

ZENworks 24.2 Patch Updates

After a version of ZENworks is released, if any enhancements or bug fixes are made based on customers' request, they are provided as patch updates. This document lists the released patches and provides instructions about the sequence in which patches have to be applied on the devices:

- ♦ [“What is a Patch?” on page 1](#)
- ♦ [“Downloading and Installing Patches” on page 2](#)
- ♦ [“Understanding the Patching Sequence” on page 2](#)
- ♦ [“Patch Updates” on page 3](#)
- ♦ [“Legal Notice” on page 5](#)

What is a Patch?

A patch is an update that is installed into an existing product and a fix between the releases. A patch can fix bugs, install drivers, address security vulnerabilities, or address stability issues. The patches can also be referred to as FTF (Field Test File), which requires no testing and can be directly deployed in the production environment.

- ♦ [“What is a Server Patch?” on page 1](#)
- ♦ [“What is Baseline Patch?” on page 1](#)
- ♦ [“What is Agent Patch?” on page 2](#)
- ♦ [“Dependencies Between Agent and Server Patches” on page 2](#)

What is a Server Patch?

The server patches are released to improve the security, fix bugs or improve the performance of the product running on the server. The release version is considered the base server patch. If any server patch is baselined, then that becomes the base for future server patches. Server patches are cumulative.

What is Baseline Patch?

A baseline patch is a pre-requisite patch that is required for all future patches.

When the patch will be Baselined?

- ♦ When a patch should be applied mandatorily such as a patch that addresses security vulnerability (example 20.2.0.998 FTF).
- ♦ To limit the size of the patch.

Once a patch is baselined, subsequent patches will be cumulative.

What is Agent Patch?

Similar to server patches, agent patches are released to improve the efficiency of the agents. Unlike server patches, agent patches are not cumulative.

Dependencies Between Agent and Server Patches

Depending on customer needs or due to binary dependencies as per implementation, agent patches might be dependent on the server patch, which implies that the server patch should be installed before installing the agent patch. If a server patch is required to be applied, then the readme provided with the server and agent patches will have cross-references to each other.

Downloading and Installing Patches

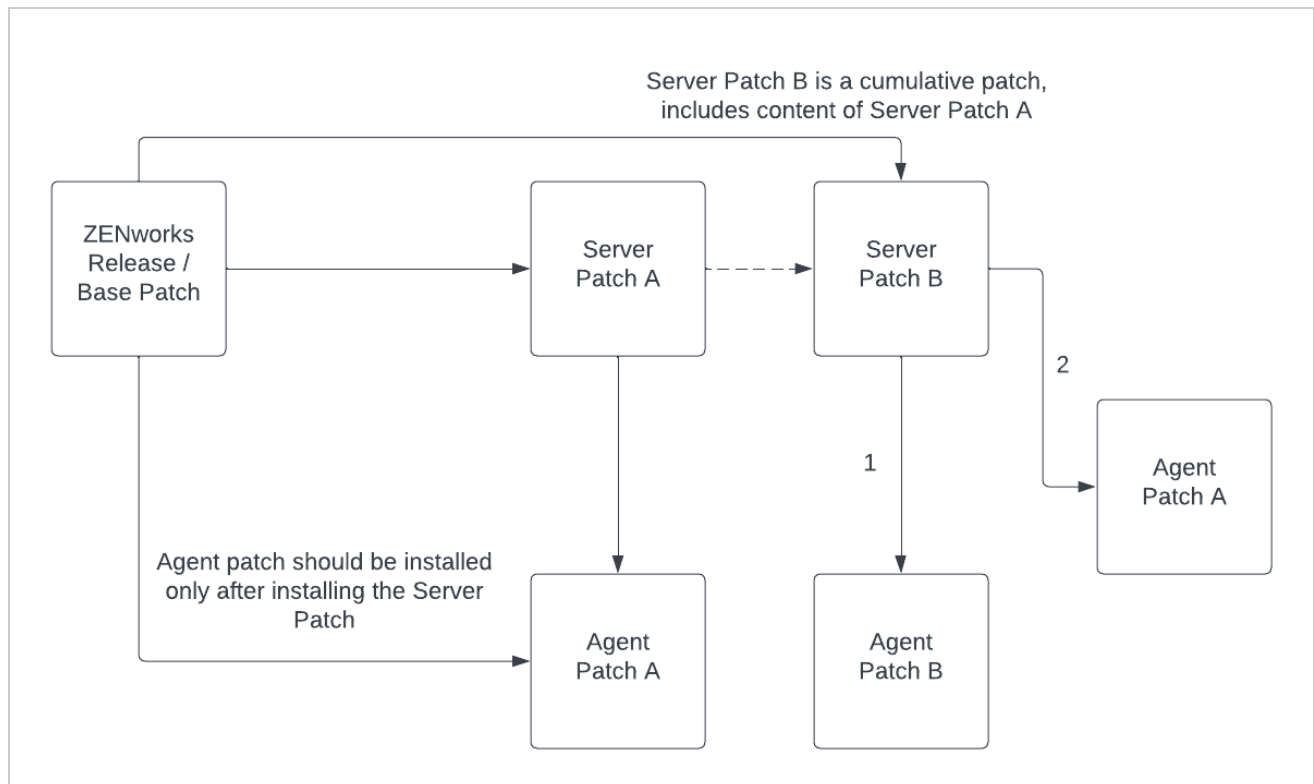
All the released patches or FTFs (*Field Test Files*) can be downloaded either from [Software Licenses and Downloads \(SLD\)](#) or [KM Viewer](#).

Each patch that is released will include a Readme. The readme section will include instructions to install a patch.

Understanding the Patching Sequence

In this document, the release version is considered as the base patch. If any server patch is baselined, then that patch becomes the base patch for future server patches.

As a best practice, it is always recommended to install the related server patch and then install the agent patch. Some patches, though they will be applied on servers, will be delivered as agent patches. For example, ZeUS.



The above chart represents the sequence in which patches have to be applied. After the ZENworks release, it will be considered as a base patch (Server Base Patch). After a next few days, Server Patch A is released. Again, after some more days, Server Patch B is released. Now, Server Patch B is a cumulative patch of Server Patch A, which implies that Server Patch B includes all the content from Server Patch A. Hence, Server Patch B can be installed without having to install Server Patch A prior to it.

In the above chart, Agent Patch A and Agent Patch B are agent patches. To install the agent patches, ensure that you have already installed the dependent server patch. In this scenario, Agent Patch A should be installed only after installing Server Patch A, or it can be installed after installing Server Patch B. However, if Agent Patch B is released before you install Agent Patch A, then you can install the agent patches in any order.

The agent patches are non-cumulative while server patches are cumulative.

Patch Updates

This section provides information on the patches that are released. After installing the server patch, install the related agent patch specified in the table, if applicable.

- ◆ [“Server Patches” on page 3](#)
- ◆ [“Agent Patches” on page 3](#)
- ◆ [“Standalone Patches” on page 4](#)
- ◆ [“Imaging Driver Updates” on page 4](#)
- ◆ [“Appliance Patches” on page 4](#)
- ◆ [“Security Patches” on page 5](#)
- ◆ [“Product Recognition Update \(PRU\)” on page 5](#)

Server Patches

This section lists all the server patches that are released for ZENworks 24.2. As server patches are cumulative, you can install the latest patch that is released.

Release Date	Patch Name	Download Link and Patch File Name	Prerequisite Patch Details	Related Agent Patch
September, 2024	Official Primary Server FTF-186 on ZENworks 24.2	PH_218252 ZCM_24.2.0_FTF_Server_186.zip	NA	PH_218411 ZCM_24.2.0_FTF_Agent_Defect_803024.zip
July, 2024	Official Primary Server FTF 185 for ZENworks 24.2	PH_217421 ZCM_24.2.0_FTF_Server_185.zip	NA	NA

Agent Patches

Unlike server patches, agent patches are not cumulative. Hence, agent patches should be installed in the following release order.

NOTE: Ensure that the agent services are not running while installing the agent patches.

Release Date	Patch Name	Download Link and File Name	Related Server Patch
September, 2024	Official Agent FTF for Issue 803024 on ZENworks 24.2	PH_218411 ZCM_24.2.0_FTF_Agent_Deffect_803024.zip	PH_218252 ZCM_24.2.0_FTF_Server_186.zip
September, 2024	Official Agent FTF for Issue 793030 on ZENworks 24.2	PH_218060 ZCM_24.2.0_FTF_Agent_Deffect_793030.zip	NA

Standalone Patches

A standalone patch is a type of update that can be applied independently. It is designed to fix a specific issue or vulnerability and can be installed without the need to update or upgrade the entire system. Standalone patches are typically small and focused and are often released in response to a bug that needs to be addressed quickly.

Imaging Driver Updates

ZENworks Imaging driver updates are designed to enhance the functionality, compatibility, and performance of ZENworks imaging, making it easier for IT administrators to manage and deploy system images. ZENworks provides driver update packages that can be imported into ZENworks. These packages contain the latest drivers for supported hardware devices, allowing administrators to easily update driver libraries to ensure that when creating or deploying system images, the most current drivers are available.

Release Date	Patch Details	Download Link and File Name	Superseded By
September, 2024	September 2024 Imaging Driver Update	PH_218456 zenworks_23.4.0_24.2.0_September24.zip	NA

Appliance Patches

Appliance patches are a type of update that is specifically designed for ZENworks Appliance. These patches are used to update and maintain the ZENworks Appliance, including the ZENworks server, operating system, and other components. These patches typically include bug fixes, security updates, and other improvements to the software.

For more information on applying Appliance patches, see [Online Update](#) in the [ZENworks Appliance Deployment and Administration Reference](#).

Security Patches

Security patches are software updates that fix vulnerabilities that could be exploited by malicious attackers. These vulnerabilities might allow attackers to gain unauthorized access to the system, steal sensitive information, or carry out other actions.

Security patches are usually released when a security flaw or vulnerability is detected. These patches are typically released on a regular schedule or as soon as a critical vulnerability is detected.

Security patches are released to address security vulnerabilities, whereas other patches to improve performance, fix bugs, or add new features. Security patches are high-priority updates that should be installed immediately to ensure security.

Product Recognition Update (PRU)

A Product Recognition Update (PRU) is a type of software update that is used to identify and classify software products on managed devices. After applying, the PRU enables ZENworks to recognize and classify new software products that may not have been previously identified.

The PRU is important as it enables ZENworks to accurately identify and manage all software products on a managed device, including those that may be less common or not well known. This allows administrators to effectively monitor and manage software license compliance, security vulnerabilities, and software updates for all devices on the network.

PRUs are released regularly and are designed to be compatible with specific versions of ZENworks. It is important to ensure that the correct PRU is downloaded and applied to the appropriate ZENworks server or zone to ensure proper identification and management of software products.

For more information, see [Downloading and Installing the PRU](#).

Released Date	PRU Details	Download Link and File Name
September, 2024	ZCM and ZAM 24.2 Sep 2024 Product Recognition Update	PH_218059 24.2.Sep2024pru.zip
July, 2024	ZCM and ZAM 24.2 July 2024 Product Recognition Update	PH_217332 24.2.Jul2024pru.zip

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 - 2024 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.

