Veritas eDiscovery Platform™

Upgrade Guide

10.2

VERITAS

Veritas eDiscovery Platform™: Upgrade Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated: 2022-09-05

Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-Party Programs"). Some of the Third-Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-Party legal notices for this product at: https://www.veritas.com/about/legal/license-agreements

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Dr
Santa Clara, CA 95054
http://www.veritas.com

Contents

Chapter 1 Preface 5

About this guide 5
Product documentation 5
Technical Support 8
Documentation 8
Documentation Feedback 8

Chapter 2 Overview 11

Installation Basics 11

Chapter 3 Upgrade Pre-Installation Steps 12

Upgrade Prerequisites 12
- Machine Configuration 12
- Hardware Compatibility 13
- Operating System 17
- Plan for Appropriate Down Time 17
- Removal of Dependency on .NET 3.5 18
- Software Requirement 18
- SSL Configuration Details 18
- Upgrade Prerequisite Checklist 19
- Download 10.2 Software 20
- Read Upgrade Overview Guide 21
- Check for De-Duplication Implications 21
- Verify that the Veritas eDiscovery Platform Product Version is Upgradeable 21
- Verify Windows Service Settings 23
- User Account for Upgrade Installer 23
- Verify Windows Firewall Settings 27
- Verify eDiscovery Platform Cases Before the Upgrade 27
- Cleanup Veritas eDiscovery Platform Jobs 28
- Verify System Time Zone Settings 29
- Verify Scheduled Tasks 29
- Close Windows Explorer and all Remote Login Sessions 29
- Check Microsoft Office Version and Activation Status 30
- Veritas Enterprise Vault API Runtime 30
- Perform Full Node Backups on All Appliances 30
- Perform Windows Updates 33

Verify Appliance Hardware 33

Chapter 4 Upgrade Installation Steps 34

Cluster Considerations 34
Veritas eDiscovery Platform Product Installation/Upgrade Instructions 35
(Optional) Setting Up Your System for Audio Processing 55
Setting Up Your System: Server-Side 55
10.2 Installation Verification and Log Files Review 58

Chapter 5 Upgrade Post-Installation Steps 60

Post-upgrade Checklist 60
Post-Upgrade Installation Steps 61
Validate Install 61
Activate Microsoft Office Professional Plus 2016 (for Windows Server 2016) 62
Activate Microsoft Office Professional Plus 2019 (for Windows Server 2019) 64
Apply the Latest 10.2 Patch (if applicable) 65
Verify the Veritas eDiscovery Platform License 65
Verify Veritas eDiscovery Platform Services 65
Verify System Settings 65
Verify Security Settings 66
Verify Indexing Settings 68
Verify Custom Logo Settings 68
Verify Configuration Settings 69
Verify Firewall Settings 69
Reconfigure LDAP authentication after upgrade 69
Reconfigure Full Node Scheduled Backup Tasks 70
Update Virus Scanning Software (if applicable) 70
Disable Adobe Automatic Updates 72
Verify Clearwell Utility 72
Clear Browser Cache 73
Configure Browser Cache Security 73
Verify Veritas eDiscovery Platform Cases 74
Associating Legal Holds and Collections with 10.2-Upgraded Cases 74
Update checksum for emails 74
OST to PST Conversion Libraries 76

Chapter 1

Preface

About this guide

This document provides detailed step-by-step installation and configuration instructions for successfully upgrading and setting up the Veritas eDiscovery Platform application. This guide assumes the reader is comfortable performing common system operations and is familiar with the Windows operating system. Before upgrading your system, be sure to read the Veritas eDiscovery Platform Upgrade Overview Guide to familiarize yourself with the changes in the release. If you are installing the Veritas eDiscovery Platform application on a machine for the first time, please read and follow the instructions outlined in the *Veritas eDiscovery Platform Installation Guide*.

Product documentation

The table below lists the end-user documentation that is available for the Veritas eDiscovery Platform product.

Veritas eDiscovery Platform Documentation

Document	Comments
Installation and Configuration	
Installation Guide	Describes prerequisites, and how to perform a full install of the Veritas eDiscovery Platform application
Upgrade Overview Guide	Provides critical upgrade information, by version, useful prior to upgrading an appliance to the current product release

Document	Comments
Upgrade Guide	Describes prerequisites and upgrade information for the current customers with a previous version of Veritas eDiscovery Platform
Utility Node Guide	For customers using utility nodes, describes how to install and configure appliances as utility nodes for use with an existing Veritas eDiscovery Platform setup
Distributed Architecture Deployment Guide	Provides installation and configuration information for the Review and Processing Scalability feature in a distributed architecture deployment
Getting Started	
Navigation Reference Card	Provides a mapping of review changes from 10.x compared to 9.x, 9.x compared to 8.x and the user interface changes from 8.x compared to 7.x
Administrator's QuickStart Guide	Describes basic appliance and case configuration
Reviewer QuickStart Guide	A reviewer's reference to getting started using the *Analysis & Review* module in Veritas eDiscovery Platform
Tagging Reference Card	Describes how tag sets and filter type impact filter counts
User and Administration	
Legal Hold User Guide	Describes how to set up and configure an appliance for Legal Holds, and use the Legal Hold module as an administrator in Veritas eDiscovery Platform
Identification and Collection Guide	Describes how to prepare and collect data for processing, using the Identification and Collection module
Case Administration Guide	Describes case setup, processing, and management, plus pre-processing navigation, tips, and recommendations. Includes processing exceptions reference and associated reports, plus file handling information for multiple languages, and supported file types and file type mapping.
System Administration Guide	Includes system backup, restore, and support features, configuration, and anti-virus scanning guidelines for use with Veritas eDiscovery Platform
Load File Import Guide	Describes how to import load file sources into Veritas eDiscovery Platform

Document	Comments
User Guide	Describes how to perform searches, analysis, and review, including detailed information and syntax examples for performing advanced searches
Audio Search User Guide	Describes how to use the Audio Search feature to process, analyze, and search and export search media content
Imaging Tool Upgrade Guide	Release 10.0 replaced the IGC Native Viewer with PrizmDoc Viewer. This guide provides details about the Imaging Tool Upgrade feature and how to perform Imaging Tool Upgrade for cases that were backed-up pre-10.0 and are restored in the current version of eDiscovery Platform, workflows affected when the cases are upgraded or not upgraded, and frequently asked questions (FAQs).
Export and Production Guide	Describes how to use and produce exports, productions, and logs (privilege and redaction logs).
Transparent Predictive Coding User Guide	Describes how to use the Predictive Coding feature in Veritas eDiscovery Platform to train the system to predict results from control set data and tag settings
Reference and Support	
Legal Hold	Legal Hold administrator's reference of how to create and manage holds
Collection	A quick reference card of how to collect data in Veritas eDiscovery Platform
OnSite Collection	A quick reference for performing OnSite collection tasks
Review and Redaction	Reviewer's reference card of all redaction functions
Keyboard Shortcuts	A quick reference card listing all supported shortcuts
Production	Administrator's reference card for production exports
User Rights Management	A quick reference card for managing user accounts
Audio Search	A quick reference card for performing multimedia search tasks
Audio Processing	A quick reference card for processing multimedia sources
Online Help	
Includes all the above documentation (excluding Installation and Configuration) accessed by clicking **Help** in the Veritas eDiscovery Platform user interface.	
Release	

Document	Comments
Release Notes	Provides latest updated information specific to the current product release

For the latest product documentation:
https://www.veritas.com/support/en_US/article.100040275

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies.

For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan): CustomerCare@veritas.com

Japan: CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. The latest documentation is available from:

- Documentation link at the bottom of any page in the eDiscovery Platform landing page.
- Veritas Products Web site: https://www.veritas.com/product/a-to-z

Documentation Feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

DL-VTAS-eDiscovery-documentation@veritas.com

You can also see documentation information or ask a question on the Veritas community site: https://vox.veritas.com/

Chapter 2

Overview

This document provides instructions for upgrading the Veritas eDiscovery Platform from 10.0 and 10.1 release to 10.2 release.

Installation Basics

The following list provides the details on what you need to do to successfully upgrade:

Note: This document is for upgrades only. For new installations, refer to the *Veritas eDiscovery Platform Installation Guide*.

1. Read the *Veritas eDiscovery Platform Upgrade Overview* to learn important insights about migration information and the release before upgrading.
2. Review this entire Upgrade Guide to understand what gets installed and uninstalled on your machine, the need for full node backup(s), potential reboots, and guidance on upgrading with minimal impact to your case and system environment.
3. Perform the pre-installation steps. See Upgrade Pre-Installation Steps.
4. Review and perform the upgrade installation steps. See Upgrade Installation Steps.

   Perform the post-installation steps. See Upgrade Post-Installation Steps.

Chapter 3

Upgrade Pre-Installation Steps

The following steps must be performed in preparation of the upgrade.

Upgrade Prerequisites

Machine Configuration

Confirm supported hardware configuration:

- Veritas eDiscovery Platform 8100 or 8200 appliance
- **C: drive** – 80 GB minimum with recommended 30 GB of disk free space – the installer will display a warning and the system may not function correctly if this space requirement is not met.
- **D: drive or designated second drive** – Minimum of 1.5 TB or more of free disk space

  IMPORTANT! For brevity and readability, this document hereinafter refers to the **D: drive**, but please note that an alternate drive can be substituted in place of the D: drive.

  Note: The D: drive is used as a temporary cache for many of the processing components in Veritas eDiscovery Platform, therefore a D: drive of at least 1.5 TB is recommended.

- Page file is configured with no page file on C: drive and with system managed page file on the D: drive.

Hardware Compatibility

The platform supports the following types of appliances for the corresponding functions and minimum requirements for hardware (and Virtual Machines if used) in a distributed architecture.

Note: Release 10.0 replaced the IGC Native Viewer with PrizmDoc Viewer, which introduced several performance improvements in review, redaction, annotation, and other imaging-related operations. However, these enhancements brought in the need for higher hardware requirements. The minimum recommended hardware requirements vary based on whether the appliance will be used for any Imaging related jobs with the Imaging role enabled.

Setup with no Imaging Related Operations

Appliance Type	Environment	Appliance Function	CPUs RAM	Disk	VM*
All-In-One (Standalone)	*Standalone*	*Hosts Cases and Review and performs Processing* **Also includes Legal Holds and Collections*	32-Core CPU x 128 GB RAM	1.5 TB (1500 IOPs)	Y
Utility		*Retrieval and HTML caching*	4-Core CPU x 8 GB RAM	500 GB on D:	Y
Case Home and Processing	*Distributed Architecture*	*Hosts Cases and Review and performs Processing*	24-Core CPU x 96 GB RAM	1.5 TB (1500 IOPs)	Y
Review and Processing	*Distributed Architecture*	*Hosts Review and performs Processing*	24-Core CPU x 96 GB RAM	1.5 TB (1500 IOPs)	Y
Case Home Only	*Distributed Architecture*	*Hosts Cases without Processing and Review*	16-Core CPU x 64 GB RAM	1.5 TB (1500 IOPs)	Y
Review Only	Not Applicable				

Appliance Type	Environment	Appliance Function	CPUs RAM	Disk	VM*
Processing Only	*Distributed Architecture*	*Performs Processing*	16-Core CPU x 64 GB RAM	1.5 TB (1500 IOPs)	Y
Cluster Admin	*Distributed Architecture*	*Administers the Distributed Architecture cluster and hosts Legal Holds and Collections*	32-Core CPU x 128 GB RAM	1.5 TB (1500 IOPs)	Y
Cluster Admin /Database	*Distributed Architecture*	*Hosts the Distributed Architecture shared database, administers the Distributed Architecture cluster and hosts Legal Holds and Collections*	32-Core CPU x 192 GB RAM	1.5 TB (1500 IOPs)	Y
Shared Remote Database MySQL	*Distributed Architecture*	Database Server	24-Core CPU** x 128 GB RAM	1.5 TB (1500 IOPs)****	N***

NOTE: The number of cores in the above table is the total number of logical processors (with hyper-threading enabled) on the machine, and not just the physical cores.

***** VM performance is lesser than that of a physical machine.

****** This is the minimum required configuration, but the recommended configuration is 32-Core CPU.

******* A physical machine is recommended, but a VM of equivalent performance (on dedicated hardware) can be used if required by local IT policies.

******** You might need 2 TB or higher if the number of cases and items is too high and multiple concurrent activities happen on the system.

IMPORTANT! Existing appliances can be repurposed for a distributed architecture deployment. For information about other appliance types, contact your Solutions Consultant, or Technical Support.

Setup Supporting Imaging Operations (With the Imaging role enabled)

Following specifications are for eDiscovery Platform deployments that are used for native review and jobs such as Image Caching, Production/Export, and Bulk redaction.

Appliance Type	Environment	Appliance Function	CPUs RAM	Disk	VM*
All-In-One (Standalone)	*Standalone*	*Hosts Cases and Review and performs Processing* **Also includes Legal Holds and Collections*	32-Core CPU x 128 GB RAM	1.5 TB (1500 IOPs)	Y
Utility		*Caching, Retrieval, Export*	8-Core CPU x 32 GB RAM	500 GB on D:	Y
Case Home and Processing	*Distributed Architecture*	*Hosts Cases and Review and performs Processing*	24-Core CPU x 96 GB RAM	1.5 TB (1500 IOPs)	Y
Review and Processing	*Distributed Architecture*	*Hosts Review and performs Processing*	24-Core CPU x 96 GB RAM	1.5 TB (1500 IOPs)	Y
Case Home Only	*Distributed Architecture*	*Hosts Cases*	24-Core CPU x 96 GB RAM	1.5 TB (1500 IOPs)	Y
Review Only	*Distributed Architecture*	*Hosts Review*	24-Core CPU x 96 GB RAM	1.5 TB (1500 IOPs)	Y
Processing Only	*Distributed Architecture*	*Performs Processing*	16-Core CPU x 64 GB RAM	1.5 TB (1500 IOPs)	Y
Cluster Admin	*Distributed Architecture*	*Administers the Distributed Architecture*	32-Core CPU x 128 GB RAM	1.5 TB (1500 IOPs)	Y

Appliance Type	Environment	Appliance Function	CPUs RAM	Disk	VM*
		cluster and hosts Legal Holds and Collections			
Cluster Admin /Database	*Distributed Architecture*	*Hosts the Distributed Architecture shared database, administers the Distributed Architecture cluster and hosts Legal Holds and Collections*	32-Core CPU x 192 GB RAM	1.5 TB (1500 IOPs)	Y
Shared Remote Database MySQL	*Distributed Architecture*	Database Server	24-Core CPU** x 128 GB RAM	1.5 TB (1500 IOPs)****	N***

NOTE: The number of cores in the above table is the total number of logical processors (with hyper-threading enabled) on the machine, and not just the physical cores.

***** VM performance is lesser than that of a physical machine.

****** This is the minimum required configuration, but the recommended configuration is 32-Core CPU.

******* A physical machine is recommended, but a VM of equivalent performance (on dedicated hardware) can be used if required by local IT policies.

******** You might need 2 TB or higher if the number of cases and items is too high and multiple concurrent activities happen on the system.

IMPORTANT! Existing appliances can be repurposed for a distributed architecture deployment. For information about other appliance types, contact your Solutions Consultant, or Technical Support.

Operating System

Installed and activated:

- Windows Server 2019 (Standard or Data Center edition)

  Note: While installing Windows Server 2019, you must use the Desktop Experience version and not the core version.

- Windows Server 2016

  Note: While installing Windows Server 2016, you must use the Desktop Experience version and not the core version.

Upgrade Considerations for Windows Server 2019:

If you need to upgrade the OS of an existing installation of eDiscovery Platform setup to Windows Server 2019, you must complete following steps:

1. Backup the current eDiscovery Platform node.
2. Install Windows Server 2019.
3. Install eDiscovery Platform 10.2.
4. Restore the node backup.

Support Considerations:

Starting with releases 10.2, Veritas eDiscovery Platform is no longer certified or supported on Windows Server 2012 R2, both Standard and Enterprise editions). If you are running the product on this operating system, please upgrade to a supported operating system.

Plan for Appropriate Down Time

Carefully determine the maximum downtime that is available and detail the upgrade tasks that must be performed during that time window. This guide helps identify tasks and recommendations to minimize appliance downtime.

Removal of Dependency on .NET 3.5

Earlier versions of eDiscovery Platform had a dependency on .NET 3.5. Starting with version 10.0.1, eDiscovery Platform has no dependency on .NET 3.5.

The following are possible upgrade scenarios and the recommended steps for each upgrade path:

Upgrade scenario: Upgrades from version 10.0.1, 10.0.2, 10.1, 10.1.1, 10.1.2, 10.1.3 to 10.2:

- If you have already uninstalled .NET 3.5 after upgrading to 10.2, no further actions are required.
- If you have not uninstalled .NET 3.5, uninstall it either before or after upgrading to 10.2.

Upgrade scenario: Direct upgrades from 10.0 to 10.2 (without upgrading to 10.0.1, 10.0.2, 10.1, 10.1.1, 10.1.2, or 10.1.3):

You are recommended to uninstall .NET 3.5 only after upgrading to 10.2, and not before upgrading. If .NET 3.5 has already been uninstalled before upgrading to 10.2, you will see two benign popups (related to .NET 3.5 not being available on the system) during the installation.

Software Requirement

- Microsoft Edge, Google Chrome, and Apple Safari
- .NET Framework 4.7.2 (Required)
- Microsoft .NET Framework 4.8.0 Runtime (Recommended)

SSL Configuration Details

Communication between browser and eDiscovery Platform
By default, the SSL configuration in the eDiscovery Platform is set to accept 128-bit or greater ciphers and requires the use of the TLSv1.2 protocol. SSLv2, SSLv3.0, TLS1 and TLS1.1 are all disabled, but the set of supported ciphers and protocols can be modified if needed. Consult your IT department's security specialists to determine secure settings for your browser.

Communication between eDiscovery Platform and MySQL Server
Starting release 10.2, the preferred mode of communication between eDiscovery Platform and MySQL server is over a secured connection using TLSv1.2.
For more information on securing MySQL server DB connections over TLSv1.2 protocol, refer to the *Veritas eDiscovery Platform System Administration Guide 10.2* document with section - *Managing encrypted connection with MySQL.*

Note: Certificates for all appliances must be issued by an external certificate issuing authority and installed on your servers by your own IT department.

For more information on secure LDAP SSL/TLS, refer to the *Veritas eDiscovery Platform System Administration Guide 10.2*.

Upgrade Prerequisite Checklist

After verifying the information in the previous sections, proceed and confirm the items on the following checklist prior to the upgrade. If you need more information, each of these items is covered in detail in the subsequent sections.

Step	Task
1	Plan for appropriate down time.
2	Download the 10.2 software from the MyVeritas Licensing portal. See Download 10.2 Software.
3	**IMPORTANT!** Read the 10.2 *Veritas eDiscovery Platform Upgrade Overview* Guide and take appropriate actions.
4	If applicable, identify de-dupe implications related to Outlook 2016. Refer to the *Veritas eDiscovery Platform Upgrade Overview Guide 10.2 for* more information.
5	Have resources available to support a system restart.
6	Verify that the Veritas eDiscovery Platform product version is upgradeable. If applicable, review and plan for cluster considerations. See Verify that the Veritas eDiscovery Platform Product Version is Upgradeable.
7	If you have a remote database server, you must update the DBMS standalone server to 8.0.30. This also applies to a configuration where the remote database server and cluster primary server are on the same appliance. See file "D:\CW\V102\utilities\DBMS\ReadMe-DBMS.txt"
8	Verify if you have administrative privileges (either a local administrator or a domain administrator). In case a domain administrator is used, ensure that you are added to the local administrators' group before starting the eDiscovery Platform installation.
9	Verify Windows firewall settings.
10	Verify Veritas eDiscovery Platform cases before the upgrade.

Step	Task
11	Clean up the Veritas eDiscovery Platform jobs.
12	Verify system time zone settings.
13	Verify scheduled tasks.
14	Close Windows Explorer and all remote login sessions.
15	Check Microsoft Office Version, Activation and License Key Status.
16	Ensure that the Imaging Tool Upgrade job has already been executed on all the cases before upgrading to release 10.2. Please refer to Imaging Tool Upgrade Guide for more details.
17	In 10.0, Veritas Enterprise Vault API Runtime 12.4.0 client is installed. If applicable, determine whether you want to use 11.x version of Veritas Enterprise Vault API Runtime.
18	**IMPORTANT!** Perform full node backups on all appliances. This is especially important for the MySQL upgrade.
19	Install Windows updates.
20	Verify appliance hardware.
21	Cluster considerations: • Upgrade all servers in the cluster starting with the primary server. • Ensure all appliances are on the same version. • In case of a legacy cluster, make sure you have the firewall turned off on the primary node, and during installation on the node you are validating against the primary database.
22	Verify that no other Remote Desktop sessions or applications are open or running.
23	Product Installation • Run **InstallClearwell.bat** which is in the V10 directory where you unzip the installation files. • Choose to upgrade to a new directory. • Verify the current version you are running.

Download 10.2 Software

Sign in and use the MyVeritas portal for downloading product software, licensing and support:

- Information and the replacement options are located here: www.veritas.com/docs/100040083
- For cumulative hotfix information and downloads, visit the support site Downloads area: https://www.veritas.com/content/support/en_US.html

You can download the appropriate Veritas eDiscovery Platform product files from the Veritas Entitlement Management System (VEMS), previously the Veritas Licensing Portal.

Read Upgrade Overview Guide

Review the 10.2 *Veritas eDiscovery Platform Upgrade Overview Guide*. Ensure all the changes in behavior and functionality are understood when upgrading existing cases.

Check for De-Duplication Implications

If applicable to your upgrade scenario, identify potential de-dupe implications when upgrading to Outlook 2016/2019. Refer to the *Veritas eDiscovery Platform Upgrade Overview Guide 10.2* for more information.

Verify that the Veritas eDiscovery Platform Product Version is Upgradeable

Veritas eDiscovery Platform 10.2 installation supports upgrades from the versions as listed in the following section. To verify that you are at the correct product level, logon to Veritas eDiscovery Platform and select **System > Appliances**. Select the appliance and verify it is at the correct product version.

Supported Upgrade Paths

From Release	To Release
10.0 GA and all CHFs	10.2
10.1 GA and all CHFs	10.2

Note: If you are on any pre-10.0 version, then upgrade to 10.0 GA before performing the 10.2 upgrade. To verify that you are at the correct product

level, log on to Veritas eDiscovery Platform and select **System** > **Appliances**. Select the appliance and verify it is at the correct product version.

For more information on supported upgrade paths, refer to: http://www.veritas.com/docs/000095769

If you are upgrading to pre-10.2 release, refer to the *Upgrade Guide* for the respective release.

Cluster

If you have a cluster of Veritas eDiscovery Platform appliances, you must:

- If you are running a remote database server, then you need to update the DBMS standalone server to 8.0.30. The DBMS installer will take care of upgrading to the latest MySQL version & then tuning the database server. This also applies to a configuration where the remote database server and cluster primary are on the same appliance. See file "D:\CW\V102\utilities\DBMS\ReadMe-DBMS.txt"
  When upgrading the DBMS server to 8.0.30, you must not abort the installation during the phase where the DBMS installer is installing MySQL 8.0.30.
- After the DBMS server is upgraded, the Primary Server should be upgraded, and then the secondary nodes. The appliances in the cluster will not start correctly if they are at incompatible version numbers.
- You must stop all eDiscovery Platform services using the Clearwell Utility on all secondary nodes before upgrading the primary node. Any secondary node that has eDiscovery Platform services running while upgrading the primary node will not be available for upgrade, which might make the Distributed Architecture environment unreliable.
- Depending on the order in which the upgrades complete, the secondary nodes may come up “offline”. If that is the case, from the **Manage Appliances** screen, make sure that every secondary node is “enabled”, and then stop and restart any secondary node that was “offline” once its upgrade completes.

Verify Windows Service Settings

Check **Windows > Services** to verify that Veritas eDiscovery Platform service accounts are setup correctly. When upgrading to 10.2, you can choose to keep the existing service account logon credentials.

User Account for Upgrade Installer

For the upgrade installation, log in to the appliance as the user with administrative privileges (either a local administrator or a domain administrator). In case a domain administrator is used, ensure that you are added to the local administrators' group before starting the eDiscovery Platform installation.

Note: Three unique Veritas eDiscovery Platform service accounts are required, and a fourth unique Veritas eDiscovery Platform account is strongly recommended to optimize performance when doing MBOX/OST conversions. Make sure that the rules described in the Guidelines for Domain User Accounts section are followed. These policies should be verified to make sure no periodic domain policies override the local appliance settings to remove these.

Guidelines for Domain User Accounts

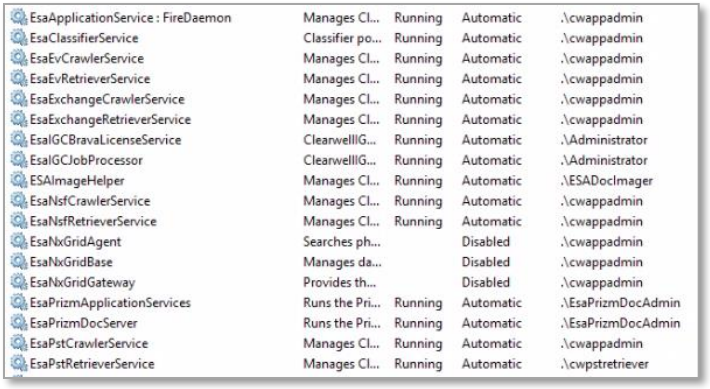
Before you start upgrading Veritas eDiscovery Platform software, you should verify the domain user accounts. Make sure that all of these domain user accounts have administrative privileges and are members of the Local Administrator group on the appliance. Also verify no Group security policies exist that will remove that new user from the Local Administrator group.

Service	Username (example)	Rules for Account Credentials
EsaApplicationService	appadmin	• Run the *EsaPstCrawlerService* and *EsaPstRetrieverService* as "Local System." These services must use different "Log On As" accounts and must have read/write access to source data. • Use the same account credentials for *EsaApplicationService*,
EsaPstCrawlerService	appadmin	
EsaPstRetrieverService	pstretriever	
EsaNsfCrawlerService	appadmin	
EsaNsfRetrieverService	appadmin	
EsaExchangeCrawlerService	appadmin	
EsaExchangeRetrieverService	appadmin	

Service	Username (example)	Rules for Account Credentials
EsaEvCrawlerService	appadmin	*EsaNsfCrawlerService*, *EsaNsfRetrieverService*, and *EsaPstCrawlerService* *EsaClassifierService* • The security settings must match the EsaApplicationService: FireDaemon "Log On As" credentials.
EsaEvRetrieverService	appadmin	
EsaPrizmDocServer	EsaPrizmDocAdmin	• The eDiscovery Platform installer creates the **EsaPrizmDocAdmin** local user with admin privileges for PrizmDoc services. • The following special characters are not supported for the PrizmDoc service password: Double quote: " Single quote: ' Backslash: \ Equal to: =
EsaPrizmApplicationServices		
EsaImageHelper	ESADocImager	• The user account for the service has the "Log On As" service right and is not an account that manages any other Clearwell services. • At a minimum, the user account must be a domain user account and have UNC access (versus a drive letter) to read and write to the Veritas eDiscovery Platform appliance. For example, \\<*appliance-IPadddress*>\d$\<*dir*>\<*dir*>\...
EsaClassifierService	appadmin	• Use the same account credentials used for *EsaApplicationService*

Requirements for the Service “Log On As” accounts:

- Use the *Domain\Account* format instead of the *Account@Domain.com* format.
- Make sure these Domain accounts have full control (read/write) access to any appropriate network shares.
- Make sure these Domain accounts are members of the Local Administrator group
- Make sure no domain or group policies will remove these accounts from the “logon locally” or “logon as a service” rights.
- In the Veritas eDiscovery Platform UI **System > Settings**, you should enter the same “Log On As” account credentials as you used for the *EsaApplicationService* for the Windows authentication user name and password.
- If you change the “Log On As” credentials for the *EsaNSFCrawlerService* or *EsaNSFRetrieverService*, then you must logon to the appliance using the same user account specified and initialize the IBM Notes Client (see 27 When the installer prompts for IBM Notes initialization, click **Yes** to initialize IBM Notes. in this document).

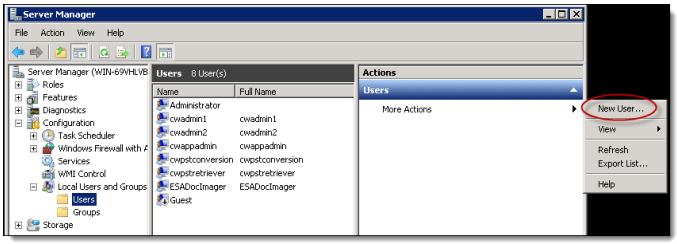


EsaApplicationService : FireDaemon	Manages Cl...	Running	Automatic	.\cwappadmin
EsaClassifierService	Classifier po...	Running	Automatic	.\cwappadmin
EsaEvCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaEvRetrieverService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaExchangeCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaExchangeRetrieverService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaIGCBravaLicenseService	ClearwellIG...	Running	Automatic	.\Administrator
EsaIGCJobProcessor	ClearwellIG...	Running	Automatic	.\Administrator
ESAImageHelper	Manages Cl...	Running	Automatic	.\ESADocImager
EsaNsfCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaNsfRetrieverService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaNxGridAgent	Searches ph...		Disabled	.\cwappadmin
EsaNxGridBase	Manages da...		Disabled	.\cwappadmin
EsaNxGridGateway	Provides th...		Disabled	.\cwappadmin
EsaPrizmApplicationServices	Runs the Pri...	Running	Automatic	.\EsaPrizmDocAdmin
EsaPrizmDocServer	Runs the Pri...	Running	Automatic	.\EsaPrizmDocAdmin
EsaPstCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaPstRetrieverService	Manages Cl...	Running	Automatic	.\cwpstretriever

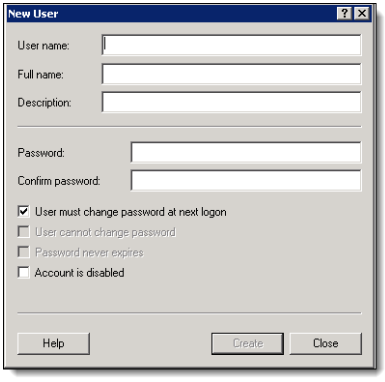
Adding domain user account to the Local Admin Group on Appliance

To add the service accounts to the Local Administrators Group on appliance:

1. Click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
2. Under **System Tools**, click **Local Users and Groups**.
3. Click **Users**. Under **Users**, click **More Actions**.

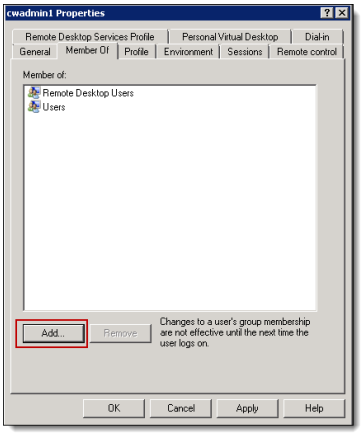


4. Click **New User**.



5. Enter the username in the **User name** field.
6. Enter the password in the **Password** field and the **Confirm password** field.
7. Clear the **User must change password at next logon** check box.
8. Click **Create**. The user will appear in the Users list.
9. Right-click on the user name, and then click **Properties**. Alternatively, under **Actions** > **<user name>** > **More Actions**, click **Properties**.

10. On the <user name> Properties dialog, click the **Member Of** tab.



11. Click **Add**.
12. On the Select Groups dialog, enter the group name (Administrators) in the **Enter the object names to select** field, and then click **Check Names**. The group name (Administrators) appears in the **Enter the object names to select** field.
13. Click **OK**. The (Administrators) group will appear in the **Member of** list on the <user name> Properties dialog.
14. Click **OK**. The user gets added to the (Administrators) group.

Verify Windows Firewall Settings

Go to **Start > Settings > Control Panel > Windows Firewall**. Note whether the Firewall is configured to be On or Off. After the 10.2 upgrade, you should verify this setting is set to Off. If you have communication problems with nodes in the cluster after you have upgraded to 10.2, then you may need to turn the firewall Off after the installation.

Verify eDiscovery Platform Cases Before the Upgrade

In Veritas eDiscovery Platform, go to **All Processing > Processing > Cases** tab and verify that all cases are online before the upgrade. You should also verify that no cases are in a "Processing" status indicating that new data is being processed, or that no exports are in progress. Additionally, you should verify that you do not have any more than 100 cases active in a non-clustered configuration.

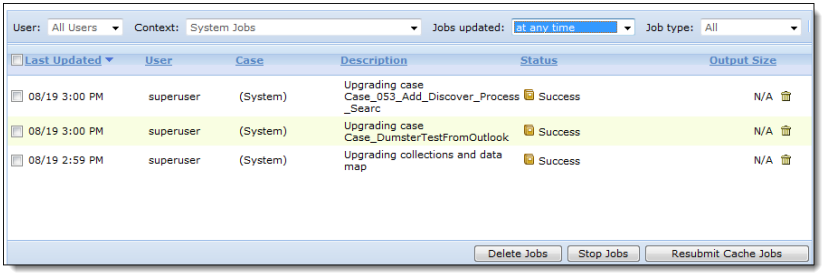
IMPORTANT! If your case backups are stored locally, Veritas recommends first backing them up to a remote location before continuing with the upgrade. Refer to the "Backup and Restore" section of the *Veritas eDiscovery Platform System Administration Guide* to back up your cases to a remote location.

Cleanup Veritas eDiscovery Platform Jobs

1. From within the Veritas eDiscovery Platform **System > Jobs** screen, change the Context to "All Jobs" and change the Jobs updated "at any time"
2. Select the Status column to sort by Status and verify that no jobs are in an "unfinished" status.

   Once you upgrade to 10.2, you will not be able to "Retry" or "Finish" any jobs that were partially completed.
3. You should also stop any Pending jobs as they will need to be rerun again once the upgrade has completed.
4. Ensure that there are no LEF processes (E01) running after the jobs stop.
5. Select the "Output Size" column to sort by size to verify if there are several large export jobs remaining in the system.
6. If there are several large export/print jobs that are no longer needed, delete them now to save considerable time during the full node backups. If the exports are still needed, they should be saved to another location and then deleted from Veritas eDiscovery Platform.

Note that if the export jobs were not zipped, the size will display as N/A, so these jobs should be checked as well to see if there is a large amount of backup content.



Verify System Time Zone Settings

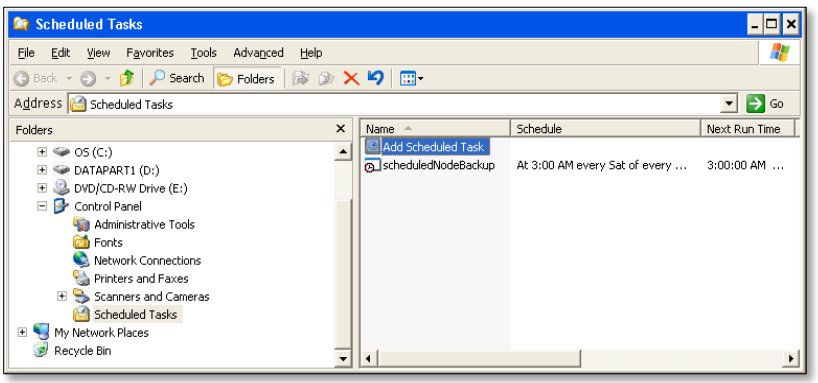
Verify the Windows time zone setting to make sure it is set appropriately for your environment.

For a cluster configuration, verify that all servers in the cluster are configured to the same time zone with their clocks within two minutes of each other. Otherwise, the systems will not be able to be clustered together.

During installation, when Veritas eDiscovery Platform services are being installed, the Date and Time dialog may also appear, allowing you to change the date/time, and/or change the time zone.)

Verify Scheduled Tasks

Verify if there are any scheduled tasks to perform routine full node backups. Go to **Start** > **Settings** > **Control Panel** > **Scheduled Tasks** or **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Task Scheduler**. Review the list of tasks to see if there any Veritas eDiscovery Platform full node backups are scheduled. If so, disable or delete this scheduled task. After the 10.2 upgrade, a new task will need to be scheduled pointing to the backup script in the new 10.2 directories.



Close Windows Explorer and all Remote Login Sessions

Ensure Windows Explorer, and all Microsoft programs and prompts are closed, so that no folder will be locked during installation. Also, be sure to close all remote login sessions, to prevent other users' login sessions from interfering with remote drive installation (<Second Drive>:\MySQL) so that the folder can be accessed by Veritas eDiscovery Platform.

Check Microsoft Office Version and Activation Status

Veritas eDiscovery Platform supports version 2016 and version 2019 of Microsoft Office Professional Plus application. To avoid compatibility and license key issues, check the appliance to see what version of Microsoft Office is currently installed and the product activation state.

To check MS Office version and activation status

1. On the appliance to be upgraded, open any Microsoft Office 2016 or Office 2019 application and click **Help** on the **File** menu. To the right of the dialog box, under the Microsoft Office logo, a message displays with either "**Product Activated**" or "**Product Activation Required**".

   If you have Office 2016 or Office 2019 with “Product Activated”, then you do not need to obtain a license key for the upgrade.

Note: You must obtain and install the Microsoft Office Professional Plus 2016 or Office 2019. Also, install all the latest patches.

Veritas Enterprise Vault API Runtime

If applicable to your environment, decide whether to use 11.x or 12.x version of Veritas Enterprise Vault API Runtime or accept the installation of Veritas Enterprise Vault API Runtime 12.4.0.

IMPORTANT! The Enterprise Vault API Runtime client must be compatible with the Enterprise Vault server version. Also, ensure that your appliance is in the same domain as the Enterprise Vault Directory server.

If your environment requires 11.x or 12.x version of Veritas Enterprise Vault, do the following:

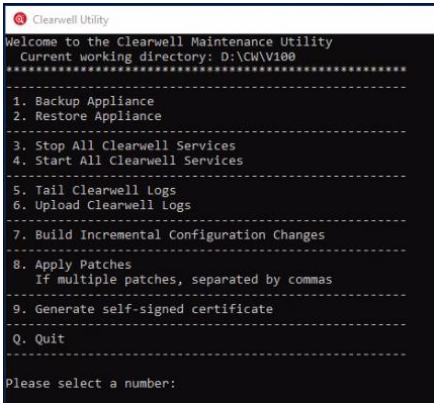
1. Select the **Custom** install option.
2. Deselect the **Veritas Enterprise Vault API Runtime12.4.0** selection.
3. Allow the Veritas eDiscovery Platform install to complete.
4. Install the required EV client runtime libraries to match the version of your EV server.

Perform Full Node Backups on All Appliances

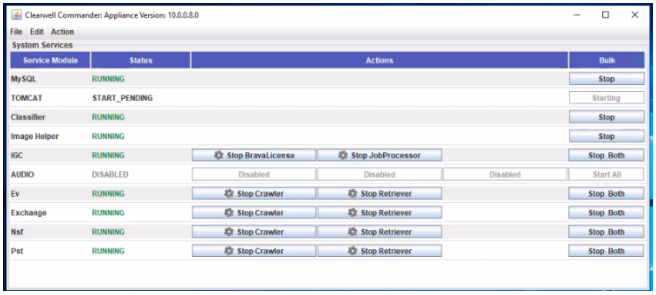
Before upgrading to 10.2, the following steps must be taken.

1. Verify space and backup locations in preparation for performing a full node backup. Verify the following on the system:
   - Total space available on the D: drive is at least 1 TB.
   - Total number of files in the <*installation directory*>*data* directory. If there are more than 100,000 files in this directory, then you most likely have several export jobs still in the **System** > **Jobs** location on the Veritas eDiscovery Platform appliance. See Cleanup Veritas eDiscovery Platform Jobs section for more information.
   - Target location for the full node backups: (Default is <*installation directory*>*backups* unless this has been configured to back up elsewhere).
   - Target location for the case backups: (Default is <*installation directory*>*caseBackups* unless this has been configured to back up elsewhere).
2. Review backup policies to make sure case and system backups are scheduled periodically and preferably in a location off of the appliance. For more information, refer to the *Veritas eDiscovery Platform System Administration Guide*.

3. Using Option 1 in the Clearwell Utility on the Appliance desktop, perform a Full Node Backup. When prompted "Would you like to include case backups? (y,n)", select **n**.



Alternatively, you can perform a backup using the **Action** > **Backup Appliance** option on the Clearwell Commander on the Appliance desktop.



Full node backups will take potentially several hours depending on the number and size of cases on the appliance. Typical full node backup rates are approximately 20 minutes per 1 million documents assuming that export jobs have been cleaned up as described in the previous section, "Cleanup Veritas eDiscovery Platform Jobs." Times may vary depending on the specifics of your deployment.

Perform Windows Updates

Make sure that the latest Windows updates are installed at the time of the upgrade. Remember to stop all Veritas eDiscovery Platform Services before restarting Windows.

Note: The best practice is to stop all Veritas eDiscovery Platform services cleanly whenever possible before restarting Windows. To stop all services, use the Clearwell Utility on the desktop. Select number 3 to "Stop All Clearwell Services."
Alternatively, use the **Action** > **Stop Appliance Services** option on the Clearwell Commander.

Verify Appliance Hardware

It is recommended you take the opportunity during this maintenance window to verify that all hardware components are operating effectively. If you have a Dell appliance, it is recommended to install the Dell DSET application if you do not currently have it installed.

This will run some Hardware diagnostics and flag any errors. Manually inspect the server to ensure that there are no red warning lights needing attention.

Chapter 4

Upgrade Installation Steps

The following steps provide instructions for upgrading an appliance from pre-10.2 version to 10.2.

Cluster Considerations

If you have a cluster of Veritas eDiscovery Platform appliances, **you need to upgrade all servers in the cluster**. The appliances in the cluster will not start correctly if they are at incompatible version numbers.

Be sure to upgrade your components in the following order:

(1) the remote database server

Note: If you have a remote database server, you must run the DBMS utility installer first irrespective of whether the remote database server is located on the same node as the cluster primary or on a remote server.

---

(2) the primary server

Note: You must stop all eDiscovery Platform services using the Clearwell Utility on all secondary nodes before upgrading the primary node. Any secondary node that has eDiscovery Platform services running while upgrading the primary node will not be available for upgrade, which might make the Distributed Architecture environment unreliable.

---

(3) any secondary appliances

Veritas eDiscovery Platform Product Installation/Upgrade Instructions

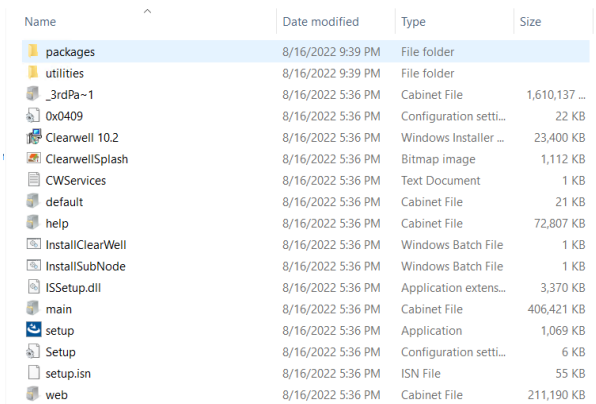
1. Complete the Pre-Installation steps required in the previous sections.
2. Confirm that a Full Node backup was completed (on all appliances in case of a Cluster configuration).
3. Verify that no other Remote Desktop sessions are open with Windows or applications running that may interfere with the installation.
4. Close all browsers and other applications prior to the upgrade. Unzip the installer into a temporary directory (D:\tmpInst directory).
5. Navigate to the directory where you want to download the file and unzip the installer zip file. For example:

   D:\CW\Installer\Distributions\<Release>

Note: The installer file naming convention is:

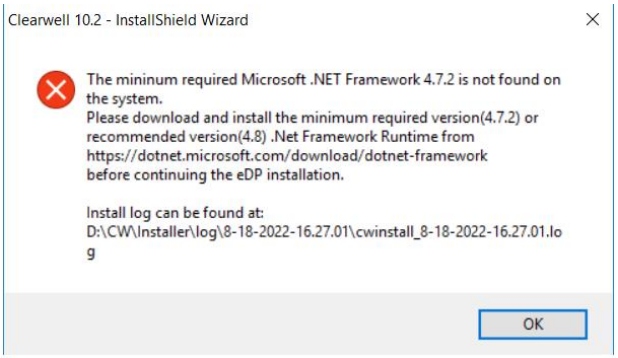
Veritas_eDiscovery_Platform_Installer_<release>_Win_EN.zip.

Double-click on the **InstallClearwell.bat** program.

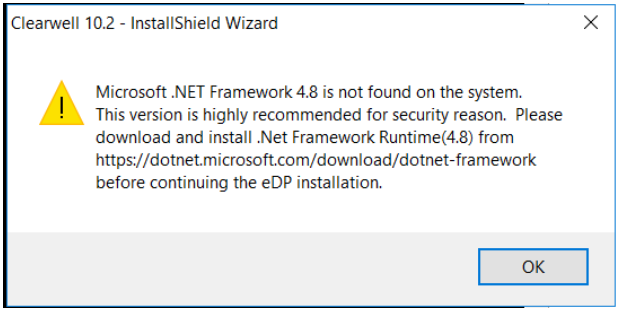


Name	Date modified	Type	Size
packages	8/16/2022 9:39 PM	File folder	
utilities	8/16/2022 9:39 PM	File folder	
_3rdPa~1	8/16/2022 5:36 PM	Cabinet File	1,610,137 ...
0x0409	8/16/2022 5:36 PM	Configuration setti...	22 KB
Clearwell 10.2	8/16/2022 5:36 PM	Windows Installer ...	23,400 KB
ClearwellSplash	8/16/2022 5:36 PM	Bitmap image	1,112 KB
CWServices	8/16/2022 5:36 PM	Text Document	1 KB
default	8/16/2022 5:36 PM	Cabinet File	21 KB
help	8/16/2022 5:36 PM	Cabinet File	72,807 KB
InstallClearWell	8/16/2022 5:36 PM	Windows Batch File	1 KB
InstallSubNode	8/16/2022 5:36 PM	Windows Batch File	1 KB
ISSetup.dll	8/16/2022 5:36 PM	Application extens...	3,370 KB
main	8/16/2022 5:36 PM	Cabinet File	406,421 KB
setup	8/16/2022 5:36 PM	Application	1,069 KB
Setup	8/16/2022 5:36 PM	Configuration setti...	6 KB
setup.isn	8/16/2022 5:36 PM	ISN File	55 KB
web	8/16/2022 5:36 PM	Cabinet File	211,190 KB

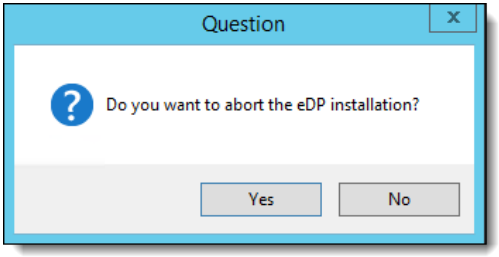
6. A warning is issued if .NET Framework 4.7.2 is not installed on the system. It is required to install this version for security reasons. Click **OK**. Install .Net Framework 4.7.2 and restart the upgrade process.



7. A Warning is issued if .NET Framework 4.8.0 is not installed on the system. It is Recommended to install this version for security reasons. Click **OK**.



8. Click **No** to continue the eDiscovery Platform installation if .NET 4.7.2 is installed on your system.



9. Click **Next** on the Clearwell 10.2 screen.
10. Read and acknowledge acceptance of the terms of the Veritas license agreement. Click **Next**.

A warning about installing Cumulative Hotfixes available for the upgraded version is displayed.

Upon accepting license terms and clicking **OK** for the warning, Veritas eDiscovery Platform stops services before continuing the installation. Click **Yes** to continue.

11. A warning will appear if Veritas eDiscovery Platform detects that the appliance does not meet the minimum requirements, or there are Windows features that should be disabled to maximize space on the C: drive:

    A. Ensure you have enough (or free up) space on the C: Drive before continuing the installation.

    B. Veritas recommends disabling the “Windows Error Reporting and Problem Reports and Solutions” feature to maximize space on the C: Drive before continuing the installation.

       Follow the steps for the Windows Server 2016, and Windows Server 2019 operating system:

       Go to **Control Panel** > **System and Security > Action Center** > **Maintenance** > **Settings** > select the option " **I don't want to participate, and don't ask me again**" > click **OK**.

       IMPORTANT! If you still do not have sufficient drive space available, contact Veritas Technical Support, who can advise on a remediation approach.

    C. Veritas recommends disabling the “Windows memory dump” feature to maximize space on the C: Drive before continuing the installation.

       To disable, follow the steps for the Windows Server 2016, and Windows Server 2019 operating system.

       Go to **Control Panel** > **System and Security** > **System** > **Advance System Settings** and click **Settings** in **Startup and Recovery**, under the **Write debugging information** drop-down menu, select **(none)** and click **OK**.

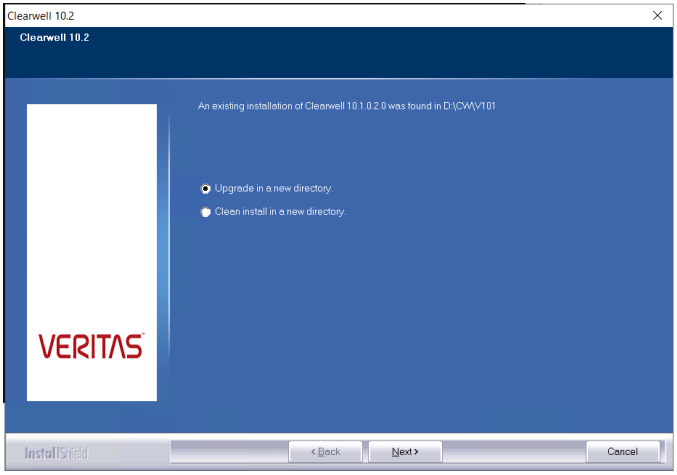
       Click **Yes** to continue.

12. At the prompt, click **Yes** to confirm stopping Veritas eDiscovery Platform services and to continue with the installation.

Note: Veritas eDiscovery Platform will automatically check for previous (upgradeable) versions. If a non-upgradeable version is installed, upgrade to the supported upgradable version before proceeding.

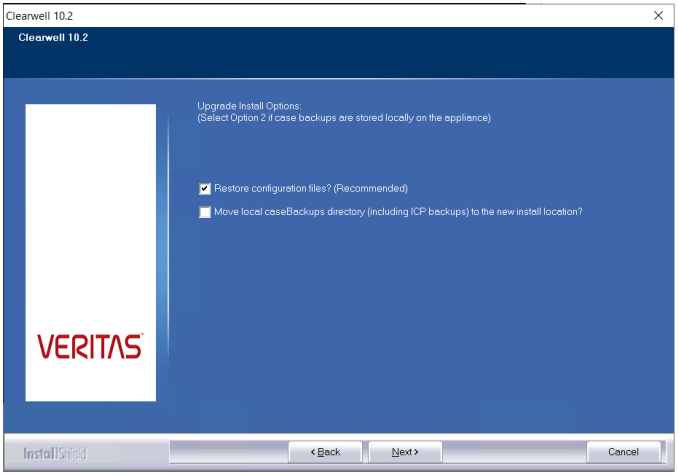
---

13. Select **Upgrade in a new directory** unless you want to remove all of your Veritas eDiscovery Platform cases and start clean with 10.2 and click **Next**.

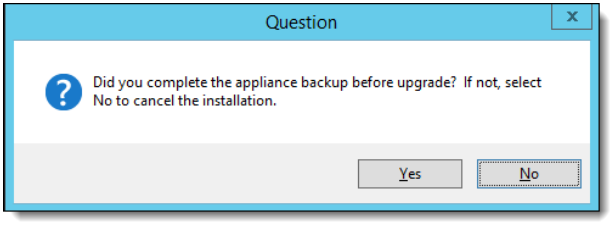


14. Choose the appropriate selection and click **Next**:
    - Option 1: Restore configuration files? (Recommended)
    - Option 2: Move local caseBackups directory (including ICP backups) to the new installation

    eDiscovery Platform keeps the existing security certificate by default.



15. The following dialog serves as a reminder to perform the appliance backup outside of this installation if it has not already been done. Click **Yes**.



16. On the Choose Destination Location screen, leave the default 10.2 installation directory as is, and click **Next**.

    IMPORTANT! Virus scanning exclusion rules must also be updated or changed to the new installation directory. Refer to the *Virus Scanning Guidelines* section in the *Veritas eDiscovery Platform System Administration Guide*.

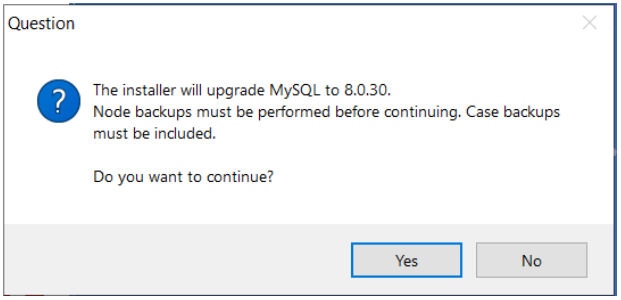
For Setup type, leave the default selection, **Complete**, and click **Next**.
The installer will only install the software components that are missing from the appliance or need upgrade.

IMPORTANT! Select **Custom** only to view the individual software components that will be installed, but do not change any of the default selections which are required as part of the installation. Selecting **Custom** displays the Select Features screen showing the third-party components to be installed with 10.2. Click **Next**.

Note: Veritas Enterprise Vault API Runtime 12.4.0 is installed with 10.0. If your environment requires the 11.x or 12.x version of Veritas Enterprise Vault API Runtime, then do the following:

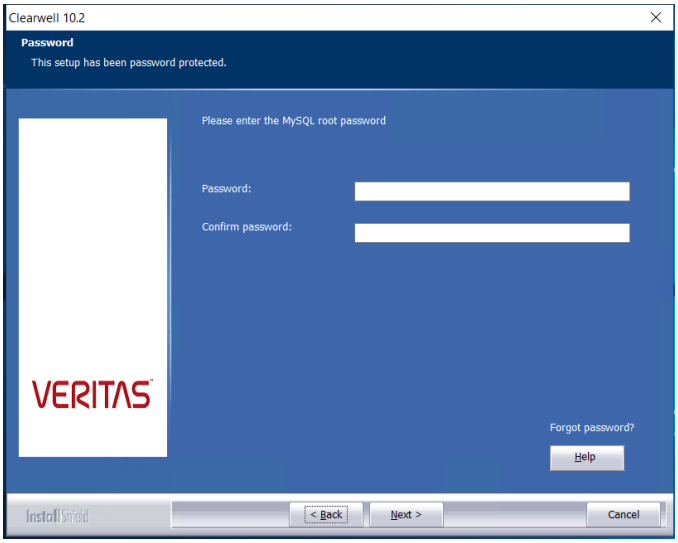
1. Select the **Custom** install option.
2. Deselect the **Veritas Enterprise Vault API Runtime 12.4.0** selection.
3. Allow the Veritas eDiscovery Platform install to complete.
4. Install the required EV client runtime libraries to match the version of your EV server.

A warning is issued to upgrade MySQL to 8.0.30. Node backup must be performed before continuing. Click **Yes**.

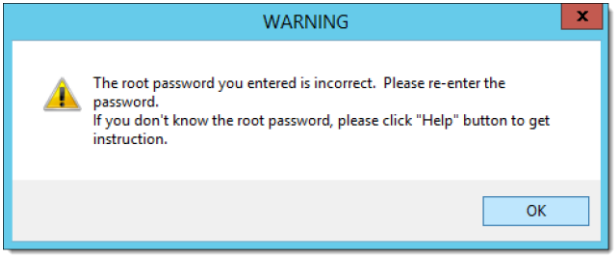


If you have changed the MySQL root password for your earlier version of installation, the system prompts you to enter and confirm the MySQL root password.

Enter your MySQL root password, and then click **Next**.



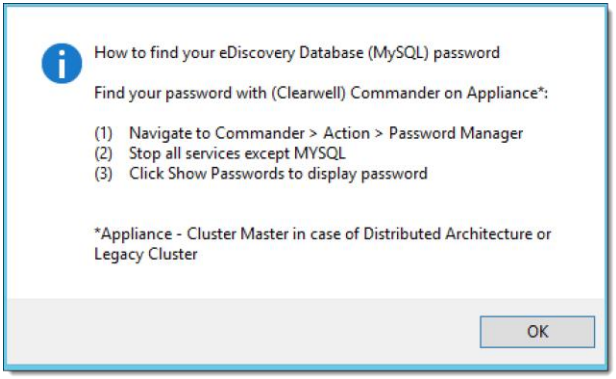
If an incorrect password is entered, a warning appears. Click **OK** to go back to the Password screen.



If you do not remember your MySQL root password, click the **Help** button.

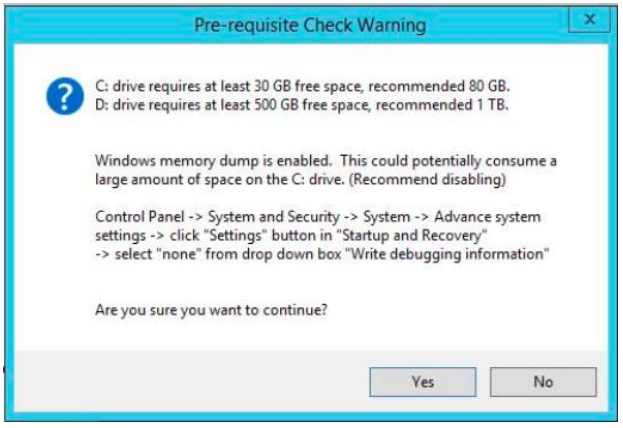
A. Navigate to **Clearwell Commander** > **Action** > **Password Manager**.
B. Stop all services except MySQL.
C. Click **Show Passwords** to display the password.

Instructions to find the password are shown in the dialog message that displays.

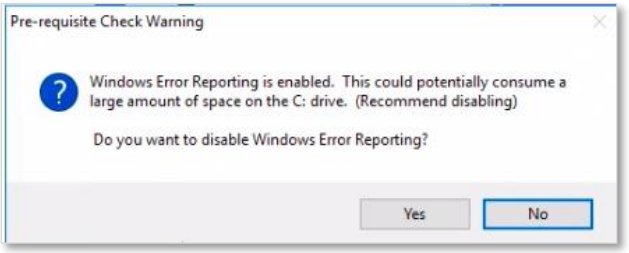


Click **OK** to continue the installation.

A warning is issued about memory space and Windows Updates requirements. Click **Yes**.



A warning is issued about Windows Error Reporting. Click **Yes**.



IMPORTANT! After Enterprise Vault is uninstalled, the following pop up will notify you of the same and a restart of the appliance will be required. Click **OK**.

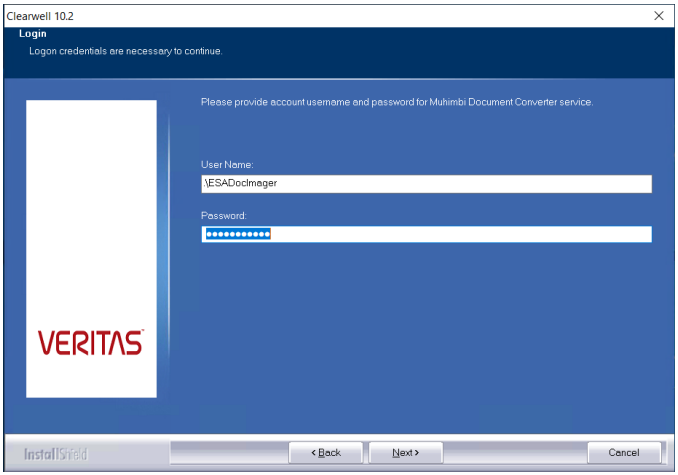
Note: If an older version of Enterprise Vault is detected, a warning is issued about uninstalling the older version. Hence the installer asks for a single reboot after uninstalling the older version of Enterprise Vault. Another reboot will be required only after the upgrade is completed as mentioned in step 31.

After the reboot, the installer starts automatically. If not, rerun **InstallClearwell.bat**.

A warning is issued about matching the Enterprise Vault versions. Click **OK**.

17. Check that the time zone settings are correct and click **OK**.

18. The system prompts you to enter credentials for Muhimbi Document Converter service. Enter account username and password, and then click **Next**.



19. The system prompts you to enter credentials for PrizmDoc service. Enter account username and password, and then click **Next**.

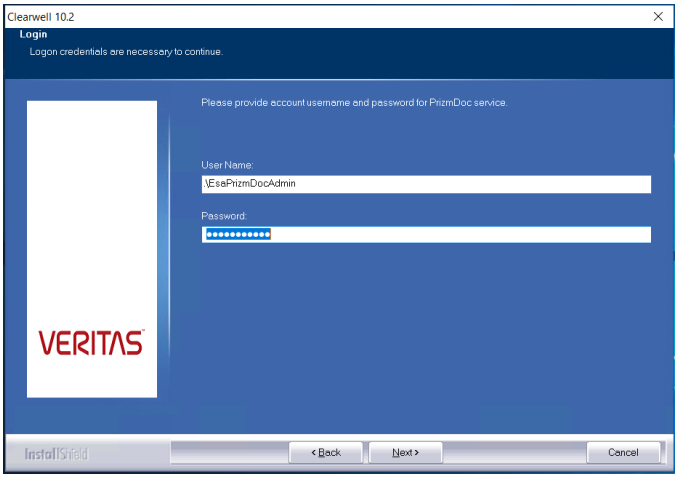
    The following special characters are not supported for the PrizmDoc service password:

    Double quote: "

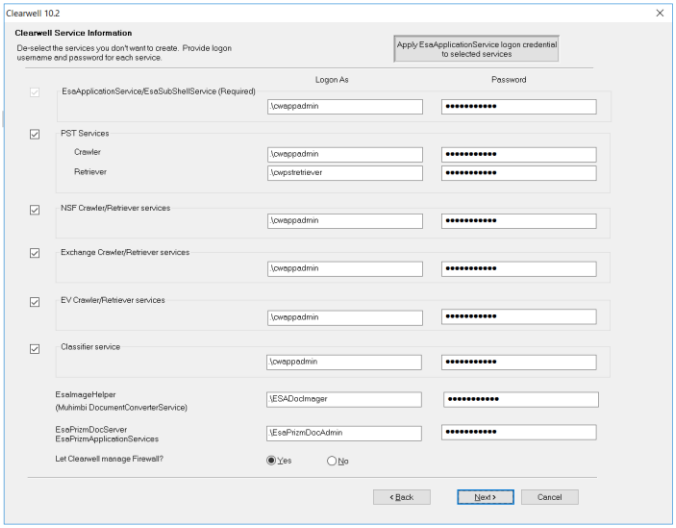
    Single quote: '

    Backslash: \

    Equal to: =


Clearwell 10.2
Login
Logon credentials are necessary to continue.
Please provide account username and password for PrizmDoc service.
User Name:
\EsaPrizmDocAdmin
Password:
VERITAS
InstallShield
< Back
Next >
Cancel

20. On the Setup Type screen, select **Yes** if you want to keep the Veritas eDiscovery Platform service accounts with all their credentials the same as in a prior version.



If you select **No**, then a prompt appears with a window where all the service accounts can be selected/deselected and logon accounts can be configured per service. The accounts are setup with the default appliance *cwappadmin* and *cwpstretriever* local account logon credentials. Click **Next**.

Selecting **No** may also prompt the Date and Time dialog, allowing you to change the Windows defaults, and/or the time zone settings. Click **OK**.

Default credentials for the various services are populated, but can be changed. When finished, click **Next**.

Selecting **Yes** and clicking **Next** prompts Veritas eDiscovery Platform to verify all service accounts. The system automatically checks whether the specified accounts have sufficient permissions to be used as service accounts.

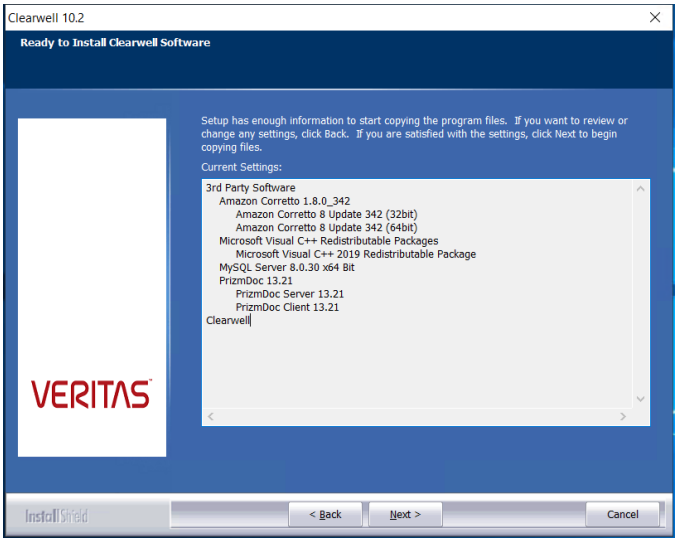
Note: Credentials can be changed on the Clearwell Service Information screen, if required. See Guidelines for Domain User Accounts.

A warning is issued if the “Log On As” account used for the Image Helper Service Account and PrizmDoc Service Account overlaps with

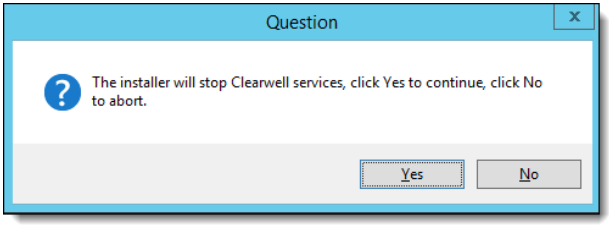
other service accounts. Make sure you use a "Log On Account" as mentioned in the Guidelines for Domain User Accounts section. Click **OK** to continue the installation.

If correct "Log On As" service accounts are used, a message confirming the same appears. Click **OK** to continue the installation.

21. At the prompt, to confirm that Veritas eDiscovery Platform will manage your firewall (recommended), click **Yes**.
22. The Ready to Install Clearwell Software screen displays the program files selected for installation. Click **Next**.



23. Click **Yes**.



24. You may get an error that the directory is in use if any of the following are true:
    - Veritas eDiscovery Platform services were not shut down
    - DOS prompt has a lock on the previous Veritas eDiscovery Platform installation directory
    - If there are file shares in place locking the directory

    A pop-up will appear to ensure that all processes are not already running.

    Important: If you click **Yes**, and you have Microsoft KB 2993651 installed, the font `D:\cw\vXXX\config\templates\jasperreports\ARIALUNI.TTF` will be locked and a "File in use" message is displayed by the Windows OS system.

    Note: There are several changes in font behavior that are associated with security update KB 2993651 (formerly called KB 2982791)

    To mitigate this situation, the question pop-up is displayed to confirm the font file. If you are sure that this font file is the ***ONLY*** file in use, click **Yes** to continue.

    Check **Windows > Task Manager** and confirm that there are no Veritas eDiscovery Platform or IBM Notes processes running such as cwjava.exe, *crawler.exe, *retriever.exe, firedaemon*, lef*.exe, ntmulti.exe, nnotesmm.exe, nlnotes.exe, nslsvice.exe and scandir.exe.

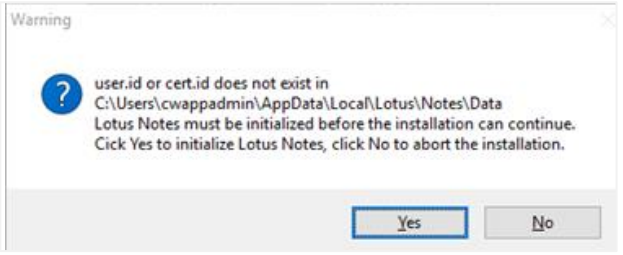
    If any of these processes are present, stop any Veritas eDiscovery Platform services if they are still running. If this does not resolve the issue, then end the process or processes with Task Manager.

    If you cannot determine which application is "locking" the prior Veritas eDiscovery Platform installation directory, the Windows Process Explorer Utility can be used to find it. You can download the Process Explorer utility is from: http://technet.microsoft.com/en-us/sysinternals/bb896653. Once downloaded, run the **procexp.exe** program. If you are unable to determine the cause of a lock, contact Veritas technical support for assistance.

    0 Select **Find > Find Handle or DLL...** Enter the locked directory (d:\cw\vXXX) and then click **Search**.

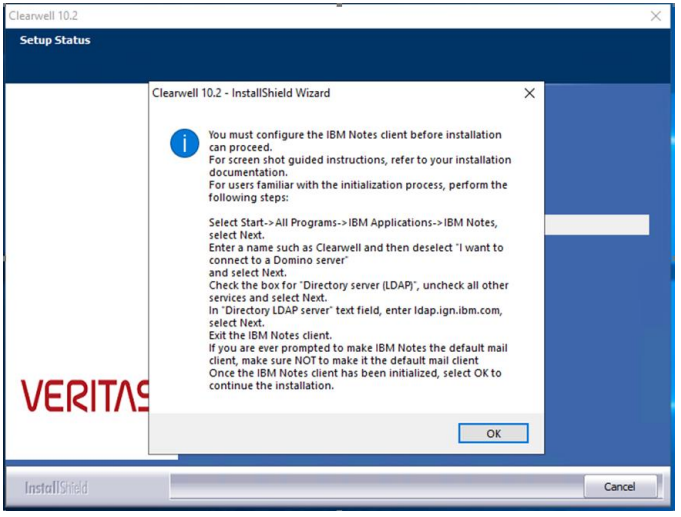
1. Once you are able to locate the program locking the installation directory, end that program, and then quit the Process Explorer program.

25. The Veritas eDiscovery Platform installation will proceed to install the necessary components. Click **Next**.
26. If IBM Notes 10.0.1 is not installed in an earlier release of eDiscovery Platform, the 10.1 installer installs IBM Notes 10.0.1. If IBM Notes 10.0.1 is already present on the system, skip to Step 33.
27. When the installer prompts for IBM Notes initialization, click **Yes** to initialize IBM Notes.



Initialization instructions and screenshots are documented in the next steps but are also shown in the dialog message that displays.

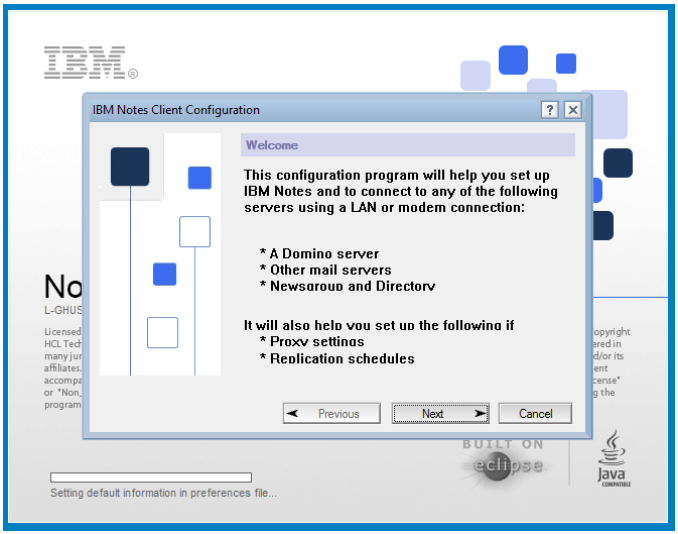
If IBM Notes is already initialized, you may not see this screen.



Click **OK** to continue. You must perform the next steps to manually initialize IBM Notes.

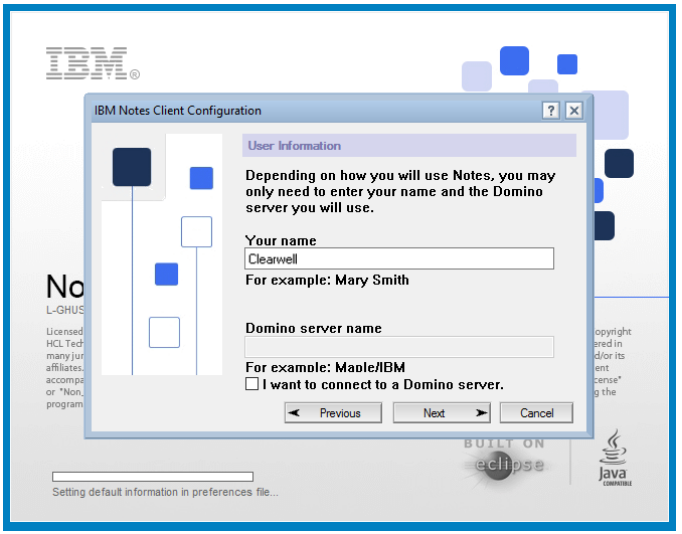
Note: Even if you do not have a Domino server, you must complete the IBM Notes installation to complete the installation of Veritas eDiscovery Platform.

28. Use Remote Desktop to the server with a second connection to proceed with the initialization of IBM Notes. Logon to the appliance with the account credential provided in the NSF Retriever or Crawler service (if you have not already done so).
Go to **Start** > (**All**) **Programs** > **IBM Applications** > **IBM Notes 10.0.1** to launch the Notes client. Click **Next**.

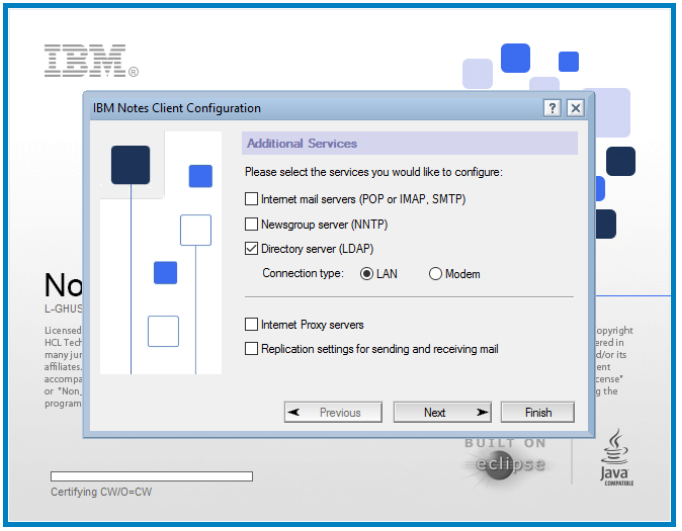


29. Enter **Clearwell** in the name field and clear (deselect) the option **I want to connect to a Domino server**. Click **Next**.

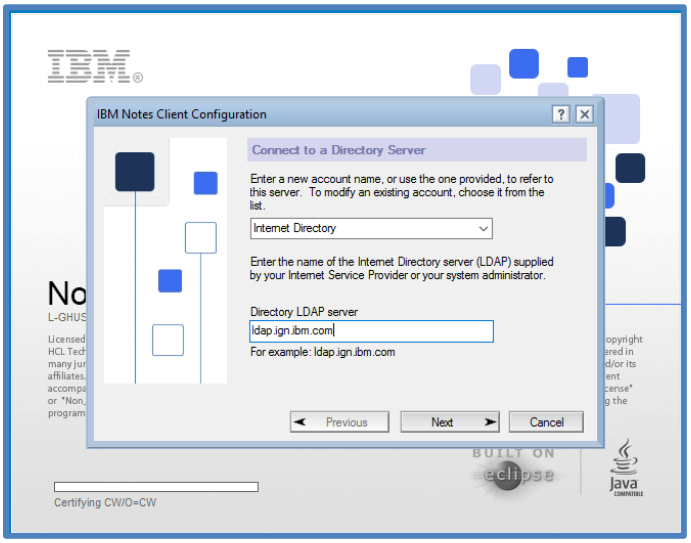
Note: If you are using a Domino server, then keep the option I want to connect to a Domino server selected and then enter the Domino settings on the following screens.



30. Select **Directory server (LDAP)**. Click **Next**.



31. Enter **ldap.ign.ibm.com** in the text box labeled **Directory LDAP server**.

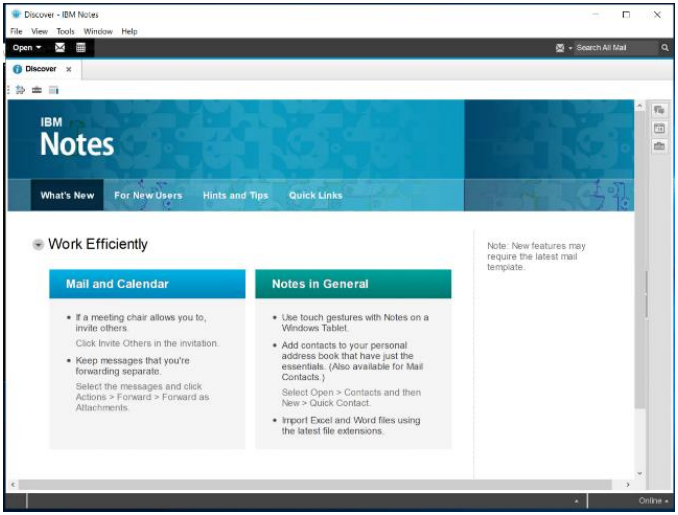


Click **Next** to complete IBM Notes setup.

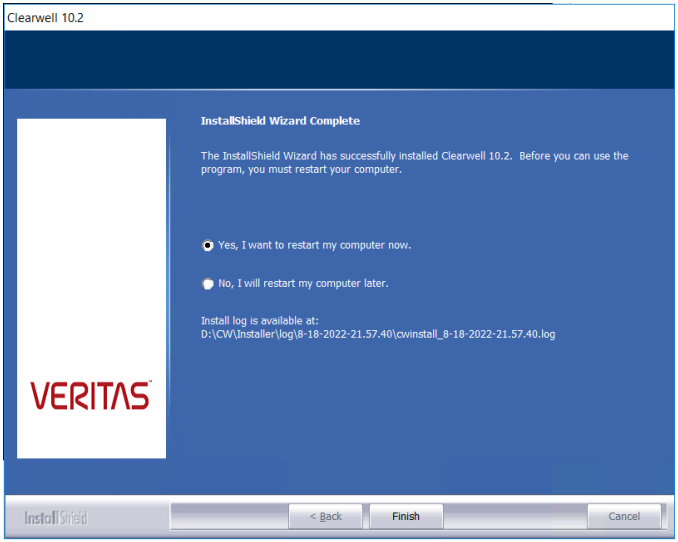
Note: You might receive a popup box stating: "IBM Notes is not currently set as your default email program. Would you like to set it now?" Make sure that IBM Notes is not set as the default mail client during the IBM Notes client installation. Microsoft Office Outlook should be the default mail client.

---

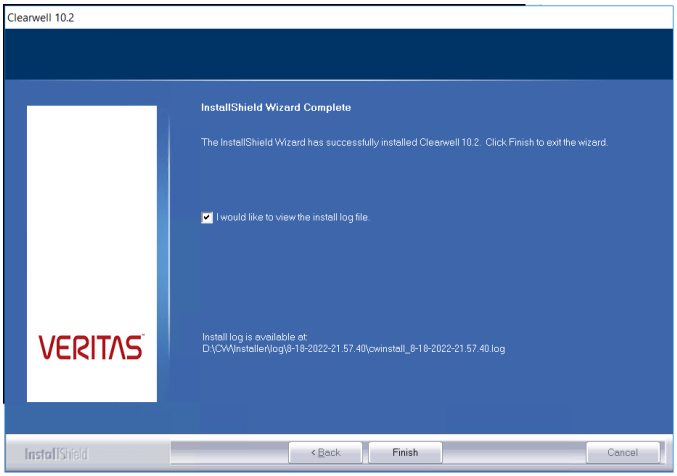
32. On the **Getting Started** screen, close **IBM Notes** and select the option **In the future, exit without prompting**.



33. Go back to the Installer dialog and click **OK** to continue.
34. The system continues the installation. After installation completes, select **Yes, I want to restart my computer now**, and then select **Finish** to reboot the system.



If you select **No, I will restart my computer later** and click **Finish**, then the following screen appears.


Clearwell 10.2
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed Clearwell 10.2. Click Finish to exit the wizard.
I would like to view the install log file.
Install log is available at:
D:\CW\installer\log\8-18-2022-21.57.40\cwinstall_8-18-2022-21.57.40.log
VERITAS
InstallShield
< Back
Finish
Cancel

(Optional) Setting Up Your System for Audio Processing

Users who have purchased the Audio Processing option can process and search the audio or media files for new cases created on the 10.2 release. This section describes the prerequisites and the installation steps for installing the Audio Search tools.

Note: Perform the procedures described in this section and if you have purchased the optional Audio Processing feature. If you already have set up your system for audio processing in earlier release and now upgrading to 10.2, you do not need to perform these procedures.

After you complete the upgrade of Veritas eDiscovery Platform, you should perform the following steps to set up your system for audio processing:

1. Make sure that you have an Enterprise Audio Processing license.
2. Exclude the Audio Search directories from antivirus scans.
3. Configure firewall software.
4. Start the start audio search services and then check if audio search services are running.

These steps are explained in detail in the following sections.

Setting Up Your System: Server-Side

You must meet the following prerequisites to successfully pre-process, analyze, search and run analytics and reports on your audio content.

Prerequisites

Audio License

Veritas eDiscovery Platform offers an Enterprise Audio Processing license which is a usage model based on the number of hours of audio content that has been processed. The system maintains an up-to-date inventory of the number of hours of audio content that has been consumed and the number of hours available. For more information, see the *Veritas eDiscovery Platform Audio Search Guide*.

Note: The system does not charge for duplicate audio processed files that have the same language pack.

Antivirus Exclusions

By default, the Audio Search software components and a series of language packs is installed when you complete the installation of Veritas eDiscovery Platform. The Audio Search software is installed into the following directories and subdirectories. To avoid interference with critical media operations, be sure to disable virus and malware scanning software. In particular, Malwarebytes Anti-Malware, Kaspersky Endpoint Security, and Microsoft Security Essentials are known to interfere with media operations. Make sure to exclude these directories from antivirus scans:

Directory	Description
C:\Program Files(86)\Nexidia	Language Packs
C:\Program Files(86)\Nexidia\Language Packs	Language-specific Search documentation
C:\Program Files\Nexidia\Search Grid 2.0	Search Grid
D:\Nexidia	Search Grid data and logs
C:\Users\<username>\AppData\Local\Temp	Temporary folder for the account under which Search Grid services run

Firewall Configuration and TCP Port Usage

Make sure you configure any firewall software or other port filtering technology to allow incoming audio-related TCP connections on the ports listed in the following table:

Component	Port #
esa.firewall.port.nexidiapublic.desc=Nexidia Search Grid Gateway Public Port esa.firewall.port.nexidiapublic.port=25002	25002
esa.firewall.port.nexidiamsgbrkr.desc=Nexidia Search Grid Message Broker Port esa.firewall.port.nexidiamsgbrkr.port=25100	25100
esa.firewall.port.nexidiadatabase.desc=Nexidia Search Grid Gateway Database Port esa.firewall.port.nexidiadatabase.port=25101	25101
esa.firewall.port.nexidiagtwyhttp.desc=Nexidia Search Grid Gateway HTTP Port esa.firewall.port.nexidiagtwyhttp.port=25102	25102
esa.firewall.port.nexidiabasehttp.desc=Nexidia Search Grid Base HTTP Port esa.firewall.port.nexidiabasehttp.port=25122	25122

Audio Search Services

By default, the Audio Search software components are installed when you complete the installation of Veritas eDiscovery Platform. Three Nexidia audio search grid services are created (but are not started!) in the Services control panel. Before proceeding any further with the audio search setup, you must start these services.

Name	Service	Description
Nexidia Search Grid Agent Service	EsaNxGridAgent	Performs search and other CPU-intensive operations like phonetic index creation, classification, and language identification
Nexidia Search Grid Base Service	EsaNxGridBase	Manages data storage and communications for Nexidia Search Grid
Nexidia Search Grid Gateway Service	EsaNxGridGateway	Provides the public interface to Nexidia Search Grid

To start audio search services

When you are first starting audio services, use the start audio services command.

- To start the audio services
  Enter the following from a command prompt:
  b start-audio-services (starts only the audio services)
- To start all of the Veritas eDiscovery Platform services including audio
  b start-services

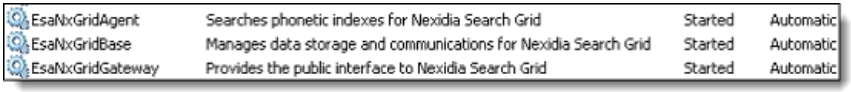
To stop and disable audio search services

Use the stop command when audio processing and search is no longer needed.

- Stop audio search services from a command prompt:
  b stop-audio-services

To check if audio search services are running

If you see the three audio grid services running via the Windows Services control panel then you have successfully installed Audio Search.



Note: The procedure for accessing the Services control panel varies, depending upon the version of Microsoft Windows you are using.

10.2 Installation Verification and Log Files Review

To verify that 10.2 is installed correctly, log on to Veritas eDiscovery Platform and select **System > Appliances**. Select the appliance and verify that it matches Product Version 10.2.0.2.0.

Note: If you have a cluster of Veritas eDiscovery Platform appliances, repeat the verification steps above on ALL appliances in the cluster. All appliances in a cluster must be at the same product version to operate correctly.

It is always a good idea to upload logs to Veritas eDiscovery Platform support following an upgrade.

Go to **System** > **Logs** > **Upload to support** and upload log files.

After the installation completes, the upgrade of all cases may take several minutes or more than an hour depending on the size of cases active in the system at the time of the upgrade. The Veritas eDiscovery Platform appliance should upgrade relatively quickly (approximately 5 minutes), and then all the case upgrades will be kicked off as jobs.

IMPORTANT! You should wait for any upgrade related jobs (case backup) to complete *before* applying any patches or restarting the system. For example, if you opt to move the case backups into the new repository, then it may take several minutes before the backups or archive jobs display.

Once the "Please wait while the Veritas eDiscovery Platform appliance finishes its initialization" warning disappears, then log on to Veritas eDiscovery Platform to track the case upgrade progress. The cases will be upgraded in order of the time the cases were created, with the newest cases being upgraded first. If you want to modify the case upgrade order, then be sure to stop all the upgrade jobs that were automatically submitted, and then manually upgrade the cases in the order you prefer. It is best to stop the upgrade jobs in the first two minutes when Veritas eDiscovery Platform is first available for logging on when cases are still in a "Pending" status.

To track the progress of the case upgrades, check the job in the Jobs window, or from the **System** > **Jobs** screen.

Each case upgrade job will have a job log that can be used to track case upgrade performance. Each case will step through a similar upgrade workflow:

- Applying upgrade of case tables
- Applying upgrade of index tables
- Applying upgrade of email_locator table

1. Applying upgrade of case_temp tables

- Applying upgrade of case_appliance tables
- Applying upgrade of case_group tables
- Checking consistency of case tables

Once cases are upgraded, a post-processing job is automatically started in every case.

Processing jobs can be viewed in the **System > Jobs** screen (by changing the Job Context to “All Jobs”).

Chapter 6

Upgrade Post-Installation Steps

The following steps should be performed *after* the Veritas eDiscovery Platform appliance has been successfully upgraded to 10.2.

Post-upgrade Checklist

After upgrading the Veritas eDiscovery Platform, use the following checklist to ensure that you have set up the software correctly. Review all the procedures in the checklist (some procedures may not be required).

Step	Task
1	Validate upgrade 1. Resolve Microsoft Office license product key issues (if applicable) 2. Review the install logs 3. Confirm correct Veritas eDiscovery Platform version (on all nodes if cluster environment)
2	Apply the latest v.10.2 patch (if applicable)
3	Verify the Veritas eDiscovery Platform license
4	Verify Veritas eDiscovery Platform services started without errors
5	Verify system settings
6	Verify security settings
7	Verify Indexing settings

Step	Task
8	Verify custom logo
9	Verify Veritas eDiscovery Platform configuration settings
10	Verify firewall settings
11	Reconfigure LDAP authentication after upgrade
12	Reconfigure full node scheduled backup tasks
13	Update virus scanning software (if applicable)
14	Disable Adobe automatic update
15	Verify Clearwell Utility
16	Clear browser cache
17	Configure Browser Cache Security (Optional)
18	Verify Veritas eDiscovery Platform cases
19	Run the checksum update job for all eligible cases created in pre-V10.2 releases.
20	Associate Legal Hold and Collections with upgraded cases
21	OST to PST Conversion Libraries
22	To use the OST to PST conversion feature, manually install .NET 4.7.2 after upgrading the eDiscovery Platform.

Post-Upgrade Installation Steps

Validate Install

- Microsoft Office Professional Plus 2016 (or 2019) requires you to enter a valid license product key to activate the product. If you do not activate Office2016 (or 2019) after you install it, the program cannot operate in a fully functional mode. For information on how to activate these Office products, see following sections.
- Review the install log to make sure there were no errors encountered. If additional log files need to be reviewed, all the logs for this installation will be located in the `D:\CW\Installer\log\mm-dd-yyyy-hh.mm.ss` directory and the name of the log file is: `cwinstall_mm-dd-yyyy-hh.mm.ss.log`.

If any of the services fail to start after the upgrade (possibly due to invalid username or password entered on the Installation Services tab), then you will get an error indicating which services were not started. Correct the services after the installation to make sure they all start successfully.

IMPORTANT! If a reboot is required, the CW services are intentionally not started so you can restart the appliance and then start the upgrade.

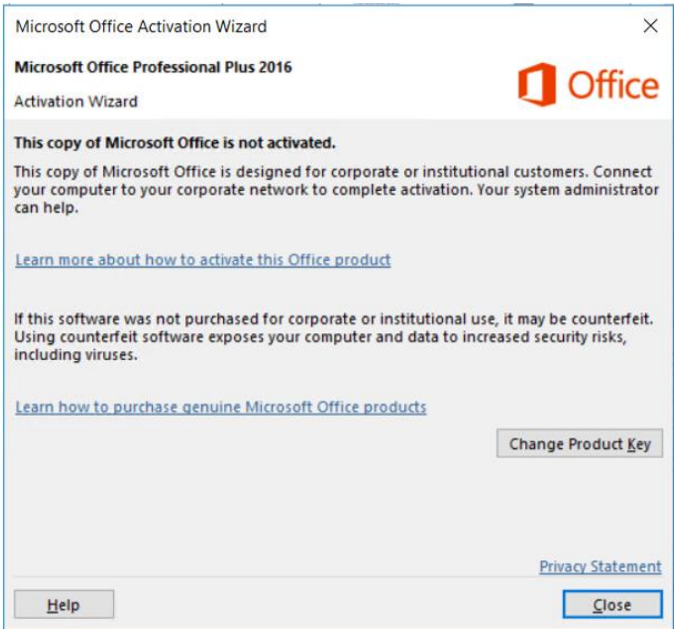
- To verify that the correct version of Veritas eDiscovery Platform was installed, log on to Veritas eDiscovery Platform and select **System** > **Appliances**. Select the appliance and verify that it matches the Product Version 10.2.0.2.0.

Activate Microsoft Office Professional Plus 2016 (for Windows Server 2016)

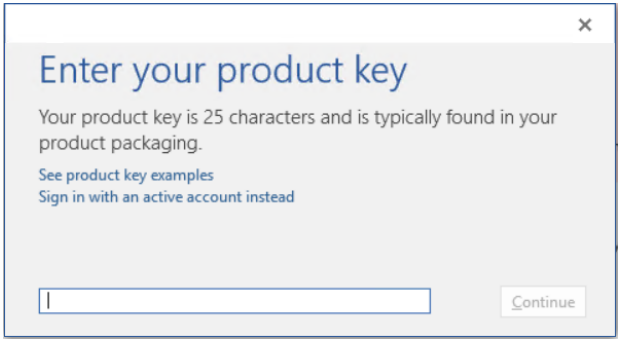
After installing the Veritas eDiscovery Platform 10.2, you must activate Office 2016.

To activate Office 2016:

2. From **Start** > **All Programs** > **Microsoft Office 2016**, open Outlook 2016 or any other Microsoft Office 2016 application such as Word. The Microsoft Office Activation Wizard appears.
3. Click **Change Product Key** on the Microsoft Office Activation Wizard.



4. Enter your 25 characters long product key for Microsoft Office and then click **Continue**..



5. Your Office 2016 gets activated.
6. To confirm the activation, open a Word file and then go to **File** > **Help**. You will see the Office 2016 activation status.

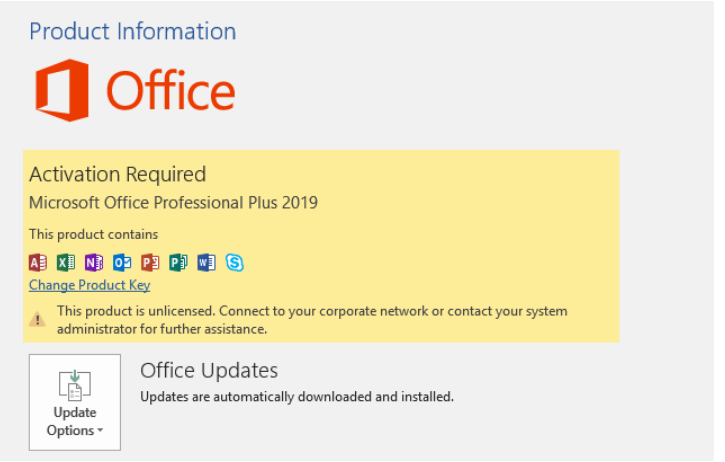
Activate Microsoft Office Professional Plus 2019 (for Windows Server 2019)

After installing the Veritas eDiscovery Platform 10.2, you must activate Microsoft Office Professional 2019.

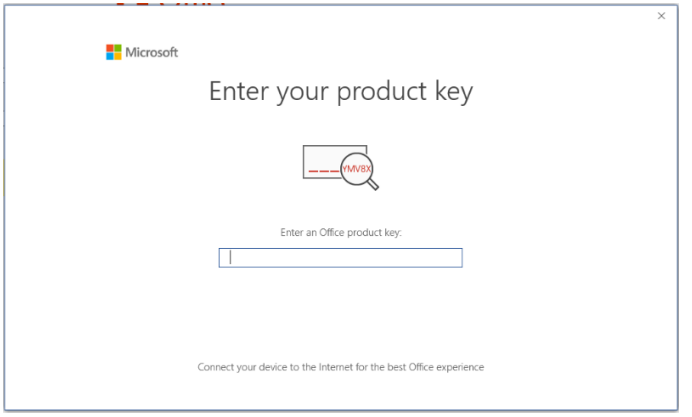
To activate Office 2019:

From **Start** > **All Programs** > **Microsoft Office 2019**, open Outlook 2019 or any other Microsoft Office application such as Word. The Microsoft Office Activation Wizard appears.

1. Click **Change Product Key** on the Microsoft Office Activation Wizard.



2. Enter your 25 characters long product key for Microsoft Office and then click **Continue..**



3. Your Office 2019 is activated.
4. To confirm the activation, open a Word file and then go to **File** > **Help**. You will see the Office 2019 activation status.

Apply the Latest 10.2 Patch (if applicable)

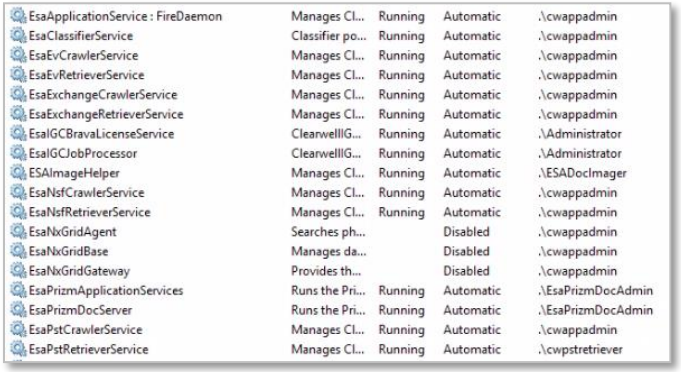
After making sure that the appliance is fully operational and all upgrade scripts have been completed, apply the latest 10.2 Patch if applicable.

Verify the Veritas eDiscovery Platform License

Go to **System > License** to verify your Veritas eDiscovery Platform license. Verify the license type and Evaluation End Date. Contact your Veritas Solution Consultant for any requested license key changes.

Verify Veritas eDiscovery Platform Services

Check the **Windows** > **Services** to verify the Veritas eDiscovery Platform services are setup correctly.



EsaApplicationService : FireDaemon	Manages Cl...	Running	Automatic	.\cwappadmin
EsaClassifierService	Classifier po...	Running	Automatic	.\cwappadmin
EsaEvCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaEvRetrieverService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaExchangeCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaExchangeRetrieverService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaIGCBravaLicenseService	ClearwellIG...	Running	Automatic	.\Administrator
EsaIGCJobProcessor	ClearwellIG...	Running	Automatic	.\Administrator
ESAImageHelper	Manages Cl...	Running	Automatic	.\ESADocImager
EsaNsfCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaNsfRetrieverService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaNxGridAgent	Searches ph...		Disabled	.\cwappadmin
EsaNxGridBase	Manages da...		Disabled	.\cwappadmin
EsaNxGridGateway	Provides th...		Disabled	.\cwappadmin
EsaPrizmApplicationServices	Runs the Pri...	Running	Automatic	.\EsaPrizmDocAdmin
EsaPrizmDocServer	Runs the Pri...	Running	Automatic	.\EsaPrizmDocAdmin
EsaPstCrawlerService	Manages Cl...	Running	Automatic	.\cwappadmin
EsaPstRetrieverService	Manages Cl...	Running	Automatic	.\cwpstretriever

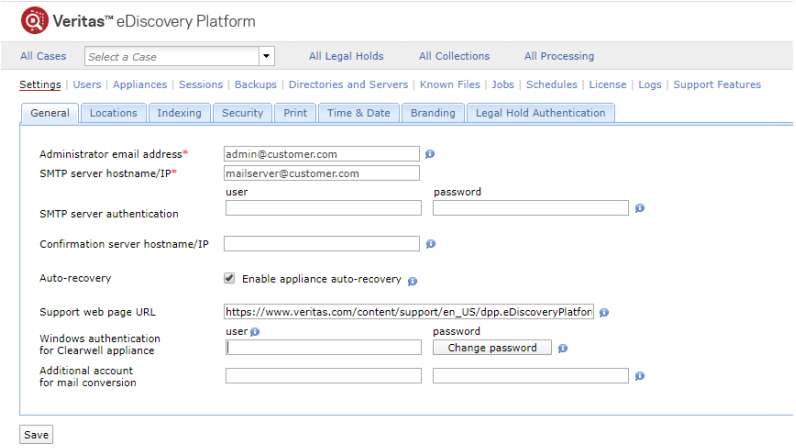
Note: Make sure that you follow the guidelines described in the Guidelines for Domain User Accounts section.

Verify System Settings

Log on to the Veritas eDiscovery Platform User Interface, then set up the appropriate customer information in the **System** > **Settings** > **General** tab.

Enter an "Administrator email address", "SMTP server hostname/IP" and the customer "Support web page URL" (which will appear as the Support link at the bottom of the screen). Add a new account for Windows authentication and/or MBOX/OST to PST file conversion.

IMPORTANT! This PST conversion account cannot overlap with any of the existing service account logon credentials and the account must be a member of the Local Administrator group with read and write permissions (or, at a minimum modify permissions) set to access the source data.

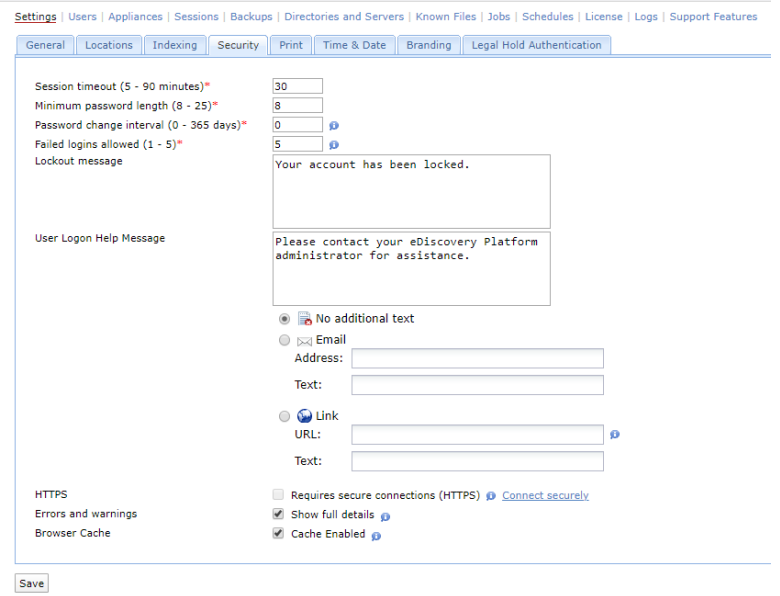


Verify Security Settings

If the system was configured for HTTPS redirection before the 10.2 installation, make sure it is enabled after the upgrade. You can verify the HTTPS redirection setting on the **System > Settings > Security** tab.

IMPORTANT! Check the "New user password policy" option. If selected after an upgrade, it will prompt all existing users to change their password. It is also critical to set up a meaningful "User Logon Help Message" text. This is the message that the end users will see on the Logon screen when they click **Need Help?**. The information should route users to the appropriate Veritas administrator, and *not* to contact Veritas Customer Support.

On the **System > Settings > Security** tab, enter your Lockout message and User Logon Help message. (Check that the **Requires secure connections (HTTPS)** option is enabled).



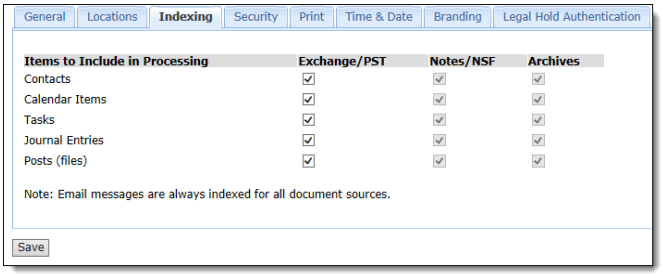
If you are using an SSL imported in your server.keystore, the upgrade should have copied the *server.keystore* file into the new installation directory. If you are still getting security warnings in your browser after the upgrade, you may need to verify the server.keystore was updated correctly.

- Verify that the `D:\CW\V102\config\templates\tomcat\server.keystore` is the correct keystore file you want to use on the server.
- Run Option 7 in the Clearwell Utility to "Build Incremental Configuration Changes". If using Clearwell Commander, use the **Action** > **Build Incremental Configuration Changes** option.

For more information, refer to the *System Administration Guide*.

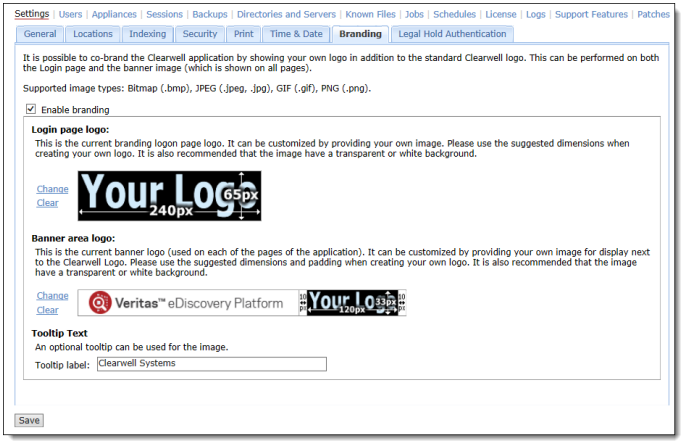
Verify Indexing Settings

On the **System > Settings > Indexing** tab, optionally setup a directory for customer specific NIST lists. Also, review if Contacts should be enabled by default. Customers may want to index contacts and then exclude them with filtering if not relevant. The Veritas eDiscovery Platform crawler services need to be restarted after making changes to these system-wide security settings. Please note that these case defaults can also be overridden.



Verify Custom Logo Settings

If the system was configured to use a custom logo before the 10.2 upgrade, then setup the custom branding after the upgrade on the **System > Settings > Branding** tab. Select **Enable branding**. The recommended logo dimensions are shown on the screen.



Note: Images must be created (or saved) using RGB color model. Attempting to upload an image in CMYK will cause the following error: "Unsupported File Type"

Verify Configuration Settings

From the **System > Support** screen, select the **Property Browser** support feature, make sure the primary appliance is selected in Step 2 and then select "Submit".

Review the properties that are returned. Make sure that the *esa.uploader.customerID* property is set to your customer name. Also verify that the location for case backups is setup to an appropriate location.

Verify Firewall Settings

In Windows, go to **Start** > **Control Panel** > **Windows Firewall** to verify and modify settings if needed. If nodes in a cluster are not communicating correctly, then you may want to disable the firewall on all nodes to verify communications. You can do this by going to **Start** > **Control Panel** > **Windows Firewall** > **Turn windows firewall on or off** > "**Turn off windows firewall (not recommended)**".

If you are having problems accessing Veritas eDiscovery Platform remotely, verify the Webserver JVM in the Programs and Services list on the Exceptions tab. If access problems persist, contact Veritas Customer Support for steps to disable, reconfigure and then re-enable the Firewall making sure it points to the appropriate Veritas eDiscovery Platform application paths.

Reconfigure LDAP authentication after upgrade

If your LDAP login fails after the upgrade is complete, perform the following steps to reconfigure the LDAP authentication. Be sure to also read the accompanying note regarding LDAP passwords and encryption:

1. Logon to your appliance as an administrator.
2. From the **System** > **Support Features** screen, select the **Property Browser** feature.
3. Select **System** from the **Select the case (or system)** list.
4. Enter the following property in the **Name of property to change** field.

   esa.ldap.connectionPassword
5. Enter your new values in the **New value (leave blank to remove)** field.
6. Select the **Confirm change. Are you sure?** check box.
7. Click **Submit**.

Note: If the LDAP password is configured to use encryption using the property ***esa.ldap.connectionPassword.enc***, clear the value for this property (***esa.ldap.connectionPassword.enc***) by executing steps 1 through o 7 specifying property ***esa.ldap.connectionPassword.enc*** in step 4 and removing the "New value" field in step 5 by leaving it blank.

A confirmation message about successful removal of the System Property ***esa.ldap.connectionPassword.enc*** appears. The LDAP logins should now work. The system does not need a restart.

Reconfigure Full Node Scheduled Backup Tasks

If there are scheduled task in place to perform routine full node backups, verify that they are updated to point to the new *D:\CW\V10* directory. Go to **Start > Settings > Control Panel > Scheduled Tasks** or **Start > Settings > Control Panel > Administrative Tools > Task Scheduler** and review the list of tasks to see if there are any updates needed.

Update Virus Scanning Software (if applicable)

Be sure to update your virus scanning exclusion rules after the install to account for any changes in folders and directory structure. For more information see "Virus Scanning Guidelines", in the *Veritas e Discovery Platform System Administration Guide*.

EXCLUDE the following directories:

Image Helper

For the Image Helper to work properly, allow access to port 41734.

```
D:\Clearwell Packages\Muhimbi Document Converter
```

PrizmDoc Service

```
D:\Prizm\Server
D:\Prizm\PAS
```

JDK Software

```
C:\ jdk-8u342-windows-x32
C:\ jdk-8u342-windows-x64
```

MySQL Database Software

```
D:\mysql
D:\MySQLData (Clearwell v7.1.4+)
D:\mysqltemp
D:\CW\<current_version>
```

Note: `D:\CW\<current_version>` contains a subfolder that needs to be scanned:
`D:\CW\<current_version>\scratch\temp\esadb\attCacheDir\`

Because you can only exclude directories from a virus scan, move the attachments directory (attCacheDir) to a different location and then update the path. For more information see, the *System Administration Guide*.

Platform Installation

```
D:\CWShared
```

Rights Management

This directory only exists if you use the Rights Management feature

```
C:\Users\<username>\AppData\Local\Microsoft\DRM
```

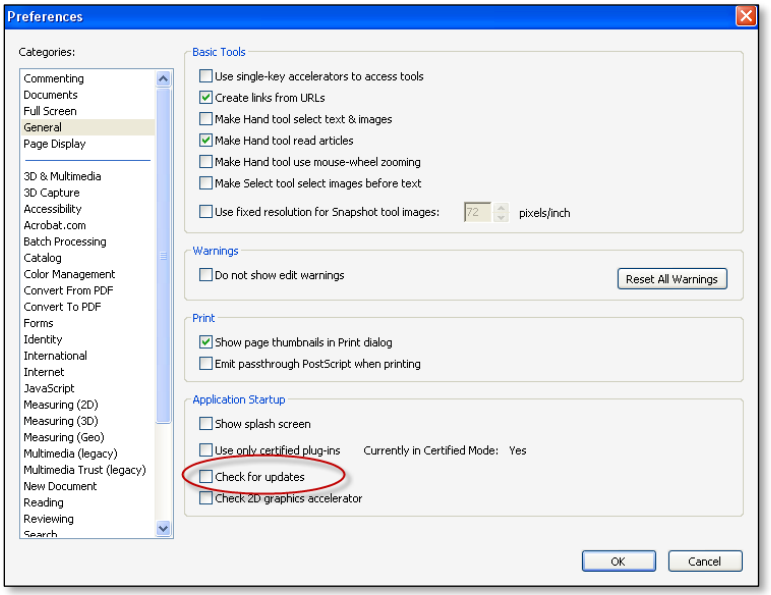
Antivirus Exclusions for Audio Search

By default, the Audio Search software is installed into the following directories and subdirectories. To avoid interference with critical media operations, be sure to disable virus and malware scanning software. In particular, Malwarebytes Anti-Malware, Kaspersky Endpoint Security, and Microsoft Security Essentials are known to interfere with media operations. See (Optional) Setting Up Your System for Audio Processing for directory details.

```
C:\Program Files(86)\Nexidia
C:\Program Files(86)\Nexidia\Language Packs
C:\Program Files\Nexidia\Search Grid 2.0
D:\Nexidia
C:\Users\<username>\AppData\Local\Temp
```

Disable Adobe Automatic Updates

Disable Adobe Reader automatic updates as follows. Launch Adobe Reader Select **Edit > Preferences > General** and make sure that the "Check for updates" option in the Application startup section is not selected.



Verify Clearwell Utility

Open the Clearwell Utility (icon on the desktop) and verify the "Current working directory" points to the current Veritas eDiscovery Platform installation directory (for example: *D:\CW\V95*).

As a final verification, upload all logs for Veritas eDiscovery Platform validation. Go to **System > Logs**, enter a Name, and then select Submit leaving the default settings.

Clear Browser Cache

Your browser's cache stores certain information about the previous version of Veritas eDiscovery Platform. Several significant changes were made to the user interface from pre-10.2 versions to 10.2. To have the application display the new pages properly, you need to clear the browser cache for your browser.

Configure Browser Cache Security

Browsers maintain a page repository (cache) that is used to speed up retrieving previously viewed pages without sending another request to the server. If a user logs out of the eDiscovery application, it is possible to press the **Back** button to view the previous page of the authenticated user. This view remains visible for just a few seconds before reverting to the login page.

A configuration setting has been added to the Security configuration which can enable or disable browser cache. If disabled, the browser cache (for example, search results) will not be stored and access or retention of sensitive information is prevented during logout. To take advantage of the browser cache security, you must uncheck the cache enabled setting. The default setting is enabled.

IMPORTANT! Once the cache is disabled, the browser will require a page refresh (F5) when the **Back** button is used to revisit certain pages (for example, navigating back through search result pages).

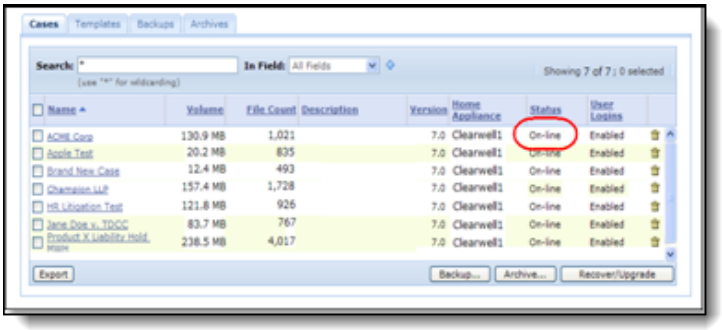
For those concerned about the accidental release of information possibly contained in the browser cache during the logout process, you can disable it by unchecking the checkbox for **Cache Enabled**.

1. In the **System** view, click **Settings** > **Security**.
2. Uncheck the **Cache Enabled** checkbox (checked by default).
3. Click **Save**.

Verify Veritas eDiscovery Platform Cases

Go to the **All Processing > Processing > Cases** tab and verify that all the cases that were previously online are still online for access. If there were any upgrade issues with a particular case, it will be listed as unavailable.

Note: Cases from prior versions that do not have any case data will show up in All Cases as not fully upgraded, and require you to click on a link to finish upgrading.



Associating Legal Holds and Collections with 10.2-Upgraded Cases

If you have cases containing Legal Holds and/or Identification and Collection tasks (contained in a collection), these can be associated with a case once upgraded to 10.2. Additionally, the Dashboard (overall view of all cases on the system), Case Home Dashboards (overall view of a specific case), and Data Analytics will reflect the changes brought by the association of the Collections and/or Legal Holds.

For more information on Legal Hold or Collection, see the *Veritas eDiscovery Platform Legal Hold User Guide* and the *Veritas eDiscovery Platform Identification and Collection Guide*.

Update checksum for emails

Deduplication of documents depends on matching checksums. Microsoft Office and IBM Notes client have altered the way in which they calculate checksums. The result is that from version to version some email documents may not be deduplicated.

Changes in Office and Notes versions from 10.0 to 10.2

- Pre-10.1, Veritas eDiscovery Platform used Outlook 2013 for extracting e-mails from PSTs and MSGs, and Lotus Notes version 8.5 for extracting e-mails from NSFs. Veritas eDiscovery Platform 10.1 requires Outlook 2019 on Windows Server 2019 platform, Outlook 2013 on other platforms, and IBM Notes 10.0.1 on all platforms.
- Pre-10.2, Veritas eDiscovery Platform used Outlook 2013 for extracting e-mails from PSTs and MSGs on Windows Server 2016 and Windows Server 2012. Veritas eDiscovery Platform 10.2 requires Outlook 2016 on Windows Server 2016 platform.

IMPORTANT! After upgrading to 10.2, the System Manager should check to see if there is data needing the checksum update. Go to **System** > **Support Features** and choose **Update checksum for emails**. Only the cases that appear in the **Select the case** field are affected. The Case Administrator should coordinate the timing of running the "Update Checksum for Emails" feature against the affected cases.

For instructions on how to enable and use this feature, as well as feature background, case qualification criteria, workflow details, and FAQs, see https://www.veritas.com/content/support/en_US/article.100051881.

Warning Message if a Case is Eligible for Running Checksum Update Job

Veritas eDiscovery Platform 10.1 upgrades the IBM Notes version from 8.5 to 10.0.1. Due to this, post upgrade to release 10.1, customers will have to run update checksum in following conditions:

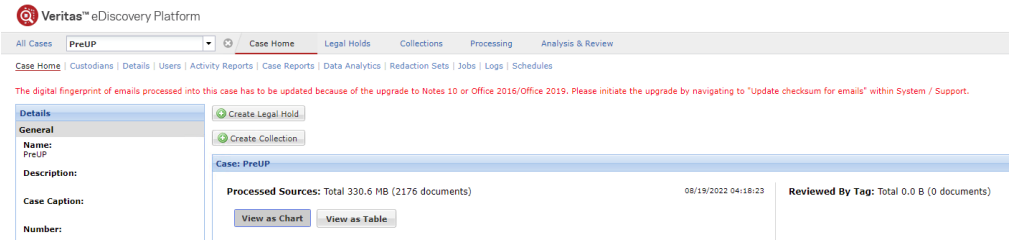
- On Windows Server 2019, if either NSF or MSG/PST data is processed earlier.
- On Windows Server 2012 and 2016, if NSF data is processed earlier.

Veritas eDiscovery Platform 10.2 upgrades the Microsoft Office version from 2013 to 2016 on Windows Server 2016. Due to this, post upgrade to 10.2 on Windows server 2016, customers will have to run update checksum in following conditions:

- On Windows Server 2016, if NSF or MSG/PST data is processed in eDP 10.0 or earlier.
- On Windows Server 2016, if MSG/PST data is processed in eDP 10.1

A warning message is shown on all case-related UI pages (except Legal Holds and Collections) if the case is eligible for checksum update job: "*The digital fingerprint of emails processed into this case has to be updated because*

of the upgrade to Notes 10 or Office 2016/Office 2019. Please initiate the upgrade by navigating to 'Update checksum for emails' within System / Support."



OST to PST Conversion Libraries

The upgrade process automatically removes older conversion libraries (such as Datanumen) and replaces them with new OST conversion libraries. This means that if OST conversion was in use prior to the upgrade, the conversion service will continue to function but will use the newly installed library. For more details, see Case Administration Guide.