UNITRENDS
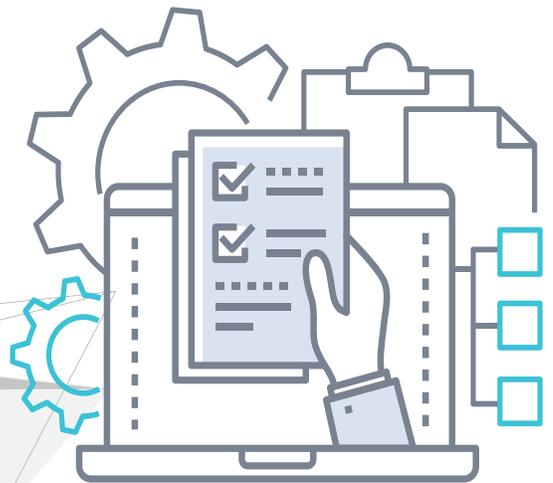
Upgrade Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup

Release 10.8.2 | Document Version 1.05082024

Copyright

Contents

Introduction

Release 10.8.2 includes enhancements and updated agents for Windows and Linux. Unitrends recommends upgrading to the latest version to benefit from new features and performance enhancements. This document provides instructions for upgrading to the Unitrends 10.8.2 release. For details on fixes included in this release, see the Release Notes for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

> **Note:** New appliance network requirement – Beginning in release 10.7.10, updates to backup and backup copy components require access to kaseyagroup-appliance-registry.jfrog.io. Before upgrading your appliance, open port 443 outbound to kaseyagroup-appliance-registry.jfrog.io for the HTTPS protocol.

New features in past releases

Upgrading to 10.8.2 includes any new features that have not yet been installed. The following features were added in recent releases:

- **On-box IR management controls** – Release 10.8.1 added VM controls for Instant Recovery of image-level backups, including CPU and RAM configurations and power management. These controls enable VM management right from the Unitrends UI for IRs that are running on the Unitrends appliance. For details, see Instant recovery of Windows image-level backups in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

- **Improved VMware integration (VMware 7 and 8)** – Release 10.8.1 added enhancements ensuring optimal performance and compatibility.

- **Windows agent** – Windows agent release 10.8.1 added these new features:

    - **Installation and deployment** – Installer validations for silent installs (RMM agent deployments, GPO, etc.) for improved deployment flexibility.

    - **Logging optimization** – Enhanced compatibility checks between agent and appliance versions for troubleshooting.

- **New Delete Final Backup setting for the 30-day retention policy** – For appliances imaged with release 10.7.11 or higher, the 30-day default retention policy enables the appliance to purge any backup that is no longer held by the retention policy. If needed, you can opt to retain an asset's last available recovery point by unchecking the **Delete Final Backup** box in the Edit Retention Policy dialog. For details, see Managing retention with long-term data management in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

- **Re-pairing of Windows and Linux agents** – Release 10.7.9 added a **Re-Pair** button on the **Configure > Protected Assets** tab that you can use to establish a secure pairing between the asset and its appliance. For detailed requirements and procedures, see Secure agent pairing for Windows and Linux agents in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

- **Copy backups to your Azure environment** – Beginning in release 10.7.9, you can store copies of your backups in your Azure environment. Simply add the Azure Blob storage container to your Unitrends appliance as a backup copy target, then add a job to copy backups to this container.

UNITRENDS
A Kaseya COMPANY

- **Secure agent pairing status** – Release 10.7.8 added a pairing status column to the **Configure > Protected Assets** tab. The asset's pairing status is updated when a backup runs, during an inventory sync, or any time the asset is re-saved. You can refresh the pairing status that is displayed on the Protected Assets tab by manually re-saving an asset or performing an inventory sync.

- **30-day retention policy** – Appliances imaged with release 10.7.8 or higher are configured with a default backup retention policy of 30 days. This 30-day policy is applied to each protected asset.

- **SQL Server 2022 on Windows** – Release 10.7.8 added support for protecting your SQL 2022 environment with application backups. To run application backups, the SQL server must be running Windows 2022 and agent version 10.7.8 or higher. The Unitrends appliance must be running release 10.7.8 or higher.

- **VMware 8.0** – Release 10.7.7 added support for deploying the Unitrends Backup appliance to vCenter 8.0 or ESXi 8.0. For details, see the Deployment Guide for Unitrends Backup on VMware.

- **VMware 8.0** – Release 10.7.5 added support for host-level backups of virtual machines hosted in vCenter 8.0 or ESXi 8.0.

  For host-level protection of VMware 8.0 environments, the Unitrends appliance must be running release 10.7.5 or higher. For additional requirements, see VMware virtual machines in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

- **Automated secure pairing of Unitrends Linux agents and support for new Linux versions** – Beginning in Linux agent release 10.7.5, a secure pairing is automatically established between the appliance and the Linux agent on each of its protected assets. This pairing enables Transport Layer Security (TLS) to encrypt data and authenticate connections between appliances and agents. Communication between appliances and agents is only allowed if there is a matching (paired) certificate. For details, see "Automated secure pairing of Unitrends Linux agents".

  The 10.7.5 agent is required for protection of these 64-bit Linux versions: Alma Linux 9, Debian 10, CentOS 9, OpenSUSE 42, RHEL 9, Rocky Linux 9, and Ubuntu 22.04.

- **Nutanix AHV 6.5** – Release 10.7.4 added support for Nutanix AHV hypervisor version 6.5. You can protect virtual machines that reside on an AHV 6.5 hypervisor by running host-level backups and deploy a Unitrends Backup virtual appliance to AHV 6.5.

- **UniView restrict local UI access** – UniView allows users to restrict local access to the Unitrends appliance on the local network. This feature applies to appliances running release 10.7.2 or higher. The appliance UI and management functions can still be accessed through UniView. Disabling local access enforces MFA, significantly reduces potential security exposure, and allows admins greater access controls through roles and scopes in UniView. For details, see *Disable or enable local network access to an appliance* in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends BackupAppliance settings topic.

- **Nutanix AHV 5.20** – Release 10.7.0 added host-level support for Nutanix AHV 5.20 environments.

- **Automated secure pairing of Unitrends Windows agents** – Beginning in Windows agent release 10.6.6, a secure pairing is automatically established between the appliance and the Windows agent on each of its protected assets. This pairing enables Transport Layer Security (TLS) to encrypt data and authenticate connections between appliances and agents. Communication between appliances and agents is only allowed if there is a matching (paired) certificate.

  This feature blocks any communication with Unitrends agent software that doesn't originate from a paired appliance (think of a Bluetooth headset, if it's not paired or in pairing mode, no one else can communicate with it).

This eliminates the threat of a rogue appliance running backups or code against an agent.

- **Windows backup** – To provide more resilient backups, backup jobs run with agent 10.6.4 or later attempt to create a Volume Shadow Copy in cases where the VSS writer is in a retryable state.

- **APC UPS support for Recovery Series appliances** – During a power outage, the Unitrends Recovery Series appliance needs to be shutdown cleanly. Beginning in release 10.6.4, you can use your APC UPS to issue a clean shutdown for Recovery Series appliances running on CentOS 7 or CentOS 6 Linux. See this article for details: Issue a clean shutdown from an APC UPS.

- **Windows Server 2022 and Windows 11** – Release 10.6.2 extended Windows support to include file-level and image-level protection of Windows Server 2022 and Windows 11. To protect these Windows environments:

  - The Unitrends appliance must be running release 10.6.2 or higher.

  - The Windows asset must be running agent release 10.6.2 or higher.

> **Notes:**
>
> - The following Windows Server 2022 features are not yet supported:
>
>   - Nano Servers (this deployment option does not install VSS components, which are required for agent backups)
>
>   - Windows Containers, such as Kubernetes clusters
>
>   - Shielded VMs
>
>   - Storage Spaces Direct
>
>   - Hyper-Converged Infrastructure (HCI) deployments

Upgrading to Release 10.8.2

Use these procedures to upgrade your appliances and protected assets to release 10.8.2.

Perform upgrade procedures in order and follow best practices for a successful upgrade. An overview of the upgrade process is given below. See the procedures that follow for instructions on upgrading your appliances and protected assets.

Step 1: Review the "Upgrade requirements and considerations".

Step 2: Upgrade the Unitrends appliance(s) as described in "Upgrading appliance software".

Step 3: Review new agent releases and upgrade agents as described in "Upgrading agent software".

For additional information, refer to these resources:

- Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup

- Release Notes for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup

- Latest Agent Releases on the Unitrends Downloads page.

UNITRENDS
A Kaseya COMPANY

Release 10.8.2 | May 2024

Upgrade requirements and considerations

Review the following table before upgrading to release 10.8.2.

Requirement or consideration	Description
Support contract	An active support contract is required to upgrade the appliance.
Backup copy target appliance	Upgrade the backup copy target appliance before upgrading its source appliance. For backup copies, the target must be running either the same version or a newer version than the source appliance. Although the source appliance can be on an older version than the backup copy target, it is highly recommended that you upgrade all appliances to the latest release to ensure optimal performance.
Remotely managed appliance	If an appliance is being remotely managed by another Unitrends appliance, the managing appliance must be upgraded first. **Note:** Support for managing CentOS 6 appliances using the Remote Appliance Management feature has been discontinued. As an alternative, please utilize UniView.

Requirement or consideration	Description

SMB 2.0	The SMB 2.0 security option is enabled by default on Unitrends appliances that were originally imaged or deployed with version 10.4.8 or higher.
	
	Notes:
	
	• The SMB 1.0 security option is enabled by default on appliances that were originally imaged or deployed with a pre-10.4.8 version. Upgrading from a pre-10.4.8 version does not change this SMB 1.0 setting.
	
	• See How Unitrends supports SMB2 for SMB 2.0 configuration procedures.
	
	The following requirements apply to appliances configured with SMB 2.0:
	
	• Oracle on Solaris – The Unitrends agent must have access to the appliance's SMB 2.0 Samba share to perform backup and recovery operations. These requirements apply:
	
	  – A Samba client must be enabled. See Oracle Database on Solaris: Samba Service Not Enabled for details.
	
	  – A Samba key must be added for the backup appliance. To add the key, issue this command (the default password is *samba*):
	
	```smbadm add-key -u samba@<applianceIP>```
	
	• Oracle on Windows – SMB 2.0 must be enabled on the Windows server so that the Unitrends agent can access the appliance's SMB 2.0 Samba share when performing backup and recovery operations.
	
	• Recover files from host-level backups of Windows VMs – To use a CIFS share for the recovery, SMB 2.0 must be enabled on the target Windows asset.
	
	• SharePoint – To perform backup and recovery operations, SMB 2.0 must be enabled on each node in the farm.
	
	Notes:
	
	• SharePoint 2007 on Windows 2003 and prior is not supported on SMB 2.0 appliances. (To configure your appliance to use SMB 1.0, see How Unitrends supports SMBv2.)
	
	• SharePoint may require custom client configuration for use with SMB 2.0. If SharePoint backups do not run successfully, see this Microsoft article for client configuration details: SharePoint Ports, Proxies and Protocols...An overview of farm communications.
	
	• Windows agent push – To push install the Windows agent, SMB 2.0 must be enabled on the Windows asset.

Release 10.8.2 | May 2024

Requirement or consideration	Description
	• Windows replica on Hyper-V – To run a Windows replica on Hyper-V, SMB 2.0 must be enabled on the Hyper-V server.
Upgrading an appliance that cannot connect to the Internet	To upgrade an appliance that cannot connect to the Internet, you can use an ISO image. Follow the instructions in this article: How to upgrade the appliance via Unitrends' media.

Upgrading appliance software

Make sure that there are no jobs running prior to upgrading your appliance. Once the upgrade begins, any running jobs terminate.

Note:	To upgrade the appliance from version 10.2 or earlier, additional steps are required. For details, see Upgrade fails when upgrading from version 10.2 or older.

To upgrade the appliance

Note:	Beginning in release 10.7.10, updates to backup and backup copy components require access to kaseyagroup-appliance-registry.jfrog.io. Before upgrading your appliance, open port 443 outbound to kaseyagroup-appliance-registry.jfrog.io for the HTTPS protocol.

1 Open a browser and connect to your appliance by entering: *https://<applianceIPaddress>/ui/*. For example: https://10.10.10.1/ui/.

2 Log in using the administrative login (e.g., user *root*).
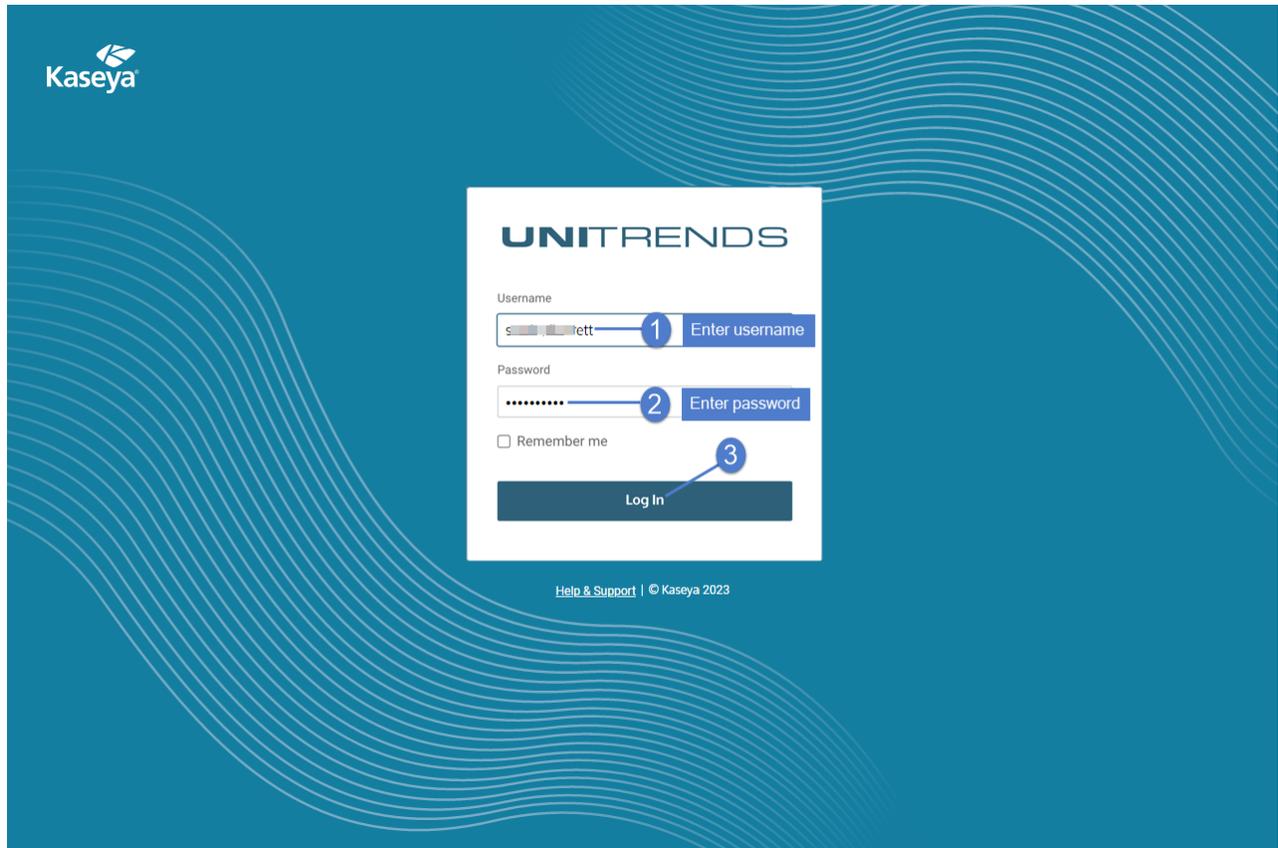
3   Click the gear icon and select **Check for Updates**.
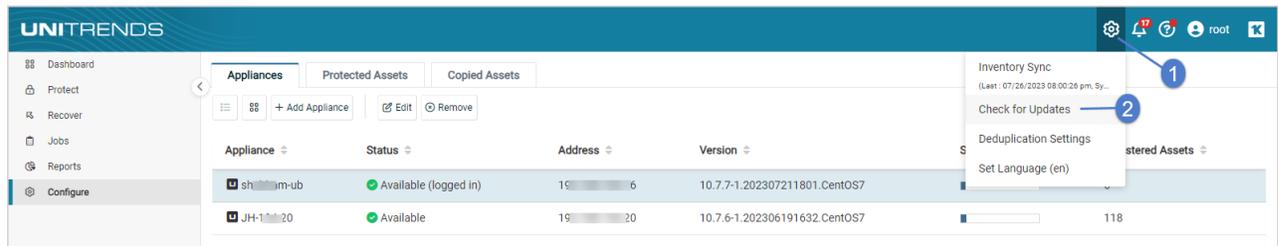
4   A list of available updates displays. Click **Update** to begin the installation.

Note: If you see the 🔴 icon, contact Unitrends Support for assistance.
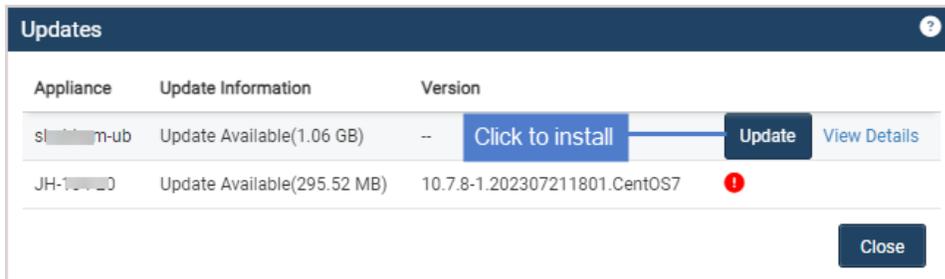
5   For some appliances, software maintenance is required with the update. If so, you see this message and the update will take some extra time:

> **Note:**   If you do not see this message, maintenance has already been performed on the appliance.
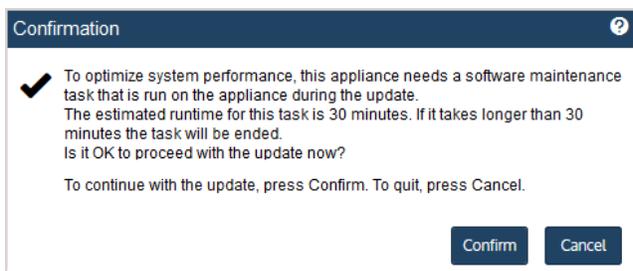
Do one of the following:

- Click **Confirm** to continue with the update.

- Click **Cancel** to quit. (You can then install the update at another time.)

6   During the upgrade, you see status messages as packages are installed. If you have trouble with the installation, see "Troubleshooting the Upgrade" for tips. After the installation completes:

- Clear your browser cache, then close the browser.

- Open the browser and log back in to continue working with your appliance.

> **Notes:**
>
> - Rebooting the Unitrends appliance is recommended upon upgrading to this release.
>
> - If you receive a message indicating that you need to reboot the appliance to take advantage of the new kernel installed during the upgrade, you can either reboot now or reboot at a later time.
>
> - If you reboot now, do the browser steps above after the appliance boots.

Upgrading agent software

After upgrading your appliance, upgrade the agent software on its protected assets. It is best practice to upgrade agents to the latest release to take advantage of performance enhancements and fixes. (For details on each fix, see the Release Notes for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.)

Release 10.8.2 includes the following agents:

- Windows 10.8.2 agent – The 10.8.2 agent is recommended for most Windows assets and is required for Windows fixes in this release. See "Installing or upgrading the Windows agent" for details.

- Linux 10.8.2 agent for the distributions listed below. See "Installing or upgrading the Linux agent" for details on upgrading the Linux agent.

  - Alma Linux 9, 64-bit
  - CentOS 7, 64-bit
  - CentOS 9, 64-bit
  - Debian 10, 64-bit
  - OpenSUSE 42, 64-bit
  - Oracle Linux 8.1, 64-bit
  - RHEL 7, 64-bit
  - RHEL 8.4, 64-bit
  - RHEL 9, 64-bit
  - Rocky Linux 9
  - SLES 11 SP3, 64-bit
  - SUSE 15, 64-bit
  - Ubuntu 22.04, 64-bit

For instructions on installing and upgrading agents for other operating systems, see Unitrends agents in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup. For a complete list of agents, see the Latest Agent Releases on the Unitrends Downloads page.

Installing or upgrading the Windows agent

To protect a Windows asset, the Windows agent must be installed on the asset. The Hyper-V, SQL, and Exchange components are included in the Windows agent.

Windows agent updates can be pushed to assets from the appliance or installed manually. Updating the agent updates all applicable components in *Unitrends_Agentx86.msi* or *Unitrends_Agentx64.msi* during installation.

Note: If you have trouble installing the agent, look at the application messages in the Windows event viewer to address the error. For details, see this KB article: Troubleshooting Windows event IDs.

Windows agent requirements and considerations

The following requirements must be met before installing the Windows agent:

- The Unitrends appliance(s) protecting the Windows asset must be running an equal or higher version than the agent that will be installed. Beginning in release 10.8.1, the agent installer enforces version compatibility by raising an error if the appliance version is older than the agent.

- Administrative privileges for the user installing the agent.

- Approximately 1100 MB of free space on the Windows system drive, usually volume *C:*.

- Single Instance Storage (SIS) on Windows Storage Server 2008 is not supported and must be disabled for the agent to properly perform backups.

- The Windows Volume Shadow Copy Service (VSS) framework must be installed.

- To protect Exchange, SQL Server, or Hyper-V, the following VSS writers are required:

  - VSS Exchange Writer is required for the Exchange agent.

  - VSS SQL Writer is required for the SQL Server agent.

  - VSS Hyper-V Writer is required for the Hyper-V agent.

- Agent operations use ports 1743, 1745, and 888. Ensure that these ports are not in use on the Windows asset.

  > **Note:** Unitrends does not officially support backup through firewalls. For details, see this KB article: Backup fails through Router, DMZ, or Firewall.

- Secure agent pairing requirements – Beginning in release 10.6.6, a secure pairing is automatically established between the appliance and the Windows agent on each of its protected assets. This pairing enables Transport Layer Security (TLS) to encrypt data and authenticate connections between appliances and agents. Communication between appliances and agents is only allowed if there is a matching (paired) certificate.

  These secure pairing requirements must be met to protect Windows assets with agent release 10.6.6 or higher:

  - The Unitrends appliance must be running release 10.6.6 or higher.

  - The Windows asset must be running agent release 10.6.6 or higher.

  - The Unitrends appliance version must be equal to or higher than the Windows agent version.

    > **IMPORTANT!** Be sure to upgrade your Unitrends appliance before upgrading your Windows agents.
    >
    > - Jobs will fail if you attempt to protect a 10.6.6 or higher agent with an appliance that is running an older release.
    >
    > - You cannot add an asset that is running a 10.6.6 or higher agent to an appliance that is running an older release. If you attempt this, you receive an error similar to: *Failed to save client: Registration for client* assetName *failed. The Unitrends System could not connect to the Unitrends Agent on* assetName*. Please ensure that the Agent software is installed on* assetName*, the Agent service is running (if applicable), and no firewall settings are preventing access*.

  - If upgrading from a pre-10.6.9 agent release, backups may fail until the pairing completes successfully (this can take up to two hours).

- To protect Hyper-V clusters, SQL clusters, or file server clusters with the secure agent pairing feature:

  - The cluster must be running agent version 10.6.9 or higher.

  - The Unitrends appliance and cluster must be running in the same time zone.

- The secure agent pairing feature is not used to protect Windows XP, 2003, and Vista. To protect a Windows XP, 2003, or Vista asset, install agent version 10.6.7 or higher. The 10.6.7+ agent detects the asset's OS version and disables secure agent pairing.

For details on working with this feature, see Secure agent pairing for Windows and Linux agents in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup

- Image-level backups – If upgrading from a pre-10.6.3 agent release, the asset's next Windows image-level backup is promoted to a full.

- The Windows agent does not require rebooting after updating as of version 10.6.1. A reboot is required if you upgrade from an agent before 10.6.1.

Upgrade and installation procedures

Windows agent updates can be pushed to assets from the appliance or installed manually for environments that do not support push installation. Use one of the following procedures to install or upgrade the Windows agent. The same procedure is used whether you are installing the agent for the first time or upgrading an existing agent.

- "Push installing agent updates"

- "Manually installing or updating Windows agent"

Push installing agent updates

Pushing updates to Windows assets greatly reduces administration time and ensures that the latest protection software is running on your assets.

See the following topics for details:

- "Requirements for pushing agent updates"

- "To push install agent updates"

Requirements for pushing agent updates

In addition to the general "Windows agent requirements and considerations" above, the following prerequisites must be met before pushing Windows agent updates:

Item	Description
Windows versions supported	These Windows versions are supported: • Windows Server – 64-bit Windows 2008 R2 and later versions listed in the Compatibility and Interoperability Matrix are supported. (32-bit versions are not supported.) • Windows Workstation – 64-bit Windows 7 and later versions listed in the Compatibility and Interoperability Matrix are supported. (32-bit versions are not supported.) Windows agent push is NOT supported for Azure virtual machines. **Note:** A known Microsoft issue may prevent successful agent push install on Windows 7 and Windows 2008 R2 systems. To resolve this issue, see the following Microsoft knowledge base article: The "Untrusted publisher" dialog box appears when you install a driver in Windows 7 or Windows Server 2008 R2.
Credentials	Trust credentials must be defined for the asset on the backup appliance. **To add a credential** 1 Click **Configure > Protected Assets > Manage Credentials > Add**. 2 Enter credential information and click **Save**. **To apply the credential to an asset** 1 Select **Configure > Protected Assets**. 2 Click to select the desired asset. 3 Click **Edit**. 4 Select the desired credential and click **Save**.

| Item	Description

Windows environment	The Windows machine must be configured with the following settings:
	
	Note: For troubleshooting steps, see [Troubleshooting Agent Push](#).
	
	• *Workstation* and *Server* services must be running and set to automatic restart.
	
	• The Windows asset must be able to access the appliance's Samba share:
	
	  – SMB 2.0 – Backup appliances running release 10.4.8 or higher are configured to use SMB 2.0 by default. SMB 2.0 must be enabled on the Windows asset.
	
	  – SMB 1.0 – Backup appliances running a pre-10.4.8 release are configured to use SMB 1.0 by default. SMB 1.0 must be enabled on the Windows asset.
	
	• For Windows 7 and later, *Network discovery* and *Printer and File Sharing* must be enabled for the current network profile (in **Control Panel > Network and Sharing Center**).
	
	• Trust credentials entered in the Add Asset dialog in the Unitrends UI must have administrative privileges. On systems with user account controls (UAC) enabled, at least one of the following must also apply:
	
	  – The trust credentials entered are for a domain administrator account.
	
	  – The trust credentials entered are for a system local administrator account. Being a different member of the Administrators group is insufficient, it must be the built-in account to bypass UAC. If the administrator account is disabled, enable it by executing the following in an elevated command prompt:
	`net user administrator /active:yes`
	
	  – The Registry key *LocalAccountTokenFilterPolicy* exists and is set to **1** (to use a local administrator that is not the 'Administrator' account).
	
	• Verify Remote IPC and Remote Admin shares are enabled. These shares should be enabled with File and Printer Sharing, but verifying is a good idea if you're still having trouble. To verify, issue the following command from an elevated command prompt and check the output for ADMIN$ and IPC$: **net share**
	
	• Firewall rules must allow inbound and outbound traffic between both machines. Default Windows firewall rules limit many services to the subnet. If the backup appliance is outside the Windows asset's subnet, modify firewall *Printer and File Sharing* settings (TCP ports 139 and 445) to allow communication between the systems.

Push install update notifications

Any time an agent update is available for Windows assets, a notification displays in the Alerts area of the Global menu. Note that alerts display only for assets that meet the push install requirements described above.
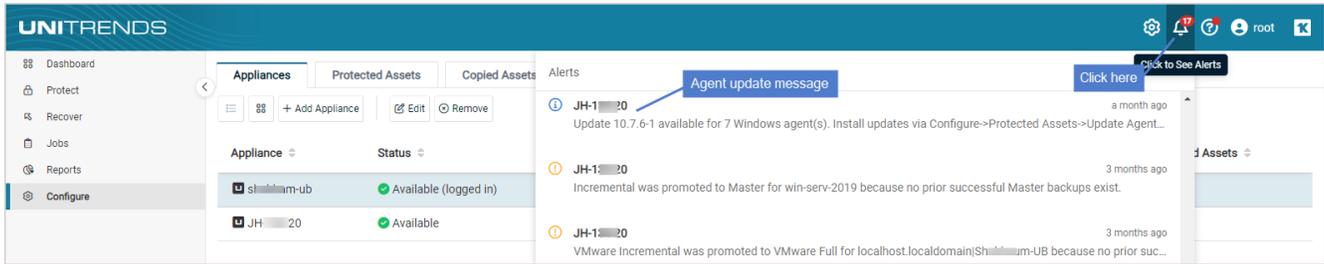
To push install agent updates

Use this procedure to update the Windows agent.

1   Select **Configure > Protected Assets**.

2   All protected assets display. Check the Agent Version to see the agent that is currently installed.

3   Do one of the following:

- To install available updates on all eligible assets, select **Update Agent > Update All**.
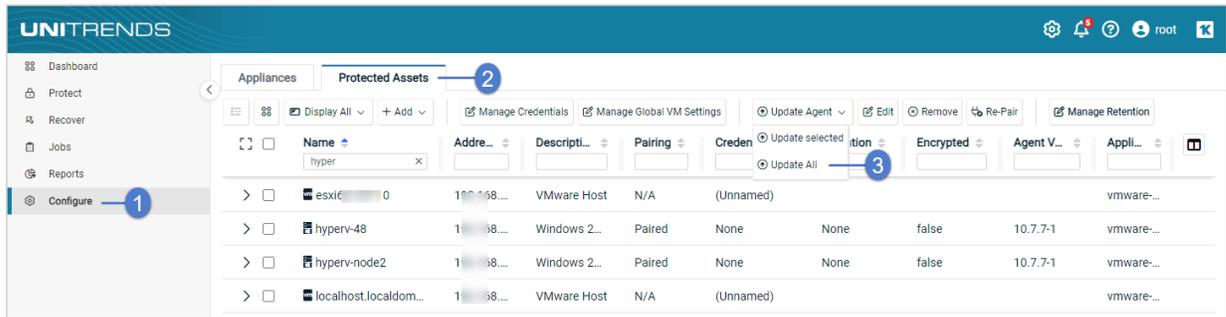
- To install available updates on a subset of eligible assets, check boxes to select assets to update, then select **Update Agent > Update selected**.
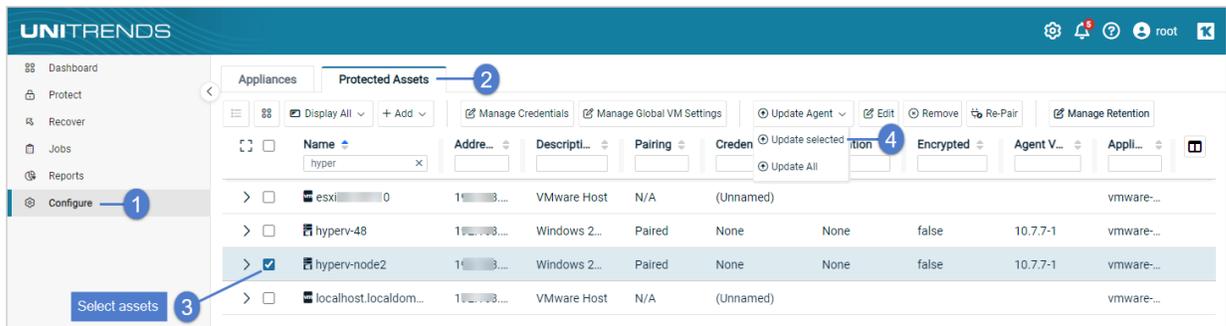
4   Updated agents are installed on all selected Windows assets meeting these conditions:

- Trust credentials are valid.

- No backup or recovery job is currently in progress or scheduled to run soon for the asset.

- Push update requirements have been met (see "Requirements for pushing agent updates").

- Updates are available for the asset (asset is not running the latest agent release).

- The Unitrends appliance(s) protecting the Windows asset is running an equal or higher version than the agent that will be installed.

  > **Note:** If you see this error, the Windows asset is paired to an appliance running an older version than the agent you're trying to install: *Appliance version validation failed. Please verify all paired appliance versions meet or exceed the agent*. Update the appliance to enable the push-install.

If applicable, the following are also updated (if new versions are present):

- For Hyper-V servers or Windows servers with the Hyper-V role enabled, the Hyper-V CBT driver is updated. This driver is used for faster Hyper-V incremental backups. (You do not need to reboot to enable this driver.)

- For Microsoft SQL and Exchange servers, SQL and Exchange components are updated. These are used to run application backups for these databases.

- For Windows assets that are eligible for image-level backups, the Windows Volume CBT driver is installed or updated if an update is available. This driver is used to enable incremental image-level backups. To enable this driver, you must reboot the Windows asset after installing the Volume CBT driver for the first time or after updating from a pre-10.3.3 agent version. (The last driver update was in agent version 10.3.3. If you are updating agent version 10.3.4 or later, a reboot is not required.)

5   If the Windows server uses Windows deduplication, run a new full backup.

Manually installing or updating Windows agent

Use the following procedure to install or upgrade the Windows agent. The same procedure is used whether you are installing the agent for the first time or upgrading an existing agent.

> **Notes:**
>
> This install procedure cannot be used in the following cases:
>
> - To install the agent on a Windows 2008 server that was deployed with the server core option. Instead, see Command-line installer for Windows agents in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.
>
> - To install to multiple Windows machines by using Windows Group Policy. Instead, see Agent deployment using Group Policy in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.
>
> If you are running Hyper-V incremental backups and are upgrading from a pre-10.1.0-3 agent version:
>
> - You must manually uninstall the older Windows agent before installing the latest agent. (In all other cases, it is not necessary to uninstall existing agent software.)
>
> - Uninstall the older agent by using the Windows Add/Remove Programs interface. For details, see To uninstall the Windows agent in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

To install or upgrade the Windows agent manually

1   Log in to the Windows asset as a user that has full access to all files and folders on the system (e.g., local administrator).

2   Download the agent MSI file from https://helpdesk.kaseya.com/hc/en-gb/articles/4407526882193-Unitrends-Downloads. (If you do not have Internet access, see "To download the Windows agent without Internet access".)

   • For the 64-bit agent, click the **MSI** link in the Windows row.

   • For the 32-bit agent, click the **Link** in the Legacy Agents row. On the Legacy Agents page, click the **Link** in the 32-bit Agents row. On the 32-bit Agents page, click the **MSI** link in the Microsoft Windows row.
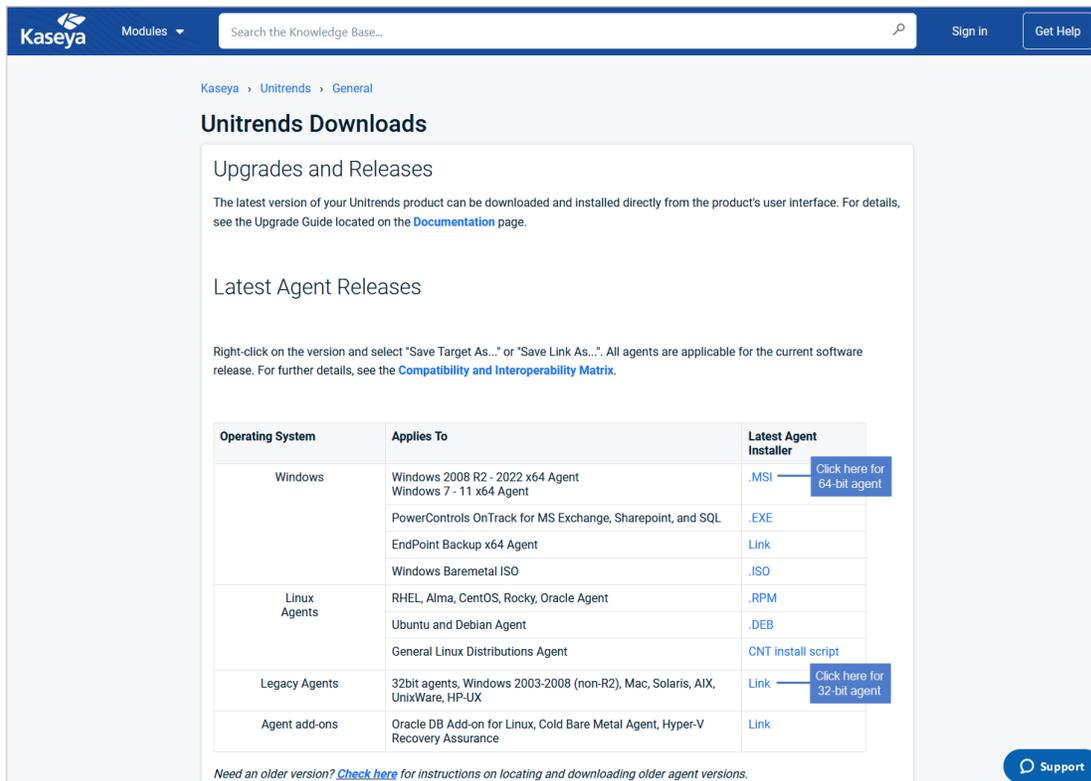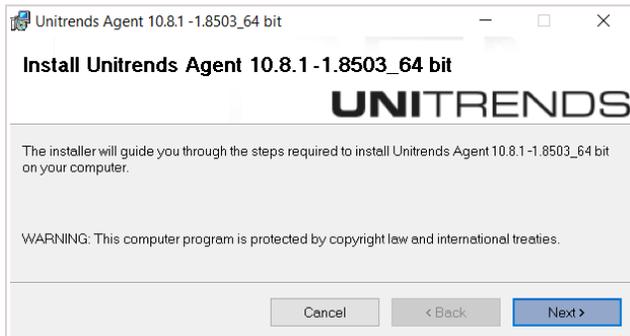

3   Double-click the MSI file to launch the installer.

   MSI file names:

   • *Unitrends_Agentx64.msi* – agent for 64-bit Windows assets

   • *Unitrends_Agentx86.msi* – agent for 32-bit Windows assets
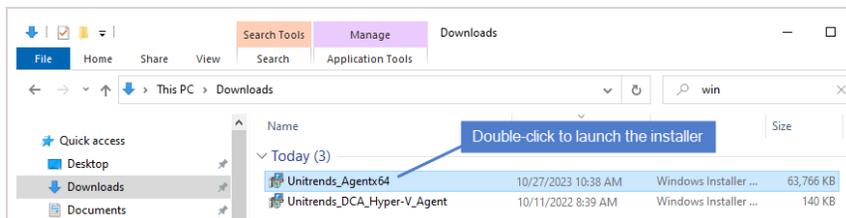
4   Click **Next** to proceed.

5   Click **Next** to begin the installation process. The installation can be interrupted at any time by clicking **Cancel**.

> **Note:**   If you receive the message *The currently installing agent version is newer than the appliance version*,
>   click **Yes** to proceed with the installation or click **No** to exit. If you proceed with the installation, be sure
>   to upgrade the older appliance as soon as possible. Running an appliance version older than the agent
>   is not supported and can cause undesirable results.
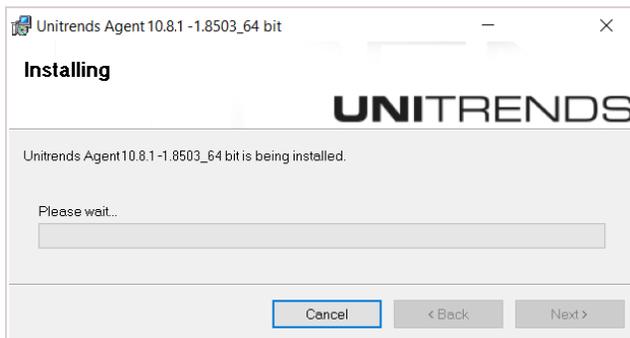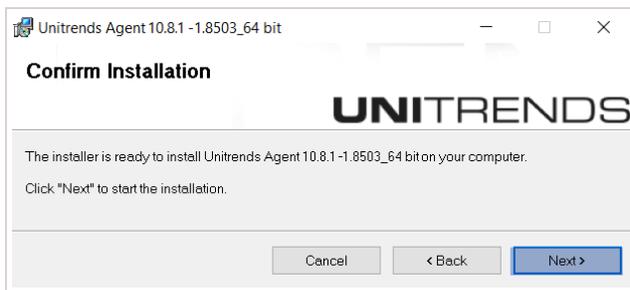
6   (Recommended) Click **Yes** to include the Windows Volume CBT driver. (This driver enables the option to run
     incremental image-level backups. You can run file-level backups and full image-level backups without installing
   this driver.)

> **Note:**   If the latest Windows Volume CBT driver is already installed, the Unitrends CBT Driver Install window
>   does not display.
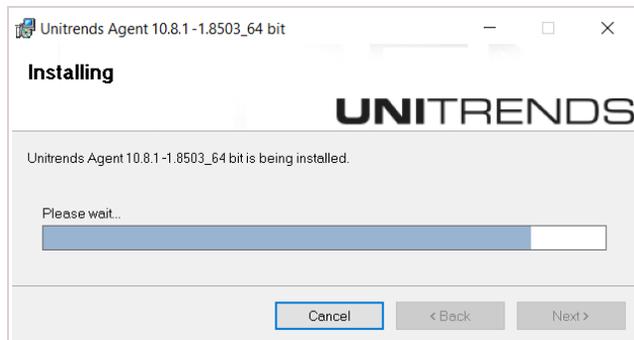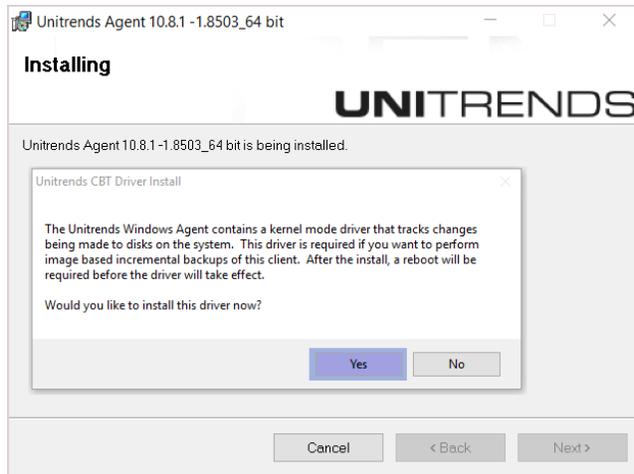
Note:	The agent is installed to the *PCBP* directory on the Windows system drive, usually volume *C:* (e.g., *C:\\PCBP*).

7   After the agent is installed, do one of the following:

- If you did not opt to install the Volume CBT driver, installation is complete. Click **Close** to exit the installer.

  OR

- If you opted to install the Volume CBT driver, click **Next** and continue with the next step in this procedure.
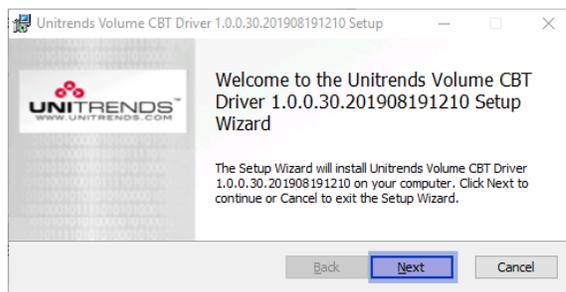
Notes:

- If this Volume CBT driver version has already been installed, the Unitrends Volume CBT Filter Driver Setup installer does not display. Windows agent installation is complete. If needed, reboot the Windows asset to enable the existing Volume CBT driver.

- If an older Volume CBT driver version has already been installed, you are given the option to install this driver version and advised as to whether the new driver is required for subsequent incrementals.

- If a newer Volume CBT driver version has already been installed, you are given the option to install this older driver version.

8   Click **Install** to begin the installation process (or click **Back** to review or modify data). The installation can be interrupted at any time by clicking **Cancel**.
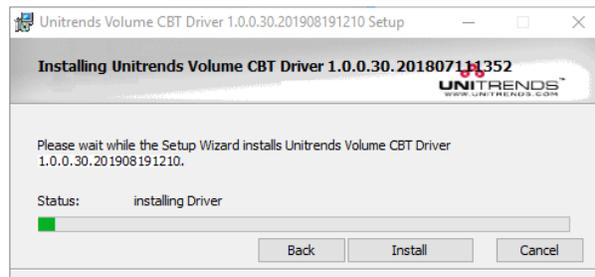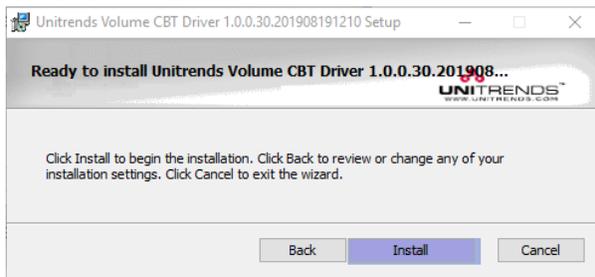
9   Click **Finish** to exit the installer.
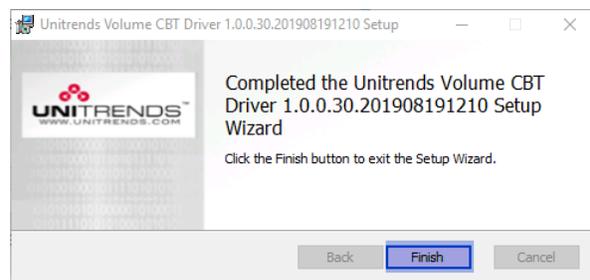
10   (If needed) If installing the driver for the first time or updating from a pre-10.3.3 agent release, you must reboot the Windows asset to enable the Volume CBT driver. Click **Yes** to reboot now or **No** to reboot at a later time.
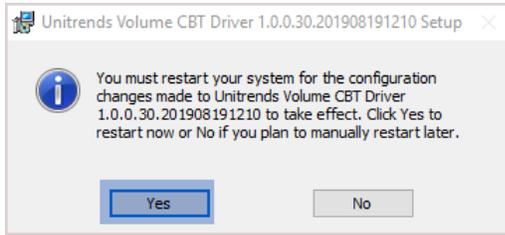
Notes:

- If the Volume CBT driver has not been installed or has not been enabled, image-level incrementals are not supported. Any scheduled incremental is automatically promoted to a full backup. If you attempt to run an on-demand incremental, you receive a message indicating that only full backups are supported.

- An image-level incremental is automatically promoted to a full backup in these other cases:

  - There is a problem detected with the Volume CBT driver.

  - A newer Volume CBT driver version is installed but has not been enabled. To run incremental backups, enable the new driver by rebooting the Windows asset.

  - The version of the Volume CBT driver that was included with the Windows agent is greater than the version that is enabled on the Windows asset. To run incremental backups, you must install the new driver and then reboot the Windows asset (see the next bullet for details).

- The installer for the associated Volume CBT driver is placed in *C:\PCBP\Installers*. You can install this driver at any time by running the installer, called *uvcbt.msi*. After installing the driver, you must enable it by rebooting the Windows asset.

- The Windows agent and the Windows Volume CBT driver are installed as separate, independent packages. Uninstalling the Windows agent does not uninstall the Windows Volume CBT driver. (To uninstall the Windows Volume CBT driver, use the Windows Control Panel Add/Remove Programs feature to remove *uvcbt.msi*.)

To download the Windows agent without Internet access

1 Log in to the Windows asset as an administrator will full system access.

2 Launch File Explorer and enter the following path to access the new agent on the Unitrends appliance: **\\ApplianceIP\windows_agents**:
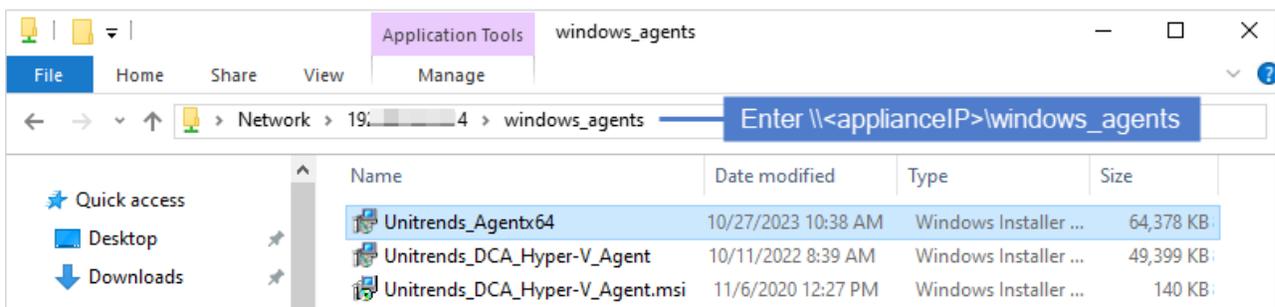
Do I need to run bare metal backups of my Windows asset?

There are two options for hot bare metal recovery (BMR) of Windows agent-based assets: Windows unified BMR (formerly known as *integrated BMR*) and Windows image-based BMR.

With Windows unified BMR, Unitrends provides Unified Bare Metal™ protection that enables you to perform disaster recovery (DR) right from a Windows file-level or image-level backup. This reduces recovery time, provides additional recovery points, increases on-appliance retention by eliminating the need for bare metal backups, and simplifies the Windows DR process. You perform unified BMR by using the Unified Bare Metal Recovery wizard and standard 32-bit and 64-bit ISO images, eliminating the need to create bare metal ISOs for each protected asset and keep them on-hand in case disaster strikes.

With image-based BMR, you must run bare metal backups and create a separate bare metal ISO for each Windows asset you want to protect. You perform image-based BMR by booting from the asset's bare metal ISO. Image-based BMR can protect older versions of Windows that are not supported by unified BMR. If you need to run bare metal backups, you must install the Windows bare metal agent as described in "To install the Windows bare metal agent".

It is recommended to use unified BMR where possible. However, in the following cases, unified BMR is not supported and you must use image-based BMR instead:

- To recover a Windows 2000 asset.

- To recover a Windows Server 2003 to dissimilar hardware.

Following is a high-level comparison of unified and image-based hot bare metal recovery. Use this information to determine which method to use for your Windows assets. For more on bare metal recovery, see Windows Bare Metal Protection and Recovery in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

Item	Unified BMR	Image-based BMR
Recovery Time Objective (RTO)	Faster recovery time than with image-based BMR.	Slower recovery time than with unified BMR.
Recovery Point Objective (RPO)	More recovery points available since you restore from any eligible file-level or image-level backup.	Fewer recovery points since you restore from a bare metal backup only.
Recovery types	Supports physical-to-virtual (P2V), virtual-to-physical (V2P), physical-to-physical (P2P), and virtual-to-virtual (V2V) DR.	Supports physical-to-virtual (P2V), virtual-to-physical (V2P), physical-to-physical (P2P), and virtual-to-virtual (V2V) DR.

Item	Unified BMR	Image-based BMR
Recovery of Windows Server 2016	Yes, recovering Windows Server 2016 to identical or dissimilar hardware is supported on appliances running Unitrends version 9.2 and higher. Recovery to dissimilar hardware is supported for file-level backups only.	No, recovering Windows Server 2016 assets is not supported.
Dissimilar recovery of Windows Server 2012	Yes, recovering Windows Server 2012 to identical or dissimilar hardware is supported. Recovery to dissimilar hardware is supported for file-level backups only.	Yes, recovering Windows Server 2012 to identical or dissimilar hardware is supported.
Dissimilar recovery of Windows Vista/Server 2008	Yes, recovering Windows Vista/Server 2008 to identical or dissimilar hardware is supported. Recovery to dissimilar hardware is supported for file-level backups only.	Yes, recovering Windows Vista/Server 2008 to identical or dissimilar hardware is supported.
Dissimilar recovery of Windows Server 2003	No, recovering Windows Server 2003 to dissimilar hardware is not supported. Recovery to identical hardware is supported.	Yes, recovering Windows Server 2003 to dissimilar hardware is supported for some distributions. See the Compatibility and Interoperability Matrix for details. Recovery to identical hardware is supported.
Dissimilar recovery of Windows XP	No, recovering Windows XP to dissimilar hardware is not supported. Recovery to identical hardware is supported.	No, recovering Windows XP to dissimilar hardware is not supported. Recovery to identical hardware is supported.
On-appliance retention	More on-appliance retention due to eliminating bare metal backups.	Less on-appliance retention due to bare metal backup storage.
ISO image/boot disk	Standard 32-bit and 64-bit ISO images used for most Windows assets; available on the Unitrends appliance.	Separate ISO required for each Windows asset; ISOs must be created manually with the Unitrends bare metal agent.
Bare Metal Interface	Simplified wizard interface enables DR to the desired point-in-time using a single process, decreasing overall recovery time. Leverages WinPE 10.0 for all Windows assets.	Two dialog-based interfaces (one WinPE 1.5 for older assets, one WinPE 2.0 for newer assets). Cannot perform DR in a single process.

Item	Unified BMR	Image-based BMR
Target disk size	For file-level backups, supports recovery of original Windows asset to a smaller disk size. (For details, see Prerequisites for file-level backups in Implementing Windows unified bare metal protection.) For image-level backups, must recover to a disk of an equal or greater size than that of the original asset. (For details, see Prerequisites for image-level backups in Implementing Windows unified bare metal protection.)	Must recover to a disk of an equal or greater size than that of the original asset.
UEFI-based assets	Supports recovery of UEFI-based assets.	Cannot recover UEFI-based assets.
GPT-partitioned assets	Supports recovery of GPT-partitioned assets.	Cannot recover GPT-partitioned assets.

To install the Windows bare metal agent

The bare metal agent is needed only for image-based bare metal protection. For most assets, you can use the newer unified bare metal protection feature, which does not require the bare metal agent. (For details, see "Do I need to run bare metal backups of my Windows asset?".)

Note: Special installation is required for assets that are running User Account Control (UAC). Do not use this install procedure for UAC assets. Instead, see Installing the bare metal agent on a Windows asset running User Account Control in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

1   Log in to the Windows asset as a user that has full access to all files and folders on the system (e.g., local administrator).

2   Download the agent MSI file from https://helpdesk.kaseya.com/hc/en-gb/articles/4407526882193-Unitrends-Downloads:

• Click the Agent Add-ons **Link**.

Release 10.8.2 | May 2024

- On the Agent Add-ons page, click the Bare Metal Agent **MSI**.

3   Double-click the *Unitrends_BareMetal.msi* file to launch the installer.
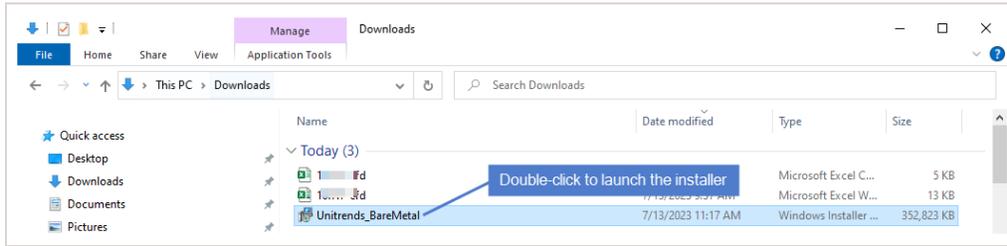
4   Click **Next** to proceed.
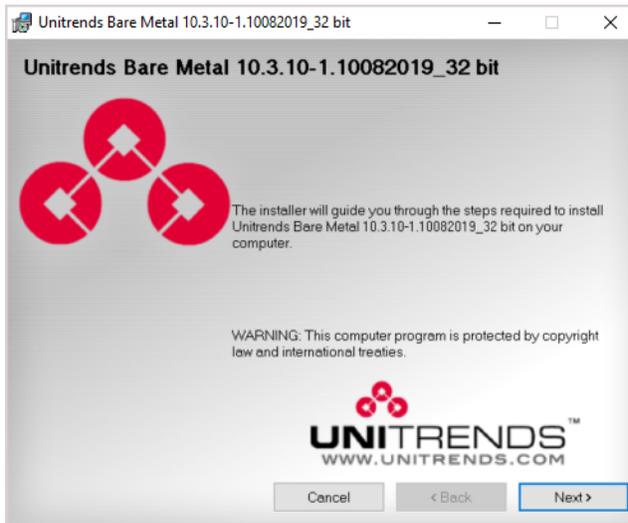
5   Click **Next** to install to the default location.

Installing to the default directory is strongly recommended. To install in another location (folder or volume), click **Browse** or manually enter the directory path.
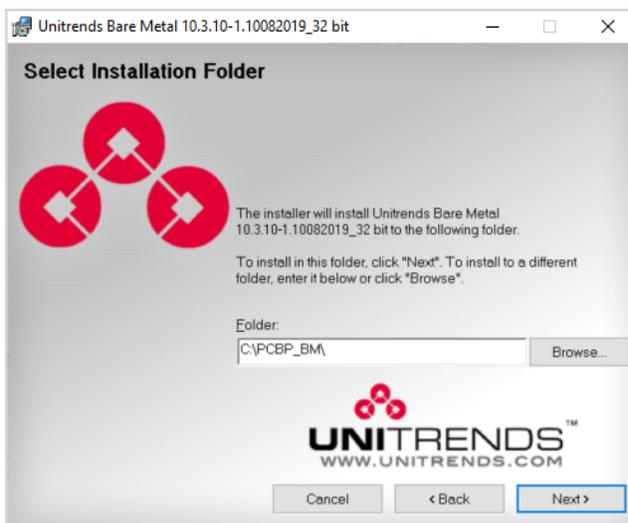
6   Click **Next** to begin the installation process. The installation can be interrupted at any time by clicking **Cancel**.

7   When installation is complete, click **Close** to exit the installer.

Installing or upgrading the Linux agent

To protect a Linux asset on a Unitrends appliance, the Linux agent must be installed on the asset.

Unitrends protects most Linux distributions, including CentOS, Debian, Red Hat, SUSE, and Ubuntu. Before adding a Linux asset to the Unitrends appliance, you must install an agent.

Once the agent is installed, you can update to a newer agent version using these same installation procedures. It is not necessar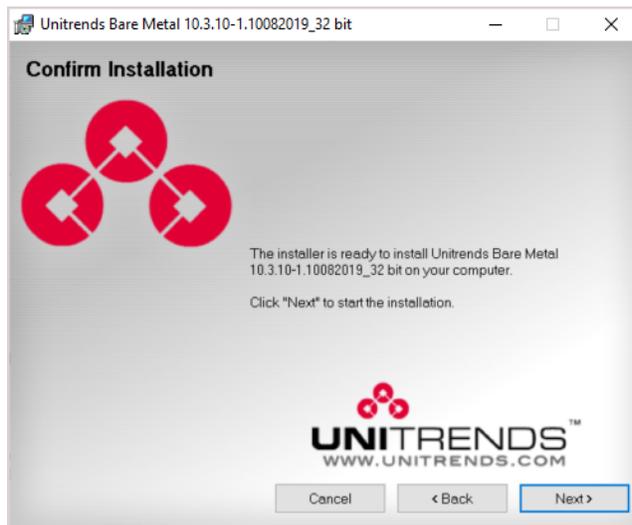y to remove the old agent. If an agent is already installed, you have the option to save any custom agent settings during installation.

Use the procedures in this section to install or update the Linux agent.

Preparing to install the Linux agent

Unitrends provides several Linux agent installers. Unitrends recommends using the RPM-based or dpkg-based installers when possible, so that needed dependencies are automatically installed with the agent. If these installers are not supported for your Linux distribution, use the GZEXE installers. With the GZEXE installers, you might need to install dependencies before installing the agent.

See "Linux distributions and agent installers" below to determine which installer to use for your Linux asset. You can download the agent installers from the Latest Agent Releases on the Unitrends Downloads page. You might not see an agent for the particular Linux distribution that you are using, but if it is a supported distribution listed in the Unitrends Compatibility and Interoperability Matrix, the standard Linux agent will work with your machine. For Oracle Linux assets, use the CentOS or Red Hat agent.

Linux distributions and agent installers

Linux distributions	Agent installers
• CentOS 64-bit • Oracle Linux 64-bit • Red Hat 64-bit	RPM-based installers. Automatically installs dependencies. For details, see "To install the Linux agent on CentOS, Oracle Linux, and Red Hat".
• All 64-bit distributions listed in the Unitrends Compatibility and Interoperability Matrix	GZEXE installers. For details, see "To install the Linux agent using GZEXE".
• Ubuntu 64-bit	dpkg-based installers. Automatically installs dependencies. For details, see "Installing the Linux agent on Ubuntu".
• All 32-bit distributions listed in the Unitrends Compatibility and Interoperability Matrix	Download the applicable agent from the 32-bit Agents page.

Where to access your agent on the Unitrends Downloads page:

UNITRENDS
A Kaseya COMPANY

About Linux agent dependencies

When using GZEXE installers, you might need to install additional libraries. If this is the case, the installer stops the installation and lists the required dependencies. The dependencies it lists are the resources needed and not the name of the package you must install. The table below identifies the packages containing the commonly needed dependencies.

Dependencies by operating system

The following dependencies are required to protect Linux environments. Red Hat dependencies replace XINETD, which was a dependency for earlier versions.

Operating System	Dependencies
Red Hat 6 i386	• ed Packages are located on the installation media.
Red Hat 6 x86_64	• ed • glibc.i686 • nss-softokn-freebl.i686 The following packages might need to be updated to match the version of a new dependency. • glibc.x86_64 (must match glibc.i686) • glibc-common.x86_64 (must match glibc.i686) • nss-softokn-freebl.x86_64 (must match nss-softokn-freebl.i686) Packages are located on the installation media.
Red Hat 8 x86_64 and Oracle Linux 8	• libwrap.so.0()(64bit) • libc.so.6 • libc.so.6(GLIBC_2.0) • libc.so.6(GLIBC_2.1) • libc.so.6(GLIBC_2.2) • libmenu.so.5()(64bit) • libncurses.so.5()(64bit) • glibc-common-2.17-260.el7.x86_64.rpm
OpenSUSE 15 SP1	• libcrypto.6

Operating System	Dependencies
Oracle on Linux (for application backups only)	Samba is only used to protect Oracle with application backups. The Samba packages listed below only need to be installed if you wish to protect Oracle data with Unitrends application backups. For assistance with these packages, you can download the Oracle Dependency plug-in from the Agent Add-ons page. You must install the Linux agent before you can install this plug-in. Depending on your Linux distribution, use the Oracle Dependency for CentOS or Red Hat. Dependencies for Oracle application backups: • samba-client (for Oracle Linux 5 and CentOS 5) • cifs-utils (for most other Linux distributions)

Automated secure pairing of Unitrends Linux agents

Beginning in Linux agent release 10.7.5, a secure pairing is automatically established between the appliance and the Linux agent on each of its protected assets. This pairing enables Transport Layer Security (TLS) to encrypt data and authenticate connections between appliances and agents. Communication between appliances and agents is only allowed if there is a matching (paired) certificate.

This feature blocks any communication with Unitrends agent software that doesn't originate from a paired appliance (think of a Bluetooth headset, if it's not paired or in pairing mode, no one else can communicate with it). This eliminates the threat of a rogue appliance running backups or code against an agent.

To use the secure pairing feature, these requirements must be met:

- The Unitrends appliance must be running release 10.7.5 or higher.

- The Linux asset must be running agent release 10.7.5 or higher.

- The Unitrends appliance version must be equal to or higher than the Linux agent version.

> **IMPORTANT!** Be sure to upgrade your Unitrends appliance before upgrading your Linux agents.
>
> • Jobs will fail if you attempt to protect a 10.7.5 or higher agent with an appliance that is running an older release.
>
> • You cannot add an asset that is running a 10.7.5 or higher agent to an appliance that is running an older release. If you attempt this, you receive an error similar to: *Failed to save client: Registration for client* assetName *failed. The Unitrends System could not connect to the Unitrends Agent on* assetName. *Please ensure that the Agent software is installed on* assetName*, the Agent service is running (if applicable), and no firewall settings are preventing access*.

- The Linux agent listens for pairing requests on port 888. Ensure that port 888 is accessible on the Linux asset. For details and other port requirements, see *Appliance network settings > Additional ports* in the Appliance settings topic in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

- The Linux asset must be running one of these versions:

> **IMPORTANT!**   Do NOT install the 10.7.5 agent on other Linux versions that are not listed below. Instead, locate your Linux version on the Unitrends Downloads page and install the latest supported agent.

- Alma Linux 9, 64-bit
- CentOS 7, 64-bit
- CentOS 9, 64-bit
- Debian 10, 64-bit
- OpenSUSE 42, 64-bit
- Oracle Linux 8.1, 64-bit
- RHEL 7, 64-bit
- RHEL 8.4, 64-bit
- RHEL 9, 64-bit
- Rocky Linux 9
- SLES 11 SP3, 64-bit
- SUSE 15, 64-bit
- Ubuntu 22.04, 64-bit

Installing the Linux agent

Installation procedures for the Linux agent vary by Linux distribution. See the following topics for instructions:

- "To install the Linux agent using GZEXE"
- "To install the Linux agent on CentOS, Oracle Linux, and Red Hat"
- "Installing the Linux agent on Ubuntu"

To install the Linux agent using GZEXE

This section explains how to install the agent using GZEXE installers, which are available for all supported Linux distributions. If the agent requires dependencies, the installer stops the installation and lists the required dependencies.

1   Save the applicable agent installer on the Linux machine that you want to add to the Unitrends appliance. You can download the installer from the Latest Agent Releases on the Unitrends Downloads page.

2   Open a terminal, and log in as root user.

3   Change directories to the location where you have saved the agent installer, and run the command `ls -l` to view the installer file and determine whether you have execute permission. If necessary, add execute permission using the command:

```
# chmod +x <file_name>
```

4   Perform one of the following depending on whether you are using a 32-bit or 64-bit installer:

- For a 32-bit installer, run the command:

    ```
    # ./lnx32_cnt
    ```

- For a 64-bit installer, run the command:

    ```
    # ./lnx64_cnt
    ```

5   If necessary, install any required dependencies. The installer notifies you of any dependencies the agent needs. The dependencies listed are the resources needed and not the name of the package that you must install. For more about locating and installing dependencies, see "About Linux agent dependencies".

   Run the applicable command from step 4 above after installing the dependencies.

6   (Optional) To protect Oracle databases, install the Oracle Dependency from the Agent Add-ons page.

7   Enter the hostname for the backup appliance that will protect the asset.

8   If you are using a firewall, configure it to allow the Unitrends appliance to communicate with the Linux machine. For details, see "Configuring a Linux firewall to communicate with the Unitrends appliance".

9   Add the Linux asset to your Unitrends backup appliance to begin protecting it. For instructions, see Managing protected assets in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

To install the Linux agent on CentOS, Oracle Linux, and Red Hat

For CentOS, Oracle Linux, and Red Hat assets, you can use RPM-based installers that often automatically install the necessary dependencies if connected to a remote repository.

1   Save the applicable agent installer on the Linux machine that you want to add to the Unitrends appliance. You can download the installer from the Latest Agent Releases on the Unitrends Downloads page.

   Note: For Oracle Linux assets, download the CentOS or Red Hat agent installer.

2   Open a terminal, and log in as root user.

3   Change directories to the location where you have saved the agent installer.

4   Perform one of the following depending on whether you are using a 32-bit or 64-bit installer:

- For a 32-bit asset, run the command:

    ```
    # yum localinstall --nogpgcheck unitrends-linux-agent-<release>.<build_
    date>.i386.rpm
    ```

- For a 64-bit asset, run the command:

    ```
    # yum localinstall --nogpgcheck unitrends-linux-agent-<release>.<build_date>.x86_
    64.rpm
    ```

5 Install any required dependencies. The installer notifies you of any dependencies the agent needs. The dependencies listed are the resources needed and not the name of the package that you must install. For more about locating and installing dependencies, see "About Linux agent dependencies".

6 (Optional) To protect Oracle databases, install the Oracle Dependency from the Agent Add-ons page.

7 If you are using a firewall, configure it to allow the Unitrends appliance to communicate with the Linux machine. For details, see "Configuring a Linux firewall to communicate with the Unitrends appliance".

8 Add the Linux asset to your Unitrends backup appliance to begin protecting it. For instructions, see Managing protected assets in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

Installing the Linux agent on Ubuntu

For Ubuntu assets, you can use dpkg-based installers that often automatically install all necessary dependencies if connected to a remote repository. You can choose to install the agent using core utilities or the GDebi tool. If you install using core utilities, you must run two commands if the necessary dependencies have not been installed on your Ubuntu machine. If you use the GDebi tool, one command installs the agent and all necessary dependencies.

For instructions, see the following topics:

- "To install the Linux agent on Ubuntu using core utilities"

- "To install the Linux agent on Ubuntu using GDebi"

To install the Linux agent on Ubuntu using core utilities

For Ubuntu assets, you can use dpkg-based installers that install all necessary dependencies.

> **Note:**   This procedure might require you to run two commands. The first command installs the agent if the necessary dependencies are already installed on the asset. If the agent requires dependencies, the second command in this procedure installs them and then installs the agent. If you have installed the GDebi tool on the asset, you can use it to install the agent using only one command. For details, see "To install the Linux agent on Ubuntu using GDebi".

1 Save the applicable agent installer on the Linux machine that you want to add to the Unitrends appliance. You can download the installer from the Latest Agent Releases on the Unitrends Downloads page.

2 Open a terminal and change directories to the location where you saved the agent installer.

3 Perform one of the following:

- For the 32-bit installer, run the command:

```
# sudo dpkg -i unitrends-linux-agent-<release>-<build_date>.i386.deb
```

- For the 64-bit installer, run the command:

```
# sudo dpkg -i unitrends-linux-agent-<release>-<build_date>.amd64.deb
```

4 If the installer stopped because the agent requires dependencies, run the following command to install them:

```
# sudo apt-get install -f
```

5   If you are using a firewall, configure it to allow the Unitrends appliance to communicate with the Linux machine. For details, see "Configuring a Linux firewall to communicate with the Unitrends appliance".

6   Add the Linux asset to your Unitrends backup appliance to begin protecting it. For instructions, see Managing protected assets in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

To install the Linux agent on Ubuntu using GDebi

To install the agent with this procedure, you must have installed the GDebi package on your Ubuntu assets. Installation of the agent using GDebi requires only one command. To install the agent using core utilities, see "To install the Linux agent on Ubuntu using core utilities".

1   Save the applicable agent installer on the Linux machine that you want to add to the Unitrends appliance. You can download the installer from the Latest Agent Releases on the Unitrends Downloads page.

2   Open a terminal and change directories to the location where you saved the agent installer.

3   Perform one of the following depending on whether you are using a 32-bit or 64-bit installer:

   - To install the 32-bit agent, run the following command:

     ```
     # sudo gdebi unitrends-linux-agent-<release>-<build_date>.i386.deb
     ```

   - To install the 64-bit agent, run the following command:

     ```
     # sudo gdebi unitrends-linux-agent-<release>-<build_date>.amd64.deb
     ```

4   If you are using a firewall, configure it to allow the Unitrends appliance to communicate with the Linux machine. For details, see "Configuring a Linux firewall to communicate with the Unitrends appliance".

5   Add the Linux asset to your Unitrends backup appliance to begin protecting it. For instructions, see Managing protected assets in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

Configuring a Linux firewall to communicate with the Unitrends appliance

If you are protecting a Linux machine with a firewall, you must configure the firewall to allow communication with the Unitrends appliance before you can add the Linux machine as an asset.

To configure the Linux firewall

1   Modify the Linux machine's firewall settings to allow ports 1743 and 1745.

2   Open a terminal or text editor with root access and log in as user root.

3   Run the following command:

   ```
   # /usr/bp/bin/bputil -p "Configuration Options" data 1745 /usr/bp/bpinit/master.ini
   ```

4   (If needed) If the Linux asset will be running agent version 10.7.5 or higher, you must also modify the Linux machine's firewall settings to allow port 888. (Beginning in Linux agent release 10.7.5, a secure pairing between the agent and appliance is required. This pairing is established over port 888.)

Installing or upgrading the Novell OES agent

Before adding a Novell OES asset to the Unitrends appliance, you must install an agent. The agent enables you to back up, verify, and recover OES server data. Use the procedures in this section to install or upgrade the Novell OES agent.

Once the agent is installed, you can upgrade to a newer agent version using these same installation procedures. It is not necessary to remove the old agent. If an agent is already installed, you have the option to save any custom agent settings during installation.

Preparing to install the Novell OES agent

Before installing a Novell OES agent:

- Make sure your Novell OES system and its applications are running supported versions listed in the Unitrends Compatibility and Interoperability Matrix.

- Add the Unitrends appliance name to the local host table or set up the TCP/IP system to use DNS with the Unitrends appliance.

- To install on a 64-bit OES system, the 32-bit runtime environment must be enabled (this is the default configuration).

Novell OES agent restrictions and limitations

- Recovering individual files and folders from a backup copy is not supported. Only full backups can be recovered from a backup copy when restoring a TSA-based backup.

- Hot bare metal is not supported for OES 2 on SUSE Linux Enterprise 11.

- If a network mount is mounted on a directory with the same name as seen on the Novell OES machine, then the backups can have difficulty traversing that file system. For example, if *server1:\data* is mounted to *\data*, this presents a problem. The mount point should use a different name, such as *server1:\data* mounted to *\netdata*. This is a known issue with TSAFS.

To install or upgrade the Novell OES agent

1 Log in to the Novell OES machine as user root.

2 Verify that the novell-sms package is running on the OES system by entering the following command:

```
# service novell-smdrd status
```

3 If the service is not running, enter the following command:

```
# service novell-smdrd start
```

4 Place the agent installation file, *oes64_cnt* or *oes_cnt*, on the OES system. (Download the agent from the Unitrends Downloads page.)

5 Grant execute permission to the file by running the following command, where *[fileName]* is *oes64_cnt* for OES 2018 or *oes_cnt* for older OES versions:

```
# chmod +x [fileName]
```

6   Begin the installation by executing the file, where *[fileName]* is *oes64_cnt* for OES 2018 or *oes_cnt* for older OES versions:

```
# .\[fileName]
```

7   Enter **y** to continue the installation and press **Enter** to continue.

8   Press **Enter** to accept the default installation directory (*\usr\bp*) or enter the full path where you prefer the software be installed. Respond with a **y** when asked if the directory can be created.

9   (Optional) Enter an email address to receive reports from the OES system.

10   Enter the hostname of the backup appliance.

11   You are asked if your server is behind a firewall. Answer **yes** or **no**. Answering **yes** forces communication over port 1745.

12   Select **Enter** to approve default port and autoexec settings.

13   After the connection is made to the TSA, enter the user name (root) and password as prompted. This enables SMS-TSA based backups.

Note: Backup and recovery speeds are limited by the TSAFS performance. The TSAFS performance on an NSS file system is superior to performance on a non-NSS file system by as much as 300%. For more information on improving the TSAFS performance, refer to the following Novell document, Fine-Tuning SMS Performance.

Installing or upgrading the data copy access Hyper-V agent

If you are using the Recovery Assurance feature with your Hyper-V environment, the data copy access agent enables additional options. The data copy access agent is required for malware scans, re-IP, and application tests of Hyper-V VMs and Windows image-level backups run on Hyper-V.

To install or upgrade the data copy access agent

Use this procedure to install or upgrade the DCA Hyper-V agent on a Hyper-V server, Hyper-V VM, or Windows asset.

1   Download the agent file from the Agent Add-ons page at https://helpdesk.kaseya.com/hc/en-gb/articles/4407526882193-Unitrends-Downloads.

2   Save the agent file to the VM, Hyper-V server, or Windows asset.

3   Right click the installer file and select **Run as administrator** to start the setup wizard.

4   Click **Next** in the first wizard screen.

5   Click **Finish** when the installation completes. When successful setup is confirmed, click **Close**.

Troubleshooting the Upgrade

In rare instances, your first attempt to update the Unitrends appliance might not be successful. See the following table for a description of upgrade issues and steps you can take to resolve them:

Issue	Next steps
The update times out because some of the packages did not install.	If the installation stops and you receive a message stating a package did not install successfully, in most instances you can resolve the issue by clicking the refresh arrows and attempting the update again. If necessary you can repeat this multiple times until the update completes. See this article for more information: Timeout error when upgrading a Unitrends appliance.
The appliance is unable to download the update packages.	There are two possible solutions if your appliance is unable to download packages: • The appliance cannot reach the repo.unitrends.com site or the sftp.unitrends.com site - A firewall or some other restriction might be preventing you from reaching the sites. Ensure that the following ports are open outbound from the appliance: – Port 443 for the HTTPS protocol to repo.unitrends.com – Port 22 for the SFTP protocol to sftp.unitrends.com • Your appliance is connected to a local network only - If your appliance is not connected to the Internet, you can update the software using an ISO image. For procedures, see this article: How to upgrade the appliance via Unitrends' media.
An error message displays stating that the managing system must be updated.	To update the appliance, you must first update any other appliances that are managing it. Verify that any backup copy target appliance and any other managing appliances are running the latest release. Upgrade these appliances as needed. You can then upgrade any appliances that they are managing.
No data displays in the UI after installing appliance updates.	To resolve this issue: 1 Clear your browser cache, then close the browser. 2 Open the browser and log back in to continue working with your appliance.