

ZENworks 2017 Update 1 - Full Disk Encryption Update Reference

July 2017



The capability to employ ZENworks Full Disk Encryption on UEFI devices is a fundamental change in ZENworks 2017 Update 1 (version 17.1). A new Linux kernel makes this change possible. This enhancement also greatly increases hardware compatibility with smart card readers for pre-boot authentication. For more information about Update 1 changes to Full Disk Encryption, see [“Full Disk Encryption”](#) in the *What’s New in ZENworks 2017 Update 1* reference.

IMPORTANT: Before updating any existing encrypted devices to ZENworks 2017 Update 1, you should carefully review the sections below.

When you are using Full Disk Encryption and update the ZENworks Agent to 17.1, you have two options:

- ♦ **Update FDE:** Remove the Disk Encryption policy and decrypt the device, and then update the ZENworks Agent.

This option updates the Full Disk Encryption Agent and gives you the new Disk Encryption features.

- ♦ **Do not update FDE:** Update the ZENworks Agent without decrypting the device or removing the Disk Encryption policy.

This option does not update the Full Disk Encryption Agent, but does update all the other Agent modules on the device. It enables you to retain your current Full Disk Encryption functionality.

This document describes the following: (1) prerequisites and best practices when updating Full Disk Encryption to 17.1, (2) what you need to know if you want to keep your current version of Full Disk Encryption, but still want to update the ZENworks Agent, and (3) how to update Full Disk Encryption at a later date on a ZENworks Agent that you previously updated to 17.1.

1 Updating Devices to ZENworks 2017 Update 1

To get the enhancements of the new Linux kernel, you must update your devices to the 17.1 ZENworks Agent and employ a new Disk Encryption policy from an updated server. Reviewing the comments in this section will help you to successfully transition Full Disk Encryption to ZENworks 2017 Update 1:

Prerequisites when updating the Full Disk Encryption agent to ZENworks 17.1

Perform the prerequisites below to successfully update the Full Disk Encryption Agent to 17.1:

- 1 If you are updating from ZENworks 17.0, enable the **Volume Decrypted** event in ZENworks Control Center before decrypting any devices. See [Monitor Agent Events in ZCC](#) in Step 3 below.
Skip this step for 11.4.3 and earlier versions.
- 2 Remove Disk Encryption policy assignments from encrypted devices, and refresh those devices to start disk decryption and, if applicable, PBA removal.

See [“Policy Removal”](#) in the *ZENworks Full Disk Encryption Policy Reference*.

- 3 Verify the completion of disk decryption on applicable devices using one of the following methods:

- ♦ **Monitor Agent Events in ZCC:** This option is only available in 17.0 and later versions of the ZENworks Control Center, and you need to have the **Volume Decrypted** event enabled before starting decryption. The events display in **Audit and Messages > Events > Agent Events**.

See [“Enabling Change Events”](#) and [“Viewing Generated Change Events”](#) in the *ZENworks 2017 Update 1 - Auditing Full Disk Encryption Events* reference.

- ♦ **Registry key value:** Open the **Search** feature from Windows Start on the device, and type `regedit` in the **Search** field to open the Registry Editor. In the Registry Editor, go to `HKEY_LOCAL_MACHINE\Software\SECUDE\SNB\FDE`. If a device is still in an encryption state: encrypted, encrypting, or decrypting, the registry keys will have the following status of encryption or decryption:

- ♦ *DriveInProgress*: SZ registry key indicates which drive is encrypted, encrypting, or decrypting by the drive letter.
- ♦ *OperationInProgress*: DWORD registry key indicates encryption status (1) or decryption status (2).
- ♦ *ProgressPercent*: DWORD registry key indicates percent complete of encryption or decryption (hex 64 or decimal 100).

If there is not an EncryptionProgress folder with the registry keys provided above, there is not a Disk Encryption policy enforced on the device.

NOTE: You can also run a batch file through the Active Directory or deploy a bundle to run the batch file rather than accessing individual devices to check the registry keys.

- ♦ **Component status FDE command:** Open a command prompt on the device and change the directory (cd) to `%ZENWORKS_HOME%\esm`. From this directory type `zescommand.exe/componentStatus FDE`
 - ♦ *Volume(s) encrypted:* If the return value is negative, then a policy is enforced with encryption in place.
 - ♦ *No policy or encryption:* If the return value is positive, there is no Disk Encryption policy in place or initialized.
- ♦ **FDE About Box:** Open the Full Disk Encryption About box on the device, and check the encryption Status. For more information, see [“Accessing the Full Disk Encryption Agent”](#) in the *ZENworks Full Disk Encryption Agent Reference*.

- 4 After first verifying they are not referencing managed devices, delete unused 17.0 or earlier version Disk Encryption policies.

To verify no devices are being referenced, select the policy in the ZENworks Control Center, and verify there are no Device, User, or Group assignments in the **Relationships** page.

For deleting a policy, see [“Deleting Policies”](#) in the *ZENworks Full Disk Encryption Policy Reference*.

Once you successfully remove Disk Encryption policies from devices, decrypt drives, and delete old Disk Encryption policies, you are prepared to update the ZENworks Agent to ZENworks 17.1 and to create and apply a new Disk Encryption policy.

For information on updating ZENworks to the ZENworks 17.1, see the [ZENworks System Updates Reference](#).

For information on creating and applying a new Disk Encryption policy, see [“Policy Deployment”](#) in the *ZENworks Full Disk Encryption Policy Reference*.

Best Practices

You cannot successfully apply a 17.0 or earlier Disk Encryption policy to a Full Disk Encryption Agent running ZENworks 17.1.

- For the reason stated above, you should delete pre-17.1 Disk Encryption policies after removing them from Full Disk Encryption agents that you are updating to 17.1.
- When deleting a pre-17.1 Disk Encryption policy, ensure that it is not referencing a managed device. See [Step 4](#) in the prerequisites below.
- We recommend that any new Disk Encryption policies you create in Update 1 have **17.1** appended to the policy name until you have a management zone that is free of any pre-17.1 Disk Encryption policies.

2 Postponing ZENworks 2017 Update 1 on the Full Disk Encryption Agent

We recognize that you may need to postpone the update of the ZENworks Full Disk Encryption Agent to ZENworks 17.1 on some of your managed devices. If this is the case, you can still update servers and the ZENworks Agent on your devices. Any devices that still have a Disk Encryption policy in place during the update will not apply the update to the Full Disk Encryption Agent.

Considerations when not updating the Full Disk Encryption Agent to 17.1:

Although we encourage you to fully update all devices, postponing the update of the Full Disk Encryption Agent enables you to focus on devices that need this update while delaying or excluding the update of devices that do not.

Why would I not update Full Disk Encryption?

- The device has an OPAL-compliant self-encrypting drive that is using native hardware encryption and drive locking only (no software encryption), and you want to continue to use it that way.
- The device encryption is working fine, and the device does not require any of the new Update 1 encryption functionality mentioned in the [What's New in ZENworks 2017 Update 1](#).

What if I delay the update of Full Disk Encryption?

- Pre-17.1 Disk Encryption policies will remain enforced with their current capabilities (17.0 or earlier version policies) on devices with a 17.1 ZENworks Agent until you remove them.
- A Disk Encryption policy created on a ZENworks 17.1 server cannot be successfully enforced on a 17.0 or earlier Full Disk Encryption Agent.
- Updating the Full Disk Encryption Agent to 17.1 on a ZENworks Agent that was previously updated to 17.1 requires a different process than the standard update with the ZENworks Agent. See [Updating Full Disk Encryption on a 2017 Update 1 Device](#).

3 Updating Full Disk Encryption on a 2017 Update 1 Device

As stated in the previous sections, if you update your server and the ZENworks Agent to ZENworks 17.1, but leave a Disk Encryption policy in place on the device, the Full Disk Encryption Agent will continue to run the older version and not complete the update, even though the other ZENworks modules will update to the new version. This section provides information for updating the Full Disk Encryption Agent to ZENworks 17.1 on a device that already has a 17.1 ZENworks Agent.

To update a 17.0 or earlier Full Disk Encryption Agent on a 17.1 ZENworks Agent:

- 1 If you are updating from ZENworks 17.0, enable the **Volume Decrypted** event in ZENworks Control Center before decrypting any devices. See Monitor Agent Events in ZCC in [Step 3](#) below.

Skip this step for 11.4.3 and earlier versions.

- 2 Remove the Disk Encryption policy assignment from the encrypted device, and refresh the device to start disk decryption and, if applicable, PBA removal.

See “[Policy Removal](#)” in the *ZENworks Full Disk Encryption Policy Reference*.

- 3 Verify the completion of disk decryption by doing one of the following:

- ♦ **Monitor Agent Events in ZCC:** This option is only available in 17.0 and later versions of the ZENworks Control Center, and you need to have the **Volume Decrypted** event enabled before starting decryption. The events display in **Audit and Messages > Events > Agent Events**.

See “[Enabling Change Events](#)” and “[Viewing Generated Change Events](#)” in the *ZENworks 2017 Update 1 - Auditing Full Disk Encryption Events* reference.

- ♦ **Registry key value:** Open the **Search** feature from Windows Start on the device, and type `regedit` in the **Search** field to open the Registry Editor. In the Registry Editor, go to `HKEY_LOCAL_MACHINE\Software\SECUDE\SNB\FDE`. If a device is still in an encryption state: encrypted, encrypting, or decrypting, the registry keys will have the following status of encryption or decryption:

- ♦ *DriveInProgress*: SZ registry key indicates which drive is encrypted, encrypting, or decrypting by the drive letter.
- ♦ *OperationInProgress*: DWORD registry key indicates encryption status (1) or decryption status (2).
- ♦ *ProgressPercent*: DWORD registry key indicates percent complete of encryption or decryption (hex 64 or decimal 100).

If there is not an EncryptionProgress folder with the registry keys provided above, there is not a Disk Encryption policy enforced on the device.

NOTE: You can also run a batch file through the Active Directory or deploy a bundle to run the batch file rather than accessing individual devices to check the registry keys.

- ♦ **Component status FDE command:** Open a command prompt on the device and change the directory (cd) to %ZENWORKS_HOME%\esm. From this directory type `zescommand.exe/componentStatus FDE`
 - ♦ *Volume(s) encrypted:* If the return value is negative, then a policy is enforced with encryption in place.
 - ♦ *No policy or encryption:* If the return value is positive, there is no Disk Encryption policy in place or initialized.

- ♦ **FDE About Box:** Open the Full Disk Encryption About box on the device, and check the encryption Status. For more information, see [“Accessing the Full Disk Encryption Agent”](#) in the *ZENworks Full Disk Encryption Agent Reference*.
- 4 After first verifying they are not referencing managed devices, delete unused 17.0 or earlier version Disk Encryption policies.

To verify no devices are being referenced, select the policy in the ZENworks Control Center, and verify there are no Device, User, or Group assignments in the **Relationships** page.

For deleting a policy, see [“Deleting Policies”](#) in the *ZENworks Full Disk Encryption Policy Reference*.
- 5 Follow one of the procedures below to update the Full Disk Encryption agent on the device to ZENworks 2017 Update 1. These scenarios assume that you have already updated the ZENworks Agent to 17.1 and the Full Disk Encryption Agent did not successfully update at that time because you had a Disk Encryption policy enforced.

- ♦ **Update FDE using a quick task:** Do the following in ZENworks Control Center:

1. Browse to and select a device group, device folder, or device(s).
2. Click **Quick Tasks** to open the drop-down menu, and select **Verify Last Update**.

This will run each MSI from the system update on applicable devices.

- ♦ **Update FDE using the Admin Command Prompt:** Do the following to rerun the Update MSI files on the device:

1. Copy the MSI files below from the server to the device, such as C:\Temp.

Server copy location: %ZENWORKS_HOME%\install\downloads\msi folder.

- ♦ novell-zenworks-fde-api-*version-number*.msi
- ♦ novell-zenworks-fde-sec-*version-number*.x86_64.msi
- ♦ novell-zenworks-fde-*version-number*.msi

2. Open the Administrator Command Prompt on the device and run each command below in sequence using the version numbers from the files you copied.

- ♦ msixexec.exe /i novell-zenworks-fde-api-*version-number*.x86_64.msi /qn /L*v C:\Windows\Temp\fde_api_install_Log.txt
- ♦ msixexec.exe /i novell-zenworks-fde-sec-*version-number*.x86_64.msi /qn UPGD=1 ADMINPWD={11111111-2222-3333-4444-555555555555} WMIQUERY=0 /L*v C:\Windows\Temp\fde_sec_install_Log.txt
- ♦ msixexec.exe /i novell-zenworks-fde-*version-number*.msi /qn /L*v C:\Windows\Temp\novell-zenworks-fde_install_Log.txt

NOTE: You can also setup batch files to rerun the MSIs if they are available on a network share or somewhere the agent can access them.

4 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.novell.com/company/legal/>.

Copyright © 2017 Micro Focus Software, Inc. All Rights Reserved.

