



# Recovery-Series and UEB 8.1.0 Release Notes

release 1.05122015

200 Wheeler Road  
North Tower, 2nd Floor  
Burlington, MA 01803, USA  
Phone: 1.866.359.5411



# Copyright

Copyright © 2015 Unitrends Incorporated. All rights reserved.

Content in this publication is copyright material and may not be copied or duplicated in any form without prior written permission from Unitrends, Inc (“Unitrends”). This information is subject to change without notice and does not represent a commitment on the part of Unitrends.

The software described in this publication is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the license agreement. See the End User License Agreement before using the software.

The software described contains certain open source components that are copyrighted. For open source licenses, see the Unitrends Open Source Compliance section of the product Administrator’s Guide.

Because of the nature of this material, numerous hardware and software products are mentioned by name. In most, if not all, cases these product names are claimed as trademarks by the companies that manufacture the products. It is not our intent to claim these names or trademarks as our own.

The following applies to U.S. Government End Users: The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

The following applies to all contracts and subcontracts governed by the Rights in Technical Data and Computer Software Clause of the United States Department of Defense Federal Acquisition Regulations Supplement:

RESTRICTED RIGHTS LEGEND: USE, DUPLICATION OR DISCLOSURE BY THE UNITED STATES GOVERNMENT IS SUBJECT TO RESTRICTIONS AS SET FORTH IN SUBDIVISION (C)(1)(II) OF THE RIGHTS AND TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE AT DFAR 252-227-7013. UNITRENDS CORPORATION IS THE CONTRACTOR AND IS LOCATED AT 200 WHEELER ROAD, NORTH TOWER, 2<sup>ND</sup> FLOOR, BURLINGTON, MASSACHUSETTS 01803.

Unitrends, Inc  
200 Wheeler Road  
North Tower, 2<sup>nd</sup> Floor  
Burlington, MA 01803, USA  
Phone: 1.866.359.5411





# Recovery-Series and UEB

## 8.1 Release Notes

The 8.1 release delivers new enterprise-level capabilities and performance enhancements. These features are described in this document. For a of defects that have been addressed in this release, see the [Customer Resolved Defects](#) document.

References to version requirements state the minimum required Unitrends version. For example, *release 8.1* indicates the system must be running version 8.1 or higher.

8.1 features include:

- **UEB on VMware and Hyper-V. Radically simple disaster recovery.**  
For UEB appliances deployed with release 8.1 on VMware and Hyper-V, all system configuration settings and backup data reside on storage that can be attached to a new UEB. This enables you to recover your appliance in minutes with your backups, protected clients, and schedules intact. For details, see the [UEB Deployment Guide for VMware](#) and the [UEB Deployment Guide for Hyper-V](#).
- **NDMP. Protect your NetApp clusters simply and efficiently.**  
With release 8.1, you can easily protect NetApp nodes configured in high availability C-mode clusters. Once you have configured your clusters for Unitrends protection, they can be backed up and restored using the standard Unitrends NDMP procedures.

For requirements and procedures used to protect NetApp clusters, see [“Implementing NetApp cluster protection” on page 9](#).



- **SQL. Complete protection of AlwaysOn Failover Clusters and SMB 3.0 shares.**  
Release 8.1 extends SQL protection to support SQL Server AlwaysON Failover Clusters and databases with disk storage located on SMB 3.0 shares. Unitrends enables you to protect and restore these complex high-availability configurations in just a few clicks.

For requirements and procedures, see these topics:

- [“Implementing SQL AlwaysON Failover Cluster protection” on page 9.](#)
- [“Implementing protection of SQL on SMB 3.0 shares” on page 14](#)

- **Oracle on Linux. Complete protection for Oracle Automatic Storage Management (ASM).**

Committed to ensuring enterprises can leverage a simplified all-in-one set of capabilities, release 8.1 enhances its existing support for mission-critical Oracle on Linux databases. Organizations leveraging the performance and availability benefits of Automatic Storage Management can rest assured that this critical data is protected both on-premise and off-site.

In addition to the requirements described in [Requirements for Oracle protection](#) in the Unitrends Recovery-Series and UEB Administrator’s Guide, the following requirements must be met to protect Oracle on Linux ASM environments:

- The Unitrends appliance must be running release 8.1.
- The Oracle on Linux version must be 12c or 11g.
- The Linux server must be running the 8.1 agent.
- The Linux server must have the Linux Oracle dependency installed.
- Download the Linux agent and Oracle dependency from the [Latest Agent Releases](#) page.

For details on installing the agent and dependency, see [Installing the Linux agent](#) and [Needed dependencies for Oracle](#) in the Unitrends Recovery-Series and UEB Administrator’s Guide. For a complete list of supported Linux versions, see the [Unitrends Compatibility and Interoperability Matrix](#).

- **Mac OS 10.10 protection.**

Release 8.1 extends Mac OS support to include file-level protection of Mac OS 10.10. Note that hot bare metal protection is not supported.

To protect your Mac OS 10.10 environment:

- The Unitrends appliance must be running release 8.0 or higher.
- The Mac OS client must be running agent release 8.0 or higher. Download the agent from the [Latest Agent Releases](#) page.









Cluster type	SQL	Windows
	2014	2012, 2012 R2
Clustered Shared Volume	2012	2012, 2012 R2
	2014	2012, 2012 R2
AlwaysOn Cluster Volume	2012	2012, 2012 R2
	2014	2012, 2012 R2
SMB	2012	2012, 2012 R2
	2014	2012, 2012 R2
SQL Failover Clusters		2012, 2012 R2

## Special considerations for adding SQL clusters

The Unitrends appliance must be able to resolve the name and IP address of every node in a SQL cluster. When adding a cluster node to a Unitrends appliance, you must enter the correct IP address and the exact name of the node. If you enter an incorrect IP address or a name that does not exactly match the name of the node, backups fail because the appliance cannot determine the owner of the database in the cluster configuration. Be sure to enter the correct hostname and IP address for every node in the cluster.

Before adding a cluster to the Unitrends appliance, you must install the agent on each cluster node and add it to the appliance. Follow these steps to add a cluster:

- I Install the agent on each cluster node. For details, see [Push installing the Windows agents](#) or [Manually installing the Windows agents](#) in the Unitrends Recovery-Series and UEB Administrator's Guide.
- II Add each node to the Unitrends appliance using the instructions in [To add a client to the Unitrends appliance](#) in the Unitrends Recovery-Series and UEB Administrator's Guide.
- III Add the cluster using the instructions in [To add a client to the Unitrends appliance](#) in the Unitrends Recovery-Series and UEB Administrator's Guide.

## Special considerations for backing up SQL clusters

Consider the following before executing backups for databases hosted on servers configured in a cluster:

- To protect virtual machines residing on cluster shared volumes (CSVs), you must select the cluster in the Navigation pane before executing backups. You cannot protect these databases by selecting the owner node.
- To protect databases that are hosted on a cluster node but that do not reside on CSVs, you must create a backup schedule for the node that hosts the databases. You cannot protect them in the same schedule as the clustered databases.
- A Microsoft limitation prevents the Unitrends appliance from running concurrent backups of clustered databases hosted on Windows Server 2008 R2. You can work around this limitation by creating aliases for the cluster and creating a separate schedule for each cluster instance. For instructions, see [“To create a client alias for a SQL cluster”](#) below.
- When backing up SQL nodes, include all local volumes and exclude the system state. Because the system state must be excluded, Windows instant recovery and integrated bare metal recovery are not supported.

### Creating an alias for a SQL cluster

To work around a Microsoft limitation that prevents the Unitrends appliance from running simultaneous backups of clustered databases hosted on a server running Windows 2008 R2, you can create a client alias for each cluster shared volume (CSV) using the procedure described below. After adding each client alias to the appliance, you can create a backup schedule for each cluster instance.

#### To create a client alias for a SQL cluster

- 1 Log in to the appliance to which the cluster is added.
- 2 Select **Settings > Clients, Networking, and Notifications > Networks > Hosts**.
- 3 Click on the client name in the table.
- 4 Type a name in the **Alias Name** field. It is recommended that you include the CSV number in the name to help you remember which CSV you would like to associate with each alias.

**Note:** Do not enter spaces in the name. You are limited to 15 characters. It is recommended that you write down the alias name so you can enter the exact name when you add it as a new client.

- 5 Click **Add**. You see the alias name in the Alias List area.  
*Note: To remove an alias name from the Alias List area, click on the alias name and click **Remove**. To remove all alias names from the Alias List area, click **Remove All**.*
- 6 Repeat to add more alias names, if necessary.
- 7 Click **Confirm**.  
*To add the alias name as a client*
- 8 Go to **Settings > Clients, Networking, and Notifications > Clients**.
- 9 Click **Add Client**. You see the Add Client screen.
- 10 Select **Windows** from the Computer Type drop-down list.
- 11 Uncheck **Establish trust** in the Authentication area.
- 12 Uncheck **Automatically create a backup schedule for this computer and apply it immediately** in the Options area.
- 13 Enter one of your new alias names in the **Computer Name** field.  
*Note: There is no need to add an IP address, since this defaults to information from the host page.*
- 14 Click **Setup**. You see a processing message, then a Reload Navigation window describing that you need to refresh the system.
- 15 Click **Yes, reload the System** or **No, reload the System later**.
- 16 After you reload the system, the new alias name displays in the Navigation pane in the list of clients protected by the system.
- 17 Repeat as needed to add additional client aliases.

## Running SQL cluster backups

Use the [Executing SQL backups](#) procedures in the Unitrends Recovery-Series and UEB Administrator's Guide to protect your SQL cluster. When running the procedures, be sure to select the cluster node itself.

## Restoring SQL cluster backups

Use the [Restoring SQL backups](#) procedures in the Unitrends Recovery-Series and UEB Administrator's Guide to restore your SQL cluster backups. When running the procedures, be sure to select the cluster node itself.

# Implementing protection of SQL on SMB 3.0 shares

SQL Server 2012 and higher can host SQL instances with disk storage located on SMB 3.0 shares. Unitrends software releases 8.1 and higher can protect these databases with SQL backups. For details, see [“Prerequisites and considerations”](#) below.

## Prerequisites and considerations

- The Unitrends appliance must be running release 8.1.
- The SQL server must be running Windows agent release 8.1. Download the Windows agent from the [Latest Agent Releases](#) page. For details on installing the agent, see [Push installing the Windows agents](#) or [Manually installing the Windows agents](#) in the Unitrends Recovery-Series and UEB Administrator’s Guide.
- The File Server and the File Server VSS Agent Service roles must be installed on the server hosting the shares. For instructions on installing these roles, see [KB 1776](#).
- The Windows agent installed on the SQL server must be granted read/write access to remote SMB 3.0 shares. For instructions on granting this access, see [“Granting the Windows agent read/write access to remote SMB 3.0 shares”](#) below.
- The SQL Server hosting the databases and the server hosting the SMB shares must belong to the same Windows domain.
- The database can contain one or more files located on SMB 3.0 shares. All files can reside on the same SMB 3.0 share or different shares hosted by one or more servers in the same domain. All servers participating in the database backup must belong to the same domain.
- For files located on remote SMB 3.0 shares, the Windows agent creates a VSS snapshot on the remote server and then exposes it to the SQL Server through the SMB share pathing. The agent then backs up the database files from the remote snapshot location. When the backup completes, all VSS snapshots created for the backup are removed from the server hosting the SMB share.

## Granting the Windows agent read/write access to remote SMB 3.0 shares

The Windows agent installed on the SQL Server must be granted read/write access to remote SMB 3.0 shares. You can grant this access using one of the following methods:

- On the SQL Server, change the login account for the Unitrends Windows agent service *bpagent* to the domain administrator account. Using these credentials will provide all necessary access to the SMB shares. This is the most secure option for SMB access. Note, however, that file-level backups of the SQL Server may encounter files whose permissions do not allow domain administrator access. If successful file-level backups for the SQL Server cannot be created and SMB share security is less of an issue, then the method below is recommended.
- Run the agent as local system account on the SQL Server and grant it read/write permission for the SMB shares. For instructions, see [KB 1777](#).

## Running SQL backups

Once you've satisfied the SMB 3.0 prerequisites and have granted the Windows agent access to the SMB 3.0 shares, run backups using the [Executing SQL backups](#) procedures in the Unitrends Recovery-Series and UEB Administrator's Guide.

## Restoring SQL backups

To restore SQL backups, use the [Restoring SQL backups](#) procedures in the Unitrends Recovery-Series and UEB Administrator's Guide.

# Upgrading to version 8.1

See the following resources for details on upgrading to version 8.1:

- The [Unitrends Recovery-Series and UEB Upgrade Guide](#) for complete upgrade instructions and considerations.
- The video tutorial [Upgrading the Unitrends Appliance](#).
- The video tutorial [Troubleshooting the Unitrends Appliance Upgrade](#).

**Note on legacy vaulting:** *Beginning in release 8.0, appliances use LZ4 compression by default. LZ4 is not compatible with legacy vaulting. If your appliance is a legacy vault that was imaged or deployed with version 8.0.0-2 or later, you must reconfigure compression settings by following these steps:*

- 1 Select **Settings > System Updates, and Licensing > General Configuration [Advanced]**.
- 2 Click to expand the **Disk2DiskDefaults** folder.

Select the row containing **CompressEngine**, enter *auto* in the Value field, and click **Confirm**.