

# ZENworks 2017 Update 4

## Neue Funktionen – Referenz

Januar 2019

## **Rechtliche Hinweise**

Informationen zu rechtlichen Hinweisen, Marken, Haftungsausschlüssen, Gewährleistungen, Ausführbeschränkungen und sonstigen Nutzungseinschränkungen, Rechten der US-Regierung, Patentrichtlinien und Erfüllung von FIPS finden Sie unter <http://www.novell.com/company/legal/>.

**© Copyright 2008–2019 Micro Focus oder eines seiner verbundenen Unternehmen.**

Für Produkte und Services von Micro Focus oder seinen verbundenen Unternehmen und Lizenznehmern („Micro Focus“) gelten nur die Gewährleistungen, die in den Gewährleistungserklärungen, die solchen Produkten beiliegen, ausdrücklich beschrieben sind. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine zusätzliche Gewährleistung. Micro Focus haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Die in diesem Dokument enthaltenen Informationen sind vorbehaltlich etwaiger Änderungen.

---

# Inhalt

<b>Allgemeines zu diesem Handbuch</b>	<b>5</b>
<b>1 Neue Funktionen in ZENworks 2017 Update 4</b>	<b>7</b>
1.1 Unterstützte Plattformen	7
1.2 ZENworks Configuration Management	8
1.2.1 Mobile Management	8
1.2.2 Client-Verwaltung	10
1.3 Imaging und Fernverwaltung	11
1.4 Inventar	11
1.5 Inventarverwaltung	12
1.6 ZENworks-Anwendung	12
1.7 Endpoint Security Management	12
1.8 Vollständige Festplattenverschlüsselung	12
1.9 Patch Management	12
1.10 Berichterstellung	13



# Allgemeines zu diesem Handbuch

In diesem Handbuch *ZENworks What's New Reference* (ZENworks Neue Funktionen – Referenz) werden die neuen Funktionen in der Version ZENworks 2017 beschrieben. Dieses Handbuch besteht aus den folgenden Abschnitten:

- ♦ [Kapitel 1, „Neue Funktionen in ZENworks 2017 Update 4“](#), auf Seite 7

## Zielgruppe

Dieses Handbuch richtet sich an ZENworks-Administratoren.

## Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Über die Funktion **Thema kommentieren**, die Sie unten auf jeder Seite der Online-Dokumentation finden, können Sie uns Ihre Vorschläge und Meinung mitteilen.

## Weitere Dokumentation

Im Lieferumfang von ZENworks finden Sie weitere Dokumentationen (im PDF- und HTML-Format), die Informationen zum Produkt und zu dessen Implementierung beinhalten. Weitere Dokumentation finden Sie auf der [Dokumentations-Website zu ZENworks](#).



# 1 Neue Funktionen in ZENworks 2017 Update 4

In den folgenden Abschnitten werden die neuen Funktionen und Verbesserungen in ZENworks 2017 Update 4 beschrieben:

- ♦ [Abschnitt 1.1, „Unterstützte Plattformen“](#), auf Seite 7
- ♦ [Abschnitt 1.2, „ZENworks Configuration Management“](#), auf Seite 8
- ♦ [Abschnitt 1.3, „Imaging und Fernverwaltung“](#), auf Seite 11
- ♦ [Abschnitt 1.4, „Inventar“](#), auf Seite 11
- ♦ [Abschnitt 1.5, „Inventarverwaltung“](#), auf Seite 12
- ♦ [Abschnitt 1.6, „ZENworks-Anwendung“](#), auf Seite 12
- ♦ [Abschnitt 1.7, „Endpoint Security Management“](#), auf Seite 12
- ♦ [Abschnitt 1.8, „Vollständige Festplattenverschlüsselung“](#), auf Seite 12
- ♦ [Abschnitt 1.9, „Patch Management“](#), auf Seite 12
- ♦ [Abschnitt 1.10, „Berichterstellung“](#), auf Seite 13

## 1.1 Unterstützte Plattformen

ZENworks 2017 Update 4 unterstützt die folgenden neuen Plattformen:

- ♦ Agent und Primärserver
  - ♦ SLES 12 SP4
- ♦ Agent und Satellitenserver
  - ♦ Windows Server 2019
  - ♦ Windows 10 1809
  - ♦ Windows 10 Enterprise LTSC 2019
  - ♦ OES 1 SP2018
  - ♦ RHEL 7.5
  - ♦ Scientific Linux 7.5
  - ♦ Mac 10.14
- ♦ Mobil:
  - ♦ iOS 12
  - ♦ Android 5 (oder höher)

Weitere Informationen zu den Systemanforderungen finden Sie in den *Systemanforderungen für ZENworks 2017*.

## 1.2 ZENworks Configuration Management

- ♦ Abschnitt 1.2.1, „Mobile Management“, auf Seite 8
- ♦ Abschnitt 1.2.2, „Client-Verwaltung“, auf Seite 10

### 1.2.1 Mobile Management

- ♦ **FRP (Factory Reset Protection) für verwaltete Android-Unternehmensgeräte:** Ab dieser Version können Sie in ZENworks verhindern, dass die Benutzer ihre verwalteten Unternehmensgeräte über die Einstellungen zurücksetzen. Außerdem können Sie eines oder mehrere Unternehmens-Entsperrkonten, die authentifiziert werden müssen, auf die Weiße Liste setzen bevor die Einrichtung auf dem Gerät nach einem unbefugten Zurücksetzen auf die Werkseinstellungen fortgesetzt werden kann, z. B. über Bootloader oder Fastboot.

Weitere Informationen finden Sie unter Enabling Factory Reset Protection on Android Work-Managed Devices (Aktivieren von FRP auf verwalteten Android-Unternehmensgeräten) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Zusätzliche Informationen zu Android-Bundles:** Der Abschnitt „App-Details“ auf der Zusammenfassungsseite „Android-Bundles“ wurde um zusätzliche Informationen erweitert, z. B. App-Version, -Track und das Datum der letzten Veröffentlichung.
- ♦ **Zusätzliche Informationen zur Gerätezusammenfassung:** Die Seite „Geräteinformationen“ für Android-Geräte enthält nunmehr zusätzliche Software-Details, z. B. die auf dem Gerät angewendete Sicherheits-Patch-Stufe. Diese Informationen werden auch in den erzeugten Mobilgeräte-Inventarberichten aufgeführt.

Weitere Informationen finden Sie unter Viewing Device Information (Abrufen von Geräteinformationen) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Geräteverwaltungs-API veraltet:** Ab dieser Version unterstützt ZENworks den Basis-Registrierungsmodus mit der Geräteverwaltungs-API auf Android-Geräten nicht mehr. Diese Maßnahme resultiert aus der Ankündigung von Google, die Geräteverwaltungs-API aus der Android P-Version herauszunehmen. ZENworks unterstützt nunmehr nur noch zwei Möglichkeiten zur Registrierung für Android-Geräte, und zwar den Arbeitsprofilmodus und den Modus für verwaltete Unternehmensgeräte.

Weitere Informationen finden Sie unter <https://www.novell.com/communities/cool-solutions/removal-device-admin-api-android-devices/>.

- ♦ **Neustarten von Android-Mobilgeräten:** Sie können verwaltete Android-Unternehmensgeräte nunmehr mit der bereits vorhandenen Schnellaufgabe „Neu starten/Herunterfahren“ neu starten.

Weitere Informationen finden Sie unter Reboot or Shutdown Devices (Neustarten oder Herunterfahren von Geräten) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Unterstützung für Direct Boot:** Ab dieser Version unterstützt ZENworks die Direct Boot-Funktion für Geräte ab Android 7.0. Mit dieser Funktion ist der ZENworks-Agent ständig auf einem Android-Gerät aktiv, und zwar auch schon vor dem Entsperrn des Geräts. Die

Administratoren können selbst dann schon Richtlinien wie die Compliance-Richtlinie erzwingen, das Arbeitsprofil entfernen oder das Gerät auf die Werkseinstellungen zurücksetzen, wenn das Gerät noch nicht entsperrt wurde.

- ♦ **Verteilen von iOS-Unternehmens-Apps:** Über die bereits vorhandene Bundles-Funktion in ZENworks können Sie nunmehr benutzerdefinierte interne Apps, die nicht öffentlich zur Distribution bereitstehen, an iOS-Geräte verteilen.

Weitere Informationen finden Sie unter Distributing iOS Enterprise Apps (Verteilen von iOS Enterprise-Apps) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Verteilen einer WLAN-Konfiguration mithilfe von Bundles:** Mit dieser Funktion können die Administratoren WLAN-Profil-Bundles auf den Geräten der Benutzer erstellen und bereitstellen, sodass die Benutzer ihre Geräte über die angegebene WLAN-Verbindung mit dem Unternehmensnetzwerk verbinden können. Diese Funktion ist sowohl auf Android-Geräten als auch auf iOS-Geräten verfügbar.

Weitere Informationen finden Sie unter Distributing Corporate Wi-Fi Settings (Verteilen von Unternehmens-WLAN-Einstellungen) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Schutzrichtlinie der Office 365-Android-App:** Mit ZENworks können Sie nunmehr Android-Apps schützen, die mit dem Intune-SDK erstellt wurden (z. B. Microsoft Office 365-Apps), ohne dass die Benutzer ihre Geräte in ZENworks registrieren müssen.

Weitere Informationen finden Sie unter Creating the App Protection Policy (Android Intune App Protection Policy) (Erstellen der App-Schutzrichtlinie [Schutzrichtlinie der Android-Intune-App]) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **ZENworks und Azure synchronisieren:** Mit dieser Funktion können Administratoren einen Zeitplan für die Synchronisierung der ZENworks-Schutzrichtlinie der Intune-App mit Microsoft Azure aufstellen.

Weitere Informationen finden Sie unter Policy Sync Schedule (Zeitplan für Richtlinien synchronisierung) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Unterstützung für neue Android-Einschränkungen:** Die Liste der Android-Einschränkungen wurde sowohl für das Android-Arbeitsprofil als auch für verwaltete Unternehmensgeräte (auch Android P-Geräte) erheblich erweitert. Diese Einschränkungen umfassen verschiedene Einstellungen, z. B. Aktivieren der Tastensperrfunktionen für ein Gerät, Einhängen physischer externer Medien, Datenfreigabe per NFC-Beam und Einschränken der Betriebssystemaktualisierungen.

Weitere Informationen finden Sie in Abschnitt 12.5.2, „Applying Device Restrictions“ (Anwenden von Geräteeinschränkungen) im Handbuch *ZENworks 2017 Update 4 Mobile Management Reference* (ZENworks 2017 Update 4 – Referenz für mobile Verwaltung).

- ♦ **Unterstützung für neue Einschränkungen in iOS 12 und DEP-Einstellungen:**

- ♦ **Neue Einschränkungen in iOS 12:** Ab dieser Version werden zusätzliche Einschränkungen in iOS 12 unterstützt, z. B. die automatische Aktualisierung des Datums und der Uhrzeit, die Einrichtung neuer Geräte in der Nähe und die Verzögerung von Betriebssystemaktualisierungen.

Weitere Informationen finden Sie unter Editing a Mobile Device Control Policy Setting (Bearbeiten einer Einstellung in der Richtlinie zur Mobilgerätesteuerung) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 Update 4 – Referenz für mobile Verwaltung).

- ♦ **Neue DEP-Einstellungen:** Die DEP-Einstellungen wurden ebenfalls erweitert und unterstützen nunmehr Funktionen, mit denen die Standardsprache und die Region beim Einrichten von Apple TV-Geräten ausgewählt werden kann. Beim Einrichten eines DEP-Geräts mit iOS 12 können Sie nunmehr bestimmte Einrichtungsbildschirme überspringen, z. B. Bildschirmzeit, iMessage und FaceTime.

Weitere Informationen finden Sie unter Managing the DEP Profile (Verwalten des DEP-Profiles) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Zurücksetzen des Passworts im Fernverfahren auf Geräten ab Android 8.0:** Mit der Schnellaufgabe **Gerät entsperren** können Sie das Passwort auf Geräten mit Android 8.0 im Fernverfahren zurücksetzen und ein neues Passwort festlegen, wenn der Benutzer das bestehende Passwort für das Gerät vergessen hat.

Weitere Informationen finden Sie unter Unlocking a Device (Entsperren eines Geräts) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **AutoFill des Berechtigungsnachweises in der ZENworks-App per QR-Code:** Der Anmeldebildschirm der ZENworks-App enthält nunmehr ein Symbol, mit dem der Benutzer den QR-Code scannen und damit die Anmeldeberechtigungen automatisch eintragen lassen kann. Wenn der Benutzer auf dieses Symbol tippt, muss er den QR-Code im Einladungsschreiben scannen. Anschließend gelangt der Benutzer zur App zurück und die Anmeldeberechtigungen (jedoch nicht das Passwort) werden automatisch eingetragen.

Weitere Informationen finden Sie unter Enrolling Mobile Devices (Registrieren von Mobilgeräten) im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

- ♦ **Überprüfung von Gerätezurücksetzungen bei geschützten Intune-App-Geräten:** Die Administratoren können nunmehr die Änderungsereignisse konfigurieren, damit die Benutzer die Einleitung der Intune-App-Zurücksetzung überprüfen können.
- ♦ **Aktualisierung der Seite „Apps-Katalog“:** Die Seite „Apps-Katalog“ enthält nunmehr Apps, die mit den iOS-App-Bundles und den iOS Enterprise-Apps erstellt wurden.

Weitere Informationen zu allen Funktionen der mobilen Verwaltung finden Sie im Handbuch *ZENworks 2017 Mobile Management Reference* (ZENworks 2017 – Referenz für mobile Verwaltung).

## 1.2.2 Client-Verwaltung

- ♦ **Auffinden von Windows 10-Geräten über die Registerkarte „Geolocation“:** Diese ZENworks-Funktion macht sich den Windows-10-Positionsdienst zunutze, um Geräte zu orten, die mit der Windows-10-Version 1709 oder neueren Windows-10-Betriebssystemversionen arbeiten. Sie können auf die Registerkarte **Geolocation** zugreifen, wenn Sie auf den Link eines Arbeitsstationsgeräts klicken.
- ♦ **Zurücksetzen eines Windows-Geräts mithilfe einer neuen Schnellaufgabe:** Über die neue Schnellaufgabe **Zurücksetzen** wird das Betriebssystem des ausgewählten Windows-Geräts auf die Werkseinstellungen zurückgesetzt und es werden alle Dateien und Anwendungen

gelöscht, die nicht Teil des Betriebssystems sind. Sie können die Schnellaufgabe implementieren, wenn Sie ein Windows-Gerät in der Liste der Arbeitsstationen ausgewählt haben. Diese Funktion wird nur auf Windows 10-Geräten unterstützt.

- ♦ **Neue Installationszeitpläne in Bundles:** Mit dem neuen Bundle-Installationszeitplan können Sie nunmehr das Datum und die Uhrzeit festlegen, zu der die Bundles auf verwalteten Geräten installiert werden sollen.
- ♦ **Möglichkeit zum Prüfen auf Prozesse oder Dienste, die auf einem verwalteten Gerät ausgeführt werden:** Es kann nunmehr eine Anforderung zum Prüfen auf Prozesse oder Dienste, die auf einem verwalteten Gerät ausgeführt werden, in ein ZENworks-Bundle eingefügt werden.
- ♦ **Änderung bei der Java-Distribution:** Ab dieser Version erfolgt die Distribution der Java-Software über eine Open-Source-Plattform.

## 1.3 Imaging und Fernverwaltung

- ♦ **Verweis auf ein bestehendes MDT-Bundle:** Mit dieser Funktion können Administratoren MDT-Bundles mithilfe von WIM-Dateien erstellen, die bereits in ein bestehendes Bundle hochgeladen wurden.

Weitere Informationen finden Sie in Abschnitt 3.8, „Configuring MDT Deployment Bundles“ (Konfigurieren von MDT-Bereitstellungs-Bundles) und Abschnitt 5.3, „Action – MDT Deployment“ (Aktion – MDT-Bereitstellung) im Handbuch *ZENworks Preboot Services and Imaging Reference* (Referenz für ZENworks Preboot Services und Imaging).

- ♦ **Unterstützung von TLS 1.2 für Fernverwaltung und Imaging:** Fernsitzungen werden mithilfe von Secured Socket Layer (TLSv1.2-Protokoll) geschützt. Diese Funktion ist nur auf Windows-Geräten verfügbar.

## 1.4 Inventar

- ♦ **Automatische Bereinigung von PRU-Bundles:** Alte PRU-Bundles, die ausgeblendet sind und nicht verwendet werden, werden nunmehr automatisch bereinigt.
- ♦ **Inventarabsuche direkt nach dem Imaging eines Geräts:** Mit dieser Funktion können Administratoren eine Komplettabsuche des Geräts ausführen, nachdem ein erneutes Imaging des Geräts erfolgt ist. Sie müssen nicht mehr abwarten, bis die geplante Absuche beendet ist und die Daten später auf den Server hochgeladen sind, sondern Sie sehen sofort die aktuellen Inventardaten und können die notwendigen Maßnahmen ergreifen, beispielsweise Software-Bundles bereitstellen.

Weitere Informationen finden Sie in Abschnitt 2.2, „Scheduling an Inventory Scan (Perform Full scan after imaging a device)“ (Planen einer Inventarabsuche [Ausführen einer Komplettabsuche nach dem Imaging eines Geräts]) im Handbuch *Referenz zu ZENworks Asset Inventory*.

- ♦ **Hardwareinventardaten zu Mobilgeräten in ZCC-Inventarberichten:** Hardwareinventardaten zu Mobilgeräten werden nunmehr in Inventartabellen gespeichert. So stehen die Daten in ZCC-Inventarberichten zur Verfügung. Die Inventarberichte wurden entsprechend um neue Felder ergänzt, was diese Funktion erleichtert.

Auch die Inventarverarbeitung wird in dieser Version optimiert.

## 1.5 Inventarverwaltung

- ♦ **Importieren von Netzwerkgeräten und Verknüpfen mit ZAM-Verträgen:** Netzwerkgeräte mit ADF-Daten können nunmehr in das ZENworks-Kontrollzentrum importiert und dann mit ZENworks Asset Management-Verträgen verknüpft werden.

Weitere Informationen finden Sie in Abschnitt 4, „Importing Devices from CSV Files“ (Importieren von Geräten aus CSV-Dateien) im Handbuch *ZENworks Discovery, Deployment, and Retirement Reference* (ZENworks: Ermittlungs-, Bereitstellungs- und Stilllegungsreferenz).

## 1.6 ZENworks-Anwendung

In dieser Version wird ein neuer Registrierungsschlüssel eingeführt, mit dem Energieoptionen deaktiviert werden, wenn ZAPP als Shell fungiert.

## 1.7 Endpoint Security Management

- ♦ **Optimierung der Platzhalterzeichen in der Richtlinie zur Anwendungssteuerung:** Durch die Optimierungen in der Richtlinie zur Anwendungssteuerung können nunmehr Platzhaltereinträge in die Anwendungssteuerungslisten eingetragen werden, sodass Sie umfassendere Zugriffssteuerungen mit weniger Konfigurationsaufwand erzielen.
- ♦ **Aktualisierte Richtlinie zur Speichergerätesteuerung:** Die Optimierungen der Richtlinie zur Speichergerätesteuerung vereinfachen die Erstellung und Pflege von Richtlinien und bahnen den Weg für weitere Steuerungen in der kommenden Version.

## 1.8 Vollständige Festplattenverschlüsselung

- ♦ **Umgehen der PBA bei bestimmten Neustarts:** Wird die Preboot-Authentifizierung (PBA) mit einer Richtlinie für die Festplattenverschlüsselung verwendet, können Sie mit dieser Befehlsoption auf verschlüsselten Agentengeräten die Preboot-Authentifizierung vorübergehend für eine bestimmte Anzahl von Gerätestarts oder -neustarts umgehen. Diese Funktion kann auf Client-Geräten über die Befehlsoption im Agenten zur vollständigen Festplattenverschlüsselung oder über die Befehlszeile auf dem Gerät mit `zescommand bypassPbaWithRebootCount` ausgeführt werden.

Weitere Informationen finden Sie unter *Bypassing PBA for Specified Reboots* (Umgehen der PBA bei bestimmten Neustarts) im Handbuch *ZENworks Full Disk Encryption Agent Reference* (ZENworks-Referenz für den Agenten zur vollständigen Festplattenverschlüsselung).

## 1.9 Patch Management

- ♦ **Freigeben von Geräte-Patches aus der Quarantäne mithilfe einer Schnellaufgabe:** Geplante Richtlinien- oder Fehlerbehebungsinstallationen von Patches auf einem Gerät werden bei Patches, die sich in Quarantäne befinden, nicht ausgeführt. Wenn Sie ein Problem behoben haben, durch das ein Patch nicht installiert werden konnte, und der Patch sich mittlerweile in Quarantäne befindet, können Sie die Patches mit der Schnellaufgabe „Patches aus der

Quarantäne freigeben“ wieder aus der Quarantäne auf einem Gerät freigeben. Patches, die aus der Quarantäne freigegeben wurden, bleiben so lange freigegeben, bis die Installation wiederholt wird.

Weitere Informationen finden Sie unter Release Quarantined Patches (Patches aus der Quarantäne freigeben) im Handbuch *ZENworks 2017 – Referenz zu Patch Management*.

- ◆ **Patch Management-Systemvariablen:** Patch Management wurde um zwei neue Systemvariablen ergänzt, mit denen das Patch-Neustartverhalten umfassender gesteuert wird sowie die Speicherung von Patch-Trending-Daten kontrolliert wird, die in einer früheren Version von ZENworks Patch Management konfiguriert wurde.

- ◆ **PATCH\_ALWAYS\_SHOW\_REBOOT\_PROMPT**

Mit dieser Variablen wird die Patch-Neustarteingabeaufforderung für die Benutzer angezeigt, wenn die Option „Neustartverhalten für Patch-Richtlinie“ für **Neustart unterdrücken** auf **Ja** eingestellt ist.

- ◆ **PATCH\_TREND\_DATA\_DAYS**

Diese Variable steuert den Zeitraum (in Tagen), über den die Patch-Dashboard- und Trending-Daten (in einer früheren Version von ZENworks konfiguriert) in der Datenbank gespeichert werden. Stellen Sie den Zeitraum auf  $x$  Tage für die Datenspeicherung ein. Mit dem Wert 0 wird die Speicherung der Daten deaktiviert.

## 1.10 Berichterstellung

Die Administratoren können nunmehr mit der ZENworks-Berichterstellung einen Bericht über eine Zone mit PostgreSQL als Datenbank erstellen.

