks=&quot;0&quot;
Days=&quot;120&quot; Hours=&quot;0&quot;
Minutes=&quot;0&quot; Seconds=&quot;0&quot;')
WHERE zuid IN (
    SELECT zuid
    FROM zzenobject
    WHERE path LIKE '%ZPM/Policy%'
    AND primarytype = 'Bundle'
    AND subtype LIKE '%Patch Bundle%'
    AND serversidedata LIKE
'%<Variables><ns2:Name xmlns="http://novell.com/
zenworks/datamodel/objects/settings" xmlns:ns2="http://
novell.com/zenworks/datamodel/objects/
settings">RebuildSchedule</ns2:Name><ns2:Value
xmlns="http://novell.com/zenworks/datamodel/objects/
settings" xmlns:ns2="http://novell.com/zenworks/
datamodel/objects/settings">&lt;Schedule
xmlns=&quot;http://www.novell.com/ZENworks/v1.0&quot;
xmlns:xsi=&quot;http://www.w3.org/2001/XMLSchema-
instance&quot; xsi:schemaLocation=&quot;http://
www.novell.com/ZENworks/
v1.0&quot;&gt;&lt;IntervalSchedule&gt;&lt;RepeatFrequen
cy Months=&quot;0&quot; Weeks=&quot;0&quot;
Days=&quot;0&quot; Hours=&quot;0&quot;
Minutes=&quot;0&quot; Seconds=&quot;0&quot;%'
    )

```

NOTE: In the above query, as an example **120** is used. However, the number can be increased if you do not want the Patch Policy to be rebuilt soon. The number 120 represents the days to rebuild the patch policy.

3. After running the query, rerun the system update.

System Update Fails During Prepare-Update

- Explanation:** During the prepare-update state, the ZENworks Updater Service (ZeUS) failed to download content on a primary server
- Possible Cause:** This issue occurred because an attempt to download the system update was made while the server was getting restarted.
- Action:** Run the `zac zeus-ref` command to retrieve the system update or wait for the next interval at which ZENworks Updater Service (ZeUS) gets refreshed. The default refresh interval is set to 6 hours.

If the update is already configured, the application uses the previously configured port after reimporting the system update

- Explanation:** After configuring an update, if the system update is deleted and reimported, the application uses the previously configured port, and the status of the update is displayed as **Ready to Deploy**, instead of **Awaiting Configuration**.
- Action:** To modify the previously configured port, in the **Configuration > System Updates** page, click **Action** and choose **Configure Update**.

System update fails on a Windows 7 agent

- Explanation:** When system update fails on a Windows 7 agent, repair or uninstall actions cannot be performed.

Following is one of the examples of the error log message in the system-update.log file:

```
"[ZENUpdater] [] [SYSTEM] [SystemUpdate] [MSI_INSTALL_ERROR] [ERROR]
[${content.0},1612] [] [] [ZENworks]"
```

Where 1612 is the MSI package is missing from the windows MSI cache.

- Action:** Perform the following:

1. Identify the package or product code for which the error is displayed.

For example, the above mentioned error 1612 is the error code for "Uninstalling {A408EF7C-6671-43EC-851A-385F1D87E847}"

2. Run `wmic product get /format:csv > Software_%Computername%.csv`

Open the file and search for the package or product code. The code should point to the path in the Windows, where the MSI copy should be present.

NOTE: The actual MSI and cached MSI will have different names.

The generic path of the file is %windir%/installer/{random_name}.msi

3. Retrieve the corresponding package from the server. The WMI command provides the actual package name. Copy the package to the agent in the cached path, and rename the file same as the name mentioned in the WMI command, which was retrieved in Step 2.
4. Reassign the update to the device.

After deploying the PRU, the Device status indicates that the Update has completed even for devices that are switched off, or deleted from the zone.

Source: ZENworks, Asset Management

Explanation: When you deploy the PRU (Product Recognition Update) and then check the update status, the Update Completed status is displayed even for devices that are switched off or deleted from the zone.

Action: To view the PRU status of devices:

- 1 Click **Bundles** in ZENworks Control Center.
- 2 The **Bundles** page is displayed, append &uid=/system to the URL of the Bundles page, system bundles are displayed.
Example: `https://ipaddress/zenworks/jsp/index.jsp?pageid=bundleList&uid=/system`
- 3 In the Bundles page, click the **System Bundles** link.
- 4 In the **System Bundles** page, click the required Knowledge Base file.
- 5 In the **Bundle Status** panel of the **Knowledge Base** page, click the **here** link to view the PRU system update status.

The PRU is passed to the managed device through a bundle. The Bundle Status panel displays the device and user count against the related deployment status.

System update fails on the device

Source: ZENworks, System Update

Possible Cause: Some antiviruses may interfere with the ZENworks Endpoint Security Management installer, resulting in a system update failure of the ZENworks Agent.

Action: Refer to your antivirus documentation and make the required configuration changes to allow exclusions, prior to deploying the system update.

For more information, see [TID 7007545 \(http://www.novell.com/support/\)](http://www.novell.com/support/)

System update hangs

Source: ZENworks, System Update

Explanation: While importing the system update into the Zone, if the database restarts, the download progress gets stuck.

Possible Cause: During the download process, the ZENworks Loader module downloads the update and updates the database with information related to the download progress. ZENworks Control Center reads this information from the database and displays the download progress. If the database restarts in between, the communication between the ZENworks Control Center Service, the Loader module, and the database is interrupted. If the download is still in progress when the database restarts, the download status gets stuck.

Action: Cancel the download which is in progress and re-initiate it again.

OR

Delete the update and download it again.

System update of a Windows device fails because the ZENUpdater.exe executable crashes

Source: ZENworks, System Update

Explanation: During the system update of a Windows device, the ZENUpdater.exe executable crashes, and the system update fails.

Possible Cause: The ZENUpdater crashes because the .NET 4.0 framework has not been installed successfully.

Action: Verify that the .NET 4.0 framework is properly installed on the device. Re-install the .NET 4.0 framework if necessary. Restart ZENUpdater.

An administrator with System Update Deploy right and device level View Leaf right is unable to create the first stage

Source: ZENworks, System Update

Explanation: In ZENworks Control Center, the administrator with System Update Deploy right and device level View Leaf right on the entire zone is unable to create the first stage.

Action: The administrator with System Update Deploy right and device level View Leaf right on the entire zone should create a stage only after the super administrator has created the first stage.

Two ZENworks icons are displayed after System update is completed on a Mac Agent

Source: ZENworks, System Update

Explanation: After System update is completed, two ZENworks icons are displayed on a Mac agent.

Action: You must re-login or restart the device.

Unable to get updates when you perform the Check For Updates action

Source: ZENworks, System Update

Explanation: In ZENworks Control Center when you perform the **Check For Updates** action, there might be a failure.

Possible Cause: The Novell Customer Center (NCC) server displays a warning that the system update entitlement has expired even when that is not the case.

Action: Initiate the Check for Updates process in the background.

- ♦ Click **OK** in the Retry Check for Updates dialog when you are prompted to initiate the **Check For Updates** process in the background. For more information, see the [Section 2.2.2, “Manually Checking for Updates,” on page 25](#).

The check for updates process, which is initiated in the background, uses the values configured for the following fields in the `SUEntitlementConf.properties` file:

- ♦ **retryCount-CheckForUpdates**
- ♦ **sleepInterval-CheckForUpdates**

http-nio CLOSE_WAIT clear connection default value is set to 1 hour

Source: ZENworks, System Update

Possible Cause: On a 11 SP4 ZENworks Server, the agent ZeUS service opens a single http-nio connection with port 80. This connection will continue to be in CLOSE_WAIT state on the server even after agent ZeUS service is stopped.

Explanation: This behavior is normal as the default close time for this connection is set to a maximum of one hour. The default value of the ZeUS configurable parameter, `notifier-socket-timeout`, is set to 3600000. The parameter is available in the `\ZeUS\Conf\zeus.conf` configuration file and the default value of the parameter can be configured between 5 minutes and 1 hour.

Action: On the servers, you will see many such connections opened from multiple devices in the zone. You can ignore these CLOSE_WAIT connections as they will be cleaned up in an hour. The maximum number of connections that can be opened to this http-nio port is 20000.

Permission prompt not getting displayed on Embedded win 7 device

Source: ZENworks, System Update

Possible Cause: This is the default behavior of Windows 7 embedded device.

Explanation: The default behavior of Windows 7 embedded device could not be changed from ZENworks as MessageBox API provided by user32.dll is used.

Action: In the Windows registry, set the value of the `Enabling Default Reply` registry key to 0. This will disable the auto reply on prompts. The folder path of the registry key is `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\`. For more information, refer to the [MSDN solution](#).

ZeUS service does not working properly when a Satellite Server is demoted and then the device is updated without a reboot

Source: ZENworks, System Update

Explanation: When you demote a Satellite Server and then update the device without performing a reboot, the ZeUS service will not work properly because the `rt.jar` file is missing.

Action: Run the `msiexec -i <filePath> TARGETDIR="<default agent installation path>" REBOOT=ReallySuppress ALLUSERS=1 /lvx*+ <log_file_path> " /qn` command to generate the `rt.jar` file again.

In this command:

- ♦ `<filePath>` is the location of the `novell-zenworks-jre` msi file.
- ♦ `<default agent installation path>` is the location where the agent is installed.
- ♦ `<log_file_path>` is the location where you want to create the log file.

Example: `msiexec -i "C:\Program Files (x86)\Novell\ZENworks\cache\zmd\ZenCache\fb739230-e0de-4460-a2d2-cc1dfelb4613\novell-zenworks-jre-1.7.0_80.x86_64.msi" TARGETDIR="C:\Program Files (x86)" REBOOT=ReallySuppress ALLUSERS=1 /lvx*+ "C:\Program Files (x86)\Novell\ZENworks\logs\system-update\5011040000fc50000000002015061004\novell-zenworks-jre-1.7.0_80.x86_64.msi.log" /qn`

The ZENworks services are not restarted on SLES servers after the system update is completed

Source: ZENworks, System Update

Explanation: On SLES servers, after performing a system update the ZENworks services are not restarted automatically. Even if you manually restart the services, they stop after a couple of minutes.

Action: Restart ZeUS.

System update fails due to the lack of sufficient disk space

Source: ZENworks, System Update

Explanation: The previous zone update or upgrade has created `.superceded` files to ensure compatibility with older versions of the ZENworks Agent. However, these files are not required in the following scenarios:

- ♦ The zone is baslined.
- ♦ There are no installations of older versions of the ZENworks Agent in the zone.

The system update might fail if the disk is completely utilized by the `.superceded` files that are available in the following location:

- ♦ **On Window:** %ZENWORKS_HOME%\install\downloads
- ♦ **On Linux:** /opt/novell/zenworks/install/downloads

Action: Baseline the zone, or delete the superceded files or refer to TID 7012095 in [Micro Focus knowledgebase](#) to delete the superceded files.

Connection fails when the QuickTask was triggered on the 20.2 agent from the 23.x primary server

Explanation: In the ZENworks 2020 Update 3, modifications were made to allow the QuickTask notification to use Apache ZooKeeper. To enable TTL-based nodes, the `extendedTypesEnabled` property is set to `true` in ZooKeeper during the system update. In a three-node ZooKeeper cluster, the `extendedTypesEnabled` property was enabled on a ZooKeeper node but failed on the other two nodes.

When the ZooKeeper connection was established with other nodes in the cluster, the QuickTask handler fails to create a node and the QuickTask notification also fails.

NOTE: This troubleshooting scenario is applicable only if you are updating from ZENworks 2020 Update 2 to ZENworks 23.3.

Action: Update all the nodes in the ZooKeeper cluster to ZENworks Update 3 or 23.x for QuickTask to work.

The ZENworks system update fails if JDBC URL does not contain the 'encrypt' entry

Explanation: In ZENworks 2020 Update 3, if are using an MS SQL Server database with a customized JDBC URL the update to ZENworks 23.3 fails while executing the `UpdateServicePathChangesConfigureAction` as it tries to make a JDBC connection.

Action: Prior to updating to ZENworks 23.3, you should modify the customized JDBC URL before applying the update to avoid system update failure. After modifying the JDBC URL, rerun the failed update on all primary servers.

In the `zdm.xml` and `zenaudit.xml` file located in path mentioned below, add `encrypt=false` to the existing entry key `JdbcUrl`.

```
<entry key="JdbcUrl">JDBC URL HERE;encrypt=false</entry>
```

Path of the `zdm.xml` for ZENworks database:

- ♦ On Windows: %ZENSERVER_HOME%\conf/datamodel/zdm.xml
- ♦ On Linux: /etc/opt/microfocus/zenworks/datamodel/zdm.xml

Path of the `zenaudit.xml` for Audit database:

- ♦ On Windows: `%ZENSERVER_HOME%/conf/datamodel/zenaudit.xml`
- ♦ On Linux: `/etc/opt/microfocus/zenworks/datamodel/zenaudit.xml`