# Readme di ZENworks 2017 Update 4

Gennaio 2019

Le informazioni contenute in questo Readme si riferiscono alla release di ZENworks 2017 Update 4.



## Novità di ZENworks 2017 Update 4

Per informazioni sulle nuove funzionalità incluse in questa release, consultare ZENworks What's New Reference (in lingua inglese).

## Pianificazione della distribuzione di ZENworks 2017 Update 4

Per pianificare la distribuzione di ZENworks 2017 Update 4 nella zona di gestione, attenersi alle seguenti linee guida:

- Se si utilizza la cifratura disco e si desidera aggiornare l'agente FDE (Full Disk Encryption) da una versione precedente a ZENworks 2017 Update 1, è NECESSARIO rimuovere la policy di cifratura disco dai dispositivi gestiti prima di aggiornarli a ZENworks 2017 Update 4.

  Se si aggiorna l'agente FDE (Full Disk Encryption) da ZENworks 2017 Update 1 o 2017 Update 2 a ZENworks 2017 Update 4, lasciare la policy di cifratura disco in opera. Non è richiesta alcuna modifica prima dell'aggiornamento di sistema.

  Per ulteriori informazioni sull'aggiornamento di FDE (Full Disk Encryption) in ZENworks 2017 Update 4 da una versione precedente a ZENworks 2017 Update 1, consultare il documento ZENworks 2017 - Full Disk Encryption Update Reference (in lingua inglese).

- L'upgrade a ZENworks 2017 Update 4 deve essere eseguito prima di tutto per i server primari, quindi per i server satellite e infine per i dispositivi gestiti. Non eseguire l'upgrade dei dispositivi gestiti e dei server satellite (o non aggiungere nuovi agenti di 2017 Update 4 nella zona) se l'upgrade a ZENworks 2017 Update 4 non è ancora stato eseguito su tutti i server primari.

  **Nota:** se sui server primari non è ancora stato eseguito l'upgrade, gli agenti potrebbero ricevere dati incoerenti dalla zona. Pertanto, questa parte del processo deve essere completata nel più breve tempo possibile, idealmente subito dopo l'upgrade del primo server primario.

- Sui seguenti dispositivi è possibile distribuire direttamente la versione 2017 Update 4:

| Tipo di dispositivo | Sistema operativo | Versione minima di ZENworks |
|---|---|---|
| Server primari | Windows e Linux | ZENworks 2017 e versioni successive |
| Server satellite | Windows, Linux and Mac | ZENworks 11.x e versioni successive |
| Dispositivi gestiti | Windows | ZENworks 11.x e versioni successive |
| | Linux | ZENworks 11.x e versioni successive |
| | Mac | ZENworks 11.2 e versioni successive |

- Una volta eseguito l'upgrade a ZENworks 2017 Update 4, il sistema viene riavviato. Tuttavia, nei seguenti casi sarà necessario un doppio riavvio:
  - Se si esegue l'aggiornamento da 11.x a ZENworks 2017 o a una versione successiva (2017 Update 1, Update 2, Update 3 o Update 4) ed è abilitata la sicurezza endpoint, sarà necessario un secondo riavvio per caricare il driver ZESNETAccess.
  - Se in un dispositivo gestito è in esecuzione Windows 10 con l'impostazione Autodifesa client abilitata e si esegue l'upgrade da 11.4.x a ZENworks 2017 o a una versione successiva (2017 Update1, Update2, Update 3 o Update 4), è necessario disabilitare tale impostazione nel Centro di controllo ZENworks, riavviare il dispositivo gestito ed eseguire l'aggiornamento, per il quale è richiesto un secondo riavvio del dispositivo.
  - Se è stata applicata una policy di cifratura disco su un dispositivo gestito e si desidera aggiornare l'agente FDE (Full Disk Encryption) da una versione precedente l'Update 1 di ZENworks 2017 a ZENworks 2017 Update 4, prima è necessario rimuovere la policy e decifrare il dispositivo. Per l'aggiornamento è richiesto il riavvio del dispositivo. Successivamente si aggiorna il dispositivo a 2017 Update 4 e si esegue una seconda volta il riavvio.

  **Importante:** per i dispositivi gestiti sui quali sono in esecuzione versioni precedenti a 11.x, prima è necessario eseguire l'upgrade a 11.x. Al termine dell'upgrade a 11.x il sistema viene riavviato, quindi, una volta completata la distribuzione di ZENworks 2017 Update 4, ha luogo un secondo riavvio.

- Prima di installare l'aggiornamento di sistema, assicurarsi di avere spazio libero su disco sufficiente nelle seguenti ubicazioni:

| Ubicazione | Descrizione | Spazio su disco |
|---|---|---|
| **Windows:** `%zenworks_home%\install\downloads`<br>**Linux:** `opt/novell/zenworks/install/downloads` | Per aggiornare i pacchetti agente. | 5,7 GB |
| **Windows:** `%zenworks_home%\work\content-repo`<br>**Linux:** `/var/opt/novell/zenworks/content-repo` | Per importare il file zip nel sistema dei contenuti. | 5,7 GB |
| Cache agente | Per scaricare il contenuto dell'aggiornamento di sistema applicabile richiesto per aggiornare il server ZENworks. | 1,5 GB |
| Ubicazione in cui viene copiato il file dell'aggiornamento di sistema. si applica solo al server ZENworks utilizzato per importare il file zip dell'aggiornamento di sistema | Memorizzare il file zip dell'aggiornamento di sistema scaricato. | 5,7 GB |

# Download e distribuzione di ZENworks 2017 Update 4

Per istruzioni su download e distribuzione di ZENworks 2017 Update 4, vedere *ZENworks System Updates Reference* (in lingua inglese).

Se la zona di gestione è costituita da server primari sui quali è installata una versione precedente a ZENworks 2017, è possibile distribuire ZENworks 2017 Update 4 a tali server primari solo dopo averli sottoposti tutti all'upgrade a ZENworks 2017. Per istruzioni, vedere *Guida all'upgrade di ZENworks*.

Per i task amministrativi, visitare il sito relativo alla documentazione di ZENworks 2017 Update 4.

**Importante:** non aggiornare il visualizzatore di Gestione remota prima di avere aggiornato tutti i Join Proxy Satellite Server della zona. Per eseguire Gestione remota attraverso Join Proxy, è necessario che la versione del visualizzatore di Gestione remota sia la stessa di quella di Join Proxy.

Leggere la "Pianificazione della distribuzione di ZENworks 2017 Update 4" a pagina 1 prima di effettuare il download e distribuire ZENworks 2017 Update 4.

**Importante:** durante la fase di preparazione della distribuzione di ZENworks Update, il servizio di aggiornamento di ZENworks (ZeUS) nei server primari viene sostituito con il nuovo pacchetto incluso nell'aggiornamento.

**Non distribuire ZENworks 2017 Update 4 prima di avere eseguito l'upgrade a ZENworks 2017 di tutti i server primari della zona.**

Per questo aggiornamento è necessario apportare modifiche allo schema nel database. Durante l'installazione iniziale delle patch, i servizi vengono eseguiti solo sul server master o su quello primario dedicato. In tal modo si ha la garanzia che gli altri server primari non tenteranno di accedere alle tabelle che vengono modificate nel database.

Dopo l'aggiornamento del server master o del server primario dedicato, i servizi riprendono sui server restanti e contemporaneamente ha luogo l'aggiornamento.

---

**Nota:** durante l'aggiornamento non è necessario interrompere o riavviare manualmente i servizi nei server. I servizi vengono interrotti e riavviati automaticamente.

---

Quando si posticipa un aggiornamento del sistema e si esegue il logout dal dispositivo gestito, su questo viene applicato l'aggiornamento del sistema.

Per l'elenco delle versioni supportate dei dispositivi gestiti e dei server satellite in una zona di gestione con ZENworks 2017 Update 4, vedere Versioni supportate dei dispositivi gestiti e dei server satellite.

# Problemi risolti in ZENworks 2017 Update 4

Alcuni dei problemi identificati nelle release precedenti sono stati risolti. Per un elenco dei problemi risolti, vedere il documento TID 7023612 nella Knowledgebase del supporto tecnico.

# Problemi che permangono in ZENworks 2017 Update 4

Alcuni dei problemi riscontrati nelle versioni precedenti a ZENworks 2017 Update 4 non sono stati ancora risolti. Per ulteriori informazioni, consultare i seguenti readme:

- Readme di ZENworks 2017
- Readme di ZENworks 2017 Update 1
- Readme di ZENworks 2017 Update 2
- Readme di ZENworks 2017 Update 3

# Problemi noti

Questa sezione contiene le informazioni relative ai problemi di che possono verificarsi durante l'uso di ZENworks 2017 Update 4:

## Impossibile applicare la percentuale di luminosità impostata come policy di controllo dispositivo mobile nei dispositivi Android

Viene assegnata una policy di controllo dispositivo mobile, con un valore specifico di percentuale di luminosità definito nel campo **Imposta percentuale di luminosità**, a un dispositivo Android gestito per il lavoro, quindi il valore di luminosità non viene applicato al dispositivo e nei messaggi relativi allo stato delle policy viene visualizzato il messaggio di errore "App non supportata".

Soluzione: nessuna.

## Avvio diretto non supportato nei dispositivi Android P (9.0)

Come riconosciuto da Google, la funzione di avvio diretto non funziona nei dispositivi Android P.

Soluzione: nessuna.

## Le impostazioni relative al blocco tastiera del dispositivo non funzionano nei dispositivi in cui è stato eseguito l'upgrade di ZENworks Agent App da una versione precedente a 17.4.0.

Quando in un dispositivo si esegue l'upgrade di ZENworks Agent App alla versione 17.4.0, le impostazioni di blocco tastiera del dispositivo, abilitate come parte della policy di controllo dispositivo mobile assegnata, non funzionano.

Soluzione: annullare la registrazione del dispositivo utilizzando il task rapido **Annulla registrazione** in ZCC ed eseguire di nuovo la registrazione. Riassegnare la stessa policy di controllo dispositivo mobile. Le impostazioni relative al blocco tastiera del dispositivo verranno abilitate sul dispositivo.

## Le impostazioni di blocco tastiera del dispositivo non vengono applicate ai dispositivi Android Lollipop e Marshmallow registrati in modalità profilo di lavoro

Quando le impostazioni di blocco tastiera del dispositivo sono abilitate come parte della policy di controllo dispositivo mobile, questa non viene applicata ai dispositivi Android Lollipop e Marshmallow registrati in modalità profilo di lavoro. Lo stato della policy viene visualizzato come non riuscito in ZCC e nei log del dispositivo viene visualizzato il messaggio di errore "Impossibile impostare configurazione agente di attendibilità per un profilo gestito".

Soluzione: nessuna.

## Il task rapido Sblocca dispositivo non funziona nei dispositivi Android Lollipop e Marshmallow registrati in modalità profilo di lavoro

Il task rapido Sblocca dispositivo non funziona nei dispositivi Android Lollipop e Marshmallow registrati in modalità profilo di lavoro. Lo stato del task rapido viene visualizzato come non riuscito in ZCC e nei log del dispositivo viene visualizzato il messaggio di errore "Impossibile reimpostare la password per il profilo gestito".

Soluzione: nessuna.

## Dopo l'aggiornamento di ZENworks, in ZDC viene visualizzata una versione errata del Redhat Package Manager (RPM) novell-zenworks-xplat-uninstall

Dopo l'upgrade della zona di gestione ZENworks, in ZDC viene visualizzata una versione errata del Redhat Package Manager (RPM) novell-zenworks-xplat-uninstall.

Soluzione: nessuna.

Attendere che venga eseguita l'azione di aggiornamento nel server primario.

## Caratteri indesiderati nel nome cartella dei dispositivi AMT

Nella scheda **ZCC** > **Dispositivi** > **Rilevati**, sono visualizzati caratteri indesiderati nel nome della cartella **Dispositivi Intel AMT**.

Soluzione: nessuna.

## La regola di controllo dell'accesso Non attendibile non blocca il traffico di rete nei dispositivi in cui è applicata la policy del firewall di sicurezza degli endpoint

Quando si configura l'elenco di controllo dell'accesso (ACL) con una o più regole ACL Non attendibile nella policy del firewall, l'accesso alla rete basato sulla regola non viene bloccato.

Soluzione: utilizzare configurazioni delle porte del firewall native per bloccare l'accesso alla rete.

## Il login in modalità passiva a ZENworks non funziona dopo l'upgrade a Windows v1709, v1803 o v1809

Dopo l'upgrade del dispositivo a Windows 10 v1709 (Fall Creator Update), v1803 o Windows 10 v1809 (April 2018 Update), il login in modalità passiva a ZENworks non funziona.

Soluzione: fare riferimento al documento TID 7022478 nella Knowledgebase di Micro Focus.

## Negli agenti ZENworks non vengono eseguiti i task rapidi e gli aggiornamenti del sistema

Quando si assegna un task rapido o un aggiornamento del sistema a un agente ZENworks, tale elemento non viene eseguito nell'agente e nel log ZeUS viene registrato l'errore **"TaskNotifier, errore 503 ricevuto dal server"**.

**Per confermare "TaskNotifier, errore 503 ricevuto dal server" eseguire le seguenti operazioni:**

1. Nell'agente, in Applicazione tecnica (fare clic con il pulsante destro del mouse su **ZENworks Icon**, selezionare **Applicazione tecnica**), la registrazione deve essere impostata su **Errori, avvisi, informazioni, debug**.
2. Dopo aver modificato il livello di log nell'agente, assegnare qualsiasi task rapido o aggiornamento del sistema.
3. Il messaggio di errore **"TaskNotifier, errore 503 ricevuto dal server"** viene registrato nel file `zeus-messages.log` (ubicazione: `%ZENWORKS_HOME%\ZeUS\logs\`).

Il messaggio di errore **"TaskNotifier, errore 503 ricevuto dal server"** indica che il server ha rifiutato la connessione in quanto la capacità di default (10000) è quasi piena.

Questo errore si verifica quando il numero di agenti che si connettono a un server è maggiore rispetto al numero di *maxConnections* nel file `server.xml`. Per default, il numero di *maxConnections* è 10000.

**Soluzione:**

Aggiungere il numero del parametro *maxConnections* nel file `server.xml`.

**Per aggiungere il numero di maxConnections nel file server.xml:**

1. Aggiungere il parametro maxConnections="20000" nella riga seguente, come illustrato sotto:

   *<!-- Define a non-SSL HTTP/1.1 Connector on port 80 --> <Connector acceptCount="1000" connectionTimeout="60000" maxConnections="20000" disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="600" minSpareThreads="25" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol" redirectPort="443" />*

   ---

   **Nota:** per default, il numero del parametro maxConnections è 10000 e non sarà elencato nel file server.xml. Se il numero 10000 non è sufficiente, aggiungere il parametro e aumentare il numero in base al numero di agenti nella zona. In questo esempio, il numero di maxConnections è 20000.

   ---

2. Riavviare i servizi ZENworks.

## Il servizio novell-proxydhcp potrebbe non funzionare nel server satellite di imaging RHEL 7.5 e 7.6

Il servizio *novell-proxydhcp* potrebbe non funzionare in RHEL 7.5 e 7.6, in quanto la porta 67 richiesta *dal* servizio viene utilizzata dal servizio *dnsmasq*.

Soluzione: eseguire il comando `systemctl disable libvirtd.service`, quindi riavviare il dispositivo.

# Documentazione aggiuntiva

Questo documento contiene informazioni specifiche per la release ZENworks 2017 Update 4. Per il resto della documentazione ZENworks 2017, consultare il *sito Web della documentazione di ZENworks 2017*.

# Note legali

Per ulteriori informazioni sulle note legali, i marchi, le dichiarazioni di non responsabilità, le garanzie, le esportazioni e altre limitazioni di utilizzo, i diritti del governo degli Stati Uniti, le norme sui brevetti e la conformità FIPS, consultare https://www.novell.com/company/legal/.