

ZENworks Patch Management Airgap Solution

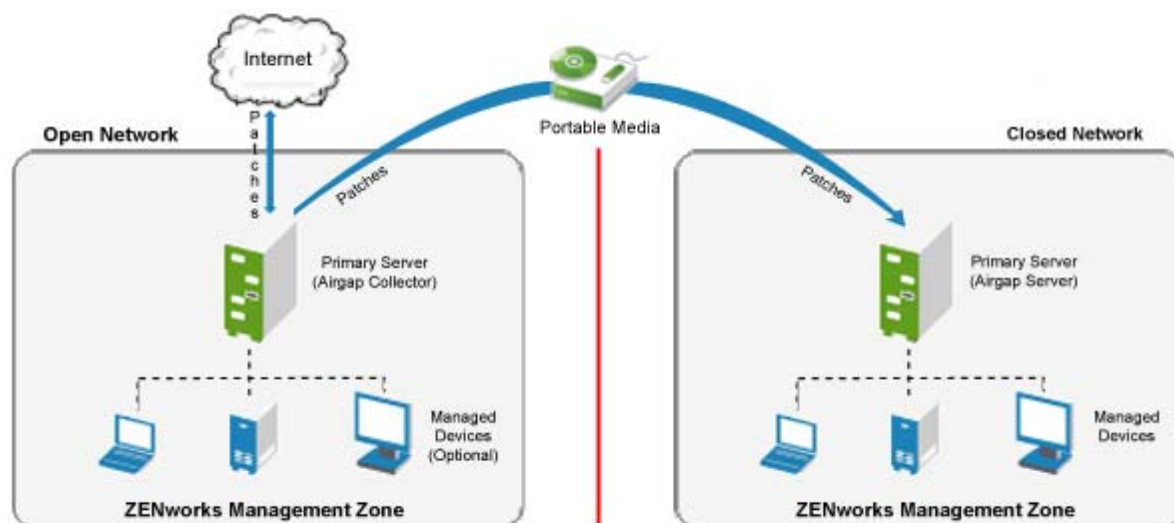
August 2023

The Airgap solution for ZENworks Patch Management enables you to deliver patches to networks that are disconnected and isolated from the Internet. These networks are referred to as “airgapped” or “closed” networks.

NOTE: Airgap supports Microsoft Windows patches, not including Microsoft Office 365. Airgap does not currently support patches for Linux distributions or Mac operating systems.

About the Airgap Solution

The Airgap solution requires two ZENworks Management Zones, one zone in the open (Internet-connected) network and one in the closed network. A Primary Server (OCM) (referred to as the Airgap Collector) in the open zone receives patches by running the Maintenance Schedule (Configuration > Management Zone Settings > Security > Patch Server Configuration). You then transfer the patches via portable media from the Airgap Collector to a Primary Server (referred to as the Airgap Server) in the closed zone. The patch agent installed on device analyzes the device to determine what patches it needs, downloads the patches on-demand through ZENworks content system and then applies the patch based on the established patching schedule. For more information, see [Patch Management Overview](#) in the [ZENworks Patch Management Reference](#).



The ZENworks Management Zone in your open network should include managed devices that you want to patch. The patches downloaded by the Airgap Collector are retained in the zone (in addition to being copied to a transfer directory) and can be deployed to managed devices within the open zone.

IMPORTANT: The CVE data cannot be imported from an Open Zone to an Airgapped Zone. Hence, the security dashboard will not be populated with any CVE information.

Prerequisites

- ♦ Two ZENworks Management Zones, one in the open network (*the Airgap Collector*) and another in the closed network (*the Airgap Server*).

ZENworks Servers must be 23.3 or later versions. For information about installing ZENworks, see the [ZENworks Server Installation](#).

- ♦ ZENworks Patch Management licensed in both zones, which includes a ZENworks Patch Management license for the Airgap Collector (open zone) and the Airgap Server (closed zone).

Migrating the Management Zone with Airgap

If you are using the Airgap solution in ZENworks 2020 Update 2 and have not upgraded to ZENworks 2020 Update 3, as the Advanced Patch Feed in ZENworks 2020 Update 3 did not support the Airgap solution, then you can upgrade your Airgap zone to ZENworks 23.3. Refer to the following sections to migrate to the Advanced Patch Feed.

Identifying an Airgap collector zone: In ZENworks 2020 Update 2 zone, open ZENworks Control Center, go to [Configuration > Management Zone Settings > Device Management > System Variables](#). If the System Variables panel includes the PATCH_AIRGAP_COLLECTOR variable and the value is set as true, then the zone is an Airgap collector zone.

Identifying an Airgap server zone: In ZENworks 2020 Update 2 zone, open ZENworks Control Center, go to [Configuration > Management Zone Settings > Device Management > System Variables](#). If the System Variables panel includes the PATCH_AIRGAP_SERVER variable and the value is set as true, then the zone is an Airgap zone.

IMPORTANT: The migration procedure remains the same for both Collector and Server zones.

Migrating the Airgap Zones

You need to migrate both zones to the Advanced Patch Feed. To migrate the zones, perform the following steps in each of the zones:

NOTE: The Patch Subscription Service Settings page and, by extension, the Migrate ZENworks Patch Management option are only applicable to ZENworks environments where ZENworks Patch Management was activated and configured before updating to ZENworks 23.3. If it was not activated and configured before the update, the zone is already set to use the new Advanced Patch Feed and no migration is necessary. In this case, skip to the [Setting Up the Open Zone](#) or [Setting Up the Closed Zone](#) section below.

1. After updating your zone to ZENworks 23.3, open ZENworks Control Center, go to [Configuration > Management Zone Settings > Security > Patch Subscription Service Settings](#).

2. In the Patch Subscription Service Settings page, click **Migrate ZENworks Patch Management**.
3. Respond to the prompts provided in the Patch Migration wizard.

You will have options to remove all data or remove all data except Patch policies and configuration settings.

Once the migration is complete, changes will reflect in the Getting Started page for Mitigating Vulnerabilities, in the Patch Server configuration options under Security, and in the Patch Remediation Wizard. You will then need to select the links for the unconfigured options in the Enable Patch Management section of the Getting Started page to start the Patch Service and to select a Patch Server. Unconfigured settings are indicated by the red icon appendage.

After successful migration, the `PATCH_AIRGAP_SERVER` variable will be renamed to `AIRGAP_SERVER` in the closed (Airgap) zone and the `PATCH_AIRGAP_COLLECTOR` variable to `AIRGAP_COLLECTOR` in the open (Airgap Collector) zone.

Setting Up the Open Zone

The tasks required to configure the ZENworks Management Zone in your open network are described in the following sections.

Mirroring the Closed Zone's Managed Devices

When a ZENworks Primary Server downloads patches ondemand, it downloads the patch fingerprints, not the entire patch. A patch fingerprint contains metadata about which operating systems the patch applies to. The Primary Server compares the downloaded patch fingerprints against the operating systems of the zone's managed devices and displays the applicable patches in the Patches list. You can then select the patches you want to cache to the Primary Server for distribution to your managed devices.

If possible, we recommend that you register devices in your open zone that mirror the operating systems of the closed zone's managed devices. This limits the Patches list to only those patches that are applicable for your closed zone's devices.

If you choose to mirror your closed zone's devices in your open zone, consider the following guidelines:

- ♦ In your closed zone, log in to ZENworks Control Center and review the Devices list. The list displays the operating system for each registered device.
- ♦ In your open zone, register devices that have the same operating systems as the ones displayed in your closed zone's Devices list.
- ♦ Registering a device in your open zone adds the device object to the zone. The device object is what is needed to automatically filter the Patches list to show applicable patches only.

Enabling the Airgap Collector

You can enable the Airgap Collector zone by adding a `AIRGAP_COLLECTOR=true` system variable to your ZENworks zone.

NOTE: Add the system variable only if you configuring the Airgap zone for the first time.

- 1 Log in to ZENworks Control Center for the zone in your open network.

- 2 Click **Configuration > Device Management** (in the **Management Zone Settings** panel) > **System Variables** to display the System Variables list.



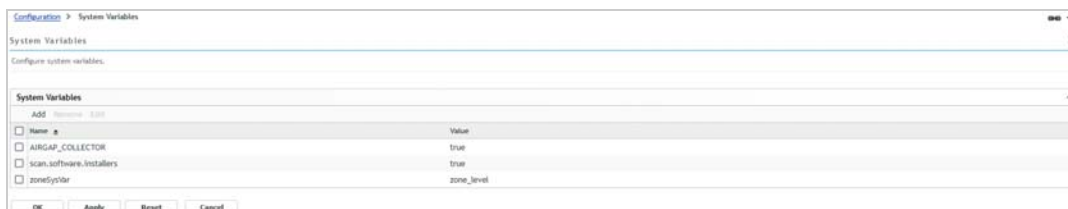
- 3 Click **Add** to display the Add Variable dialog box.

- 4 Fill in the following fields:

Name: AIRGAP_COLLECTOR

Value: true

- 5 Click **OK** to add the variable to the list.




- 6 Click **OK** to save the list.

- 7 Go to **Configuration > Server Hierarchy**.

- 8 In the Server Hierarchy panel, select an Ondemand Content Master (indicated by a cloud icon), click **Action**, and then select the **Set as Airgap Collector Ondemand Content Master** option.



NOTE: The **Set as Airgap Collector Ondemand Content Master** will be disabled if you select a Primary Server with an older ZENworks version (ZENworks 2020 Update 3 or earlier).

The Airgap Collector Ondemand Content Master is indicated by .

- 9 Optionally, you can set a schedule when the Airgap Ondemand Content Master should export patch data to the Airgap folder.

For more information, see [“Export Schedule for Patch Content”](#) on page 7.

Setting Up the Closed Zone

In your closed network, you need to configure the ZENworks Management Zone to enable the Primary Server to act as an Airgap Server. When you transfer downloaded patches from your open network to the closed network, the Airgap Server pulls them into the ZENworks Management Zone as if it had downloaded ondemand. You then deliver the patches using the standard ZENworks Patch Management methods.

- 1 Log in to ZENworks Control Center for the zone in your closed network.
- 2 Enable the Airgap Server by adding several system variables:
 - 2a Click **Configuration > Device Management** (in the **Management Zone Settings** panel) > **System Variables** to display the System Variables list.
 - 2b Click **Add** to display the Add Variable dialog box.
 - 2c Fill in the following fields:
Name: AIRGAP_SERVER
Value: true
 - 2d Click **OK** to save the list.

NOTE: Add the system variable only if you are configuring the zone for the first time.

- 3 In ZCC, go to Configuration > Server Hierarchy.
- 4 In the Server Hierarchy panel, select an Ondemand Content Master (indicated by ) , click **Action**, and then select the **Set as Airgap Ondemand Content Master** option.



NOTE: The **Set as Airgap Ondemand Content Master** will be disabled if you select a Primary Server with older an ZENworks version (ZENworks 2020 Update 3 or earlier).

The Airgap Ondemand Content Master is indicated by .

- 5 Optionally, you can set a schedule when the Airgap Ondemand Content Master should import patch data from the Airgap folder.

For more information, see [“Import Schedule for Patch Content”](#) on page 7.

Important Point to Remember

- ♦ In a zone, both AIRGAP_SERVER and AIRGAP_COLLECTOR system variables should not be set to true. In such conditions, you might not get the expected results.

Transferring Patches from the Open Zone to the Closed Zone

To transfer patches from the open zone to the closed zone:

1 On the Airgap Collector in the open zone:

- 1a** In ZCC, click **Configuration > Security** (in the **Management Zone Settings** panel) > **Patch Server Configuration** to display the Maintenance Schedule panel. Click the **Run Maintenance Now** button to start the maintenance schedule tasks, which create DAU bundle and generate email notifications about the new patches that are available.

When a new DAU bundle is assigned and installed on a device, new patches will be reported to the server. Use the Patch Dashboard (**Security > Dashboard** tab) to monitor the status of the patch update.

- 1b** Pre-fetch patch content all patches that you want to copy. To do so, click **Security > Patches** to display the patch list. Select the patches you want to pre-fetch, click **Actions > Pre-fetch Patch Content**.

If you chose not to mirror your closed zone's devices in your open zone (see [Mirroring the Closed Zone's Managed Devices](#)), the **Patches** list does not display any applicable patches. In this case, you can get the patches list by running the `zac ps --generate-metadata-for-all-patches` on a Windows agent. Use this list to select the patches you want to pre-fetch. You will also need to do this if you mirrored some but not all of your closed zone's devices.

- 1c** After pre-fetching the selected patches is complete, click **Run Export Now** in the Airgap Content Schedule, to get the data immediately.

- 1d** Copy all contents (files and folders) from the following folder to your portable media:

- ♦ On Windows: `%ZENSERVER_HOME%\work\common\airgap\`
- ♦ On Linux/Appliance: `/var/opt/microfocus/zenworks/common/airgap`

2 On the Airgap Server in the closed zone, copy the patch content from the portable media to the following Airgap directory:

- ♦ On Windows: `%ZENSERVER_HOME%\work\common\airgap\`
- ♦ On Linux/Appliance: `/var/opt/microfocus/zenworks/common/airgap`

If you have previously copied patch content to the Airgap Server, do not remove that content. Add the new patch content to the existing content.

3 Log in to ZENworks Control Center for the Airgap Server zone (in your closed network).

4 To get the data immediately, click **Run Import Now** in the Airgap Content Schedule.

5 Click **Configuration > Security** (in the **Management Zone Settings** panel) > **Patch Server Configuration > Run Maintenance Now** to create the DAU bundle.

6 After the maintenance task completes, wait for the devices to report the applicable patches. After patches are reported, go to the Patches tab (**Security > Patches** tab) to check the device patched status for each patch.

7 Deploy the patches. If necessary, see the [ZENworks Patch Management Reference](#).

Airgap Content Schedule

In the Airgap Content Schedule page, you can set a schedule for when the Airgap Ondemand Content Master should import/export patch data from the Airgap folder.

Based on the System Variable (AIRGAP_COLLECTOR or AIRGAP_SERVER) that you have set in your zone, Export Schedule for Patch Content or Import Schedule for Patch Content is displayed.

- ♦ [“Export Schedule for Patch Content” on page 7](#)
- ♦ [“Import Schedule for Patch Content” on page 7](#)

Export Schedule for Patch Content

In the Export Schedule for Patch Content panel, you can set a schedule for when the Airgap Ondemand Content Master should export patch data to the Airgap folder.

1. In ZCC, click Configuration > Security (Management Zone Settings) > Airgap Content Schedule.
2. The export interval can be set to Hourly or Daily.
 - ♦ If the export interval is set Hourly, then you need to select an interval (H) after which the export should be initiated.
 - ♦ If the export interval is set Daily (24 Hour Time Format - Hours: Minutes), then select the time at which the export will be initiated. By default, the export schedule is set at 2:00 A.M.

If required, you can click Run Export Now to initiate the export immediately.

In this page, you can also view the last export status.

- ♦ Last Export Successfully Run at: Displays the date and time when the last export was successful.
- ♦ Export Status: Displays the status of the export.

Import Schedule for Patch Content

In the Import Schedule for Patch Content panel, you can set a schedule for when the Airgap Ondemand Content Master should import patch data from the Airgap folder.

1. In ZCC, click Configuration > Security (Management Zone Settings) > Airgap Content Schedule.

2. The import interval can be set to Hourly or Daily.
 - ♦ If the import interval is set Hourly, then by default the import will be initiated every 2 hours. If required, the import schedule (H) can be modified.
 - ♦ If the import interval is set Daily, then you need to select a time (24 Hour Time Format - Hours: Minutes) when the import should be initiated.

If required, you can click Run Import Now to initiate the export immediately.

In this page, you can also view the last export status.

- ♦ Last Import Successfully Run at: Displays the date and time when the last import was successful.
- ♦ Import Status: Displays the status of the import.

NOTE: If the Airgap status (import/export) is partial success or failure, then a link is displayed. Click the link to view the reason.

Partial Success: The status is partial only if a few files are copied.

Failure: The status is failure when none of the files are copied.

Troubleshooting

Unable to Re-initiate the External Communication After Removing Airgap Solution

If you have configured the Airgap solution (AIRGAP_SERVER) on an OCM server and remove the Airgap solution. After removing the Airgap solution, unable to reinitiate the external communication.

Workaround: After removing the Airgap solution, you can either wait for 24 hours or perform the following steps:

1. In ZCC, go to Configuration > Management Zone Settings > Ondemand Content.
2. In the Content Type Configurations, select Patch Content or any other configuration, and then click Edit.
3. Make any type of change and click Apply.

After a few minutes of applying this change, external communication will be reinitiated.

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 [Legal Information \(https://www.microfocus.com/en-us/legal\)](https://www.microfocus.com/en-us/legal).

© Copyright 2008 - 2023 Open Text

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Open Text") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.