Veritas eDiscovery Platform™

Installation Guide

10.1

VERITAS

Veritas eDiscovery Platform™: Installation 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: 2021-12-06

Legal Notice

Copyright © 2021 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 9

Installation Prerequisites 10
Machine Configuration 10
Hardware Compatibility 10
Operating System 15
Disk Space 15
Software Requirements 16
Guidelines for Domain User Accounts 17

Chapter 3 Installing eDiscovery Platform 23

Chapter 4 Optional: Setting Up Your System for Audio Processing 35

Setting Up Your System: Server-Side 35

Chapter 5 Post-Installation Steps 39

Post-Installation Checklist 39
Validate Install 40
Activate Microsoft Office Professional Plus 2013 SP1 (for Windows Server 2012 R2 and 2016) 40
Activate Microsoft Office Professional Plus 2019 (for Windows Server 2019) 42
Validate if Outlook is enabled to connect to Microsoft 365 using MAPI/HTTP 43
Apply the Latest V100 Patch (If Applicable) 44
Verify the Veritas eDiscovery Platform License 44
Verify Veritas eDiscovery Platform Services 44
Verify System Settings 45
Verify Security Settings 45
Verify Indexing Settings 46

Configure Custom Logo 47
Verify Configuration Settings 47
Verify Firewall Settings 47
Configure Full Node Scheduled Backup Tasks 48
Update Virus Scanning Software Exclusions (if applicable) 48
Disable Adobe Automatic Updates 50
Configure Browser Cache Security 50

Chapter 1

Preface

About this guide

This document provides detailed step-by-step installation and configuration instructions for successfully installing and setting up the Veritas eDiscovery Platform application from scratch (not a product upgrade). It is sometimes referred to as a clean install.

This document assumes the reader is comfortable performing common system operations and is familiar with the Windows operating system.

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
Upgrade Guide	Describes prerequisites and upgrade information for the current customers with a previous version of Veritas eDiscovery Platform

Document	Comments
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
User Guide	Describes how to perform searches, analysis, and review, including detailed information and syntax examples for performing advanced searches

Document	Comments
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	Provides details about the Imaging Tool Upgrade feature and how to perform Imaging Tool Upgrade after the eDiscovery Platform appliance is upgraded to version 10.1, 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	
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 section and the following sections provide prerequisite steps and installation steps to install Veritas eDiscovery Platform. Make sure you have completed all the prerequisites before you start the installation.

After the installation section, additional steps are provided to:

- Configure the system for the optional audio search feature
- Activate Microsoft Office Professional Plus 2013 SP1 on Windows Server 2012 R2, or Windows Server 2016
- Activate Microsoft Office Professional Plus 2019 on Windows Server 2019

Note: The installation steps for eDiscovery Platform 10.1 using Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 are similar. However, you might observe some differences in the appearance and color scheme. This guide uses screenshots from a Windows Server 2016 server.

Installation Prerequisites

The Veritas eDiscovery Platform appliance must meet the following minimum requirements.

Machine Configuration

Confirm supported hardware configuration:

- Veritas eDiscovery Platform 8300 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 replaces 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*				
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*	32-Core CPU x 192 GB RAM	1.5 TB (1500 IOPs)	Y

Appliance Type	Environment	Appliance Function	CPUs RAM	Disk	VM*
		database, administers the Distributed Architecture cluster and hosts Legal Holds and Collections			
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 cluster and hosts*	32-Core CPU x 128 GB RAM	1.5 TB (1500 IOPs)	Y

Appliance Type	Environment	Appliance Function	CPUs RAM	Disk	VM*
		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.

- Windows Server 2012 R2 (Standard or Data Center edition)

  Note: eDiscovery Platform installer will install the Ink and Handwriting Services feature for Windows Server 2012 R2 in case it is not installed.

At the beginning of the installation, if an unsupported operating system is detected, a warning message displays. The install cannot continue until this issue is resolved.

Disk Space

Veritas recommends disabling Windows Memory dump option, to maximize space on the C: drive before continuing the installation. If this feature is not disabled, a pop-up window displays with the following text:

"Windows memory dump is enabled. This could potentially consume a large amount of space on the C: drive. It is recommended to disable this feature."

Follow the steps for the Windows Server 2012 R2 operating system:

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

Software Requirements

Details for the following software requirements can be found in the Installation steps. The following software components are required and are installed if they do not exist on the system. If these components are installed, then they require reboots before the installation proceeds.

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

IMPORTANT! For Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, you must not select other features including HTTP and Non-HTTP Activation.

Guidelines for Domain User Accounts

Before you start installing Veritas eDiscovery Platform software, you should gather, create or 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*, *EsaNsfCrawlerService*, *EsaNsfRetrieverService*, and *EsaPstCrawlerService* *EsaClassifierService* • The security settings must match the EsaApplicationService: FireDaemon "Log On As" credentials.
EsaPstCrawlerService	appadmin	
EsaPstRetrieverService	pstretriever	
EsaNsfCrawlerService	appadmin	
EsaNsfRetrieverService	appadmin	
EsaExchangeCrawlerService	appadmin	
EsaExchangeRetrieverService	appadmin	
EsaEvCrawlerService	appadmin	
EsaEvRetrieverService	appadmin	
EsaPrizmDocServer EsaPrizmApplicationServices	EsaPrizmDocAdmin	• The eDiscovery Platform installer creates the **EsaPrizmDocAdmin** local user with admin privileges for PrizmDoc services.
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

Service	Username (example)	Rules for Account Credentials
		drive letter) to read and write to the Veritas eDiscovery Platform appliance. For example, \\<appliance-IPadddress>\d$\<dir>\<dir>\... • The account must have local administrative rights on the appliance.
EsaClassifierService	appadmin	• Use the same account credentials used for *EsaApplicationService* **Note**: The Classifier service account is required to use the automatic classification of information feature. The Classifier service allows the eDiscovery Platform to access the information classifier policies using the interface accessed by Veritas products. For details, see the *User Guide 10.1*.

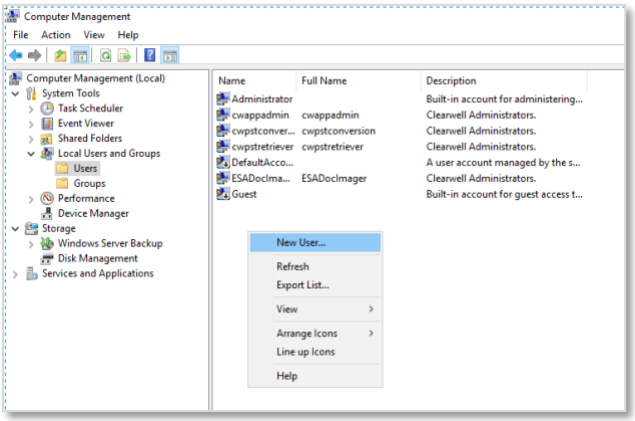
IMPORTANT! You must log on to the appliance using the same account configured as the "Log On As" account. Once logged on, ensure that the IBM Notes client was initialized correctly. If at any time you modify the "Log On As" accounts for these services, be sure the Lotus Notes client is initialized for that particular account.

An error or warning message is generated if service accounts are not members of the Local Admin group, or do not have the "Log on as Service" rights. If the rules defined above are not followed, an error message is displayed and you must change the credentials prior to proceeding.

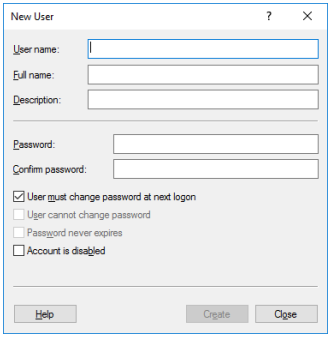
Adding domain user account to the Local Admin Group on Appliance

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**.

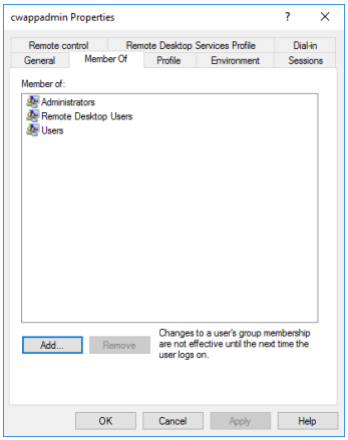


4. Click **New User**.



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.

Install Prerequisite Checklist

After verifying the information in the previous sections, proceed and confirm the items on the following checklist prior to the install.

Step	Task
1	Disable virus scanning.
2	Install all Windows Updates.
3	Verify that Internet Information Server (IIS) is not installed, or starts on a port other than port 80.
4	Verify that *User Account Control (UAC)* is disabled. **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options** > **User Account Control: Run all administrators in Admin Approval Mode** > select **Disabled**.
5	Verify you have the local administrator password for the services listed in the *Guidelines for Domain User Accounts* section. **Note**: This account is your Local Administrator account that belongs to a Local Windows Administrator group on the Veritas eDiscovery Platform Server. For more information on Service Accounts, see Guidelines for Domain User Accounts.
6	Verify that service accounts have been added to the Local Administrator group. If any additional accounts are being used as service accounts, they must be added to the local admin group. For more information on Service Accounts, see see Guidelines for Domain User Accounts.
7	Log in to the Administrator account and enter account password. Set up the following security settings and user rights assignments for the Administrator account: 1. Act as part of the operating system 2. Log on as a Service 3. Allow log on locally You can assign these settings and rights by going to: **Control Panel > System and Security** > **Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment**.

8	Ensure the Print Spooler & Windows Management Instrumentation (WMI) services are running and the Interactive Services Detection service is disabled.
9	Verify that the time zone and time/date settings on the server are accurate.
10	Verify you have a valid Microsoft Office Professional Plus 2013 SP1 (or 2019) license key. **Note**: You can get this from the Sales Purchase Order or your Solutions Consultant.
11	Determine the correct version of Veritas Enterprise Vault API Runtime required for collecting from Enterprise Vault sources in your environment. For more information on determining the correct version of Veritas Enterprise Vault, see the *Veritas eDiscovery Platform, Identification and Collection Guide*.
12	Sign in and use the MyVeritas portal for downloading product software. Information and the replacement options are located here: www.veritas.com/docs/100040083
13	Keep your Veritas eDiscovery Platform license and Audio Search license (if applicable) information ready for post-installation activation.

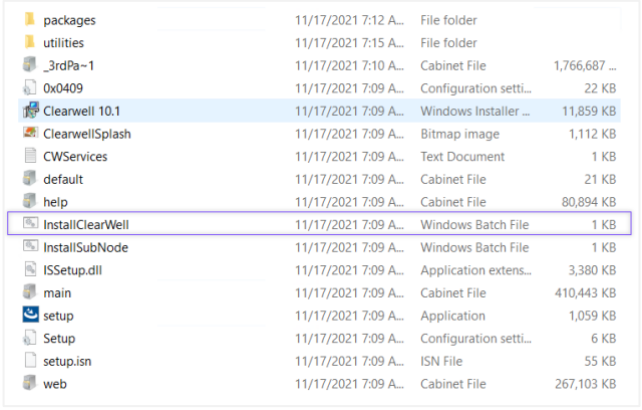
Chapter 3

Installing eDiscovery Platform

To perform a clean install of the platform and it's required software on the operating system, ensure that a prior version of the platform is not present. Or, if you are installing the platform for the first time ensure that the operating system does not have any old configurations or preferences set.

1. Log in to the machine as the Administrator. Unzip the installer into a temporary directory (D:\tmpInst directory). After the files are unzipped, double-click on the ***InstallClearwell.bat*** file (as shown).

   IMPORTANT! Be sure to run the .bat file (not the setup.exe), or the installation will fail. This is because a clean or fresh install relies on a number of important environment variables that are set by running ***InstallClearwell.bat***.



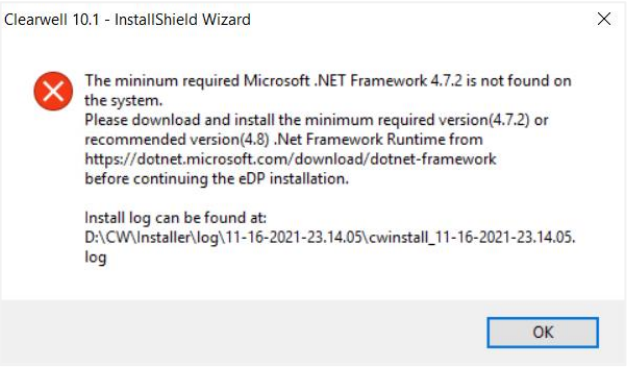
   The Open File dialog appears.

2. Click **Run**.

3. If Microsoft .NET Framework 4.7.2 is not installed, then you will be required to install them before installation can proceed. It is recommended to install Microsoft .NET Framework 4.8 Runtime. At the prompt to begin installation, click **Install**.

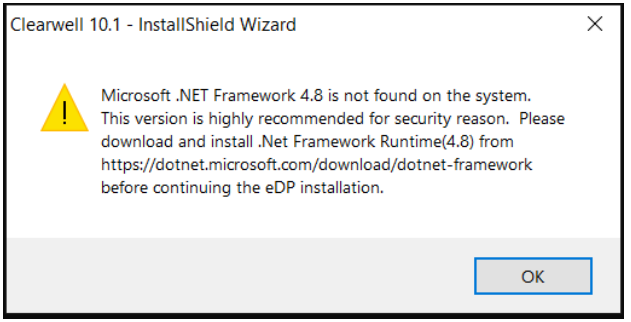
   You must reboot after installation of Microsoft .NET components.

4. A warning is issued if .NET 4.7.2 is not installed on the system. It is recommended to install .NET 4.8.0 version for security reasons. Click **OK**.

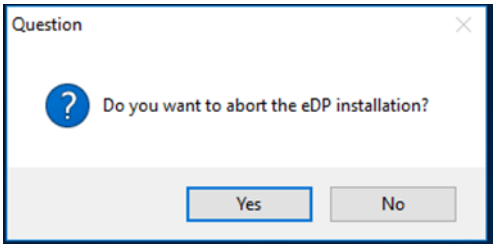


5. A warning is issued if .NET 4.8.0 is not installed on the system.

   It is recommended to install this version for security reasons. Click **OK**.



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



7. After installing Microsoft .NET and rebooting the system (may need more than one reboot), proceed with re-launching the installer ***InstallClearwell.bat***.

   The Clearwell screen appears displaying the version being installed. Click **Next**.

8. Read and acknowledge acceptance of the terms of the Veritas software license agreement. Click **Next**.

9. A warning will appear if the installer detects that the appliance doesn't meet the minimum requirements, or there are Windows features that should be disabled in order to maximize space on the C: drive:

   a. Ensure you have enough (or free up) space on the C: drive before continuing the installation. Click Yes.

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

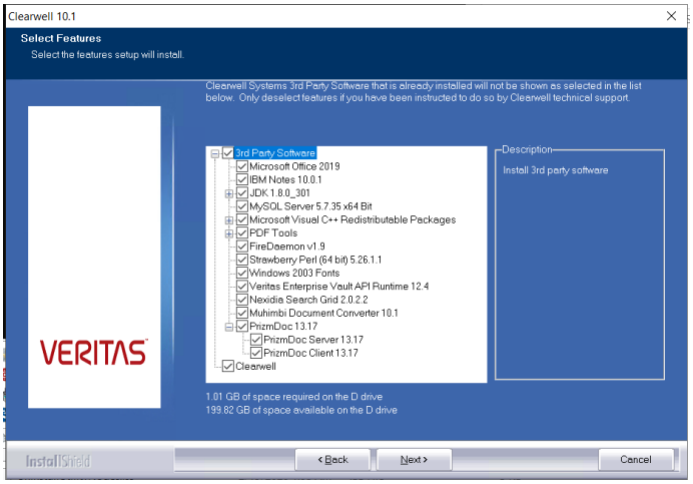
   See Disable Windows memory dump for instructions. Click **Yes** to continue.

10. On the Choose Destination Location screen, leave the default 10.1 installation directory as is, and click **Next**.

11. For Setup type, leave the default selection, **Complete**, and click **Next**.

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 10.1. Click **Next**.



Note: Third party components are not configurable. Components may be installed on the C: or D: drive.

A warning is issued if any of the following services are not running:

- Windows Management Instrumentation (WMI)
- Print Spooler service

The install will continue after issuing these service warnings. When the installation is finished, ensure these services are running (start by locating the service in the list of services and confirm that the status is **Started**. If it is not, select the service and on the **Action** menu, click **Start**).

A check is done to see if your setup meets the prerequisites. A warning screen is displayed with any issues that need addressing.

Veritas Enterprise Vault API Runtime 12.4 is installed with eDiscovery Platform 10.1.

Important! If your environment requires Veritas Enterprise Vault API Runtime 11.x, or 12.x , then do the following:

a. Select the custom install option

b. Deselect the Veritas Enterprise Vault API Runtime 12.4 selection

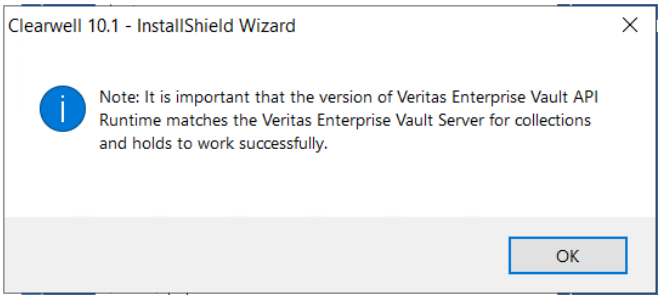
c. Allow the Veritas eDiscovery Platform install to complete

d. Install the required EV client runtime libraries to match the version of your Enterprise Vault server.

e. Click **OK** to continue the installation.

A pre-requisite warning about free space requirement and Windows updates is issued. Click **Yes** to continue the installation.

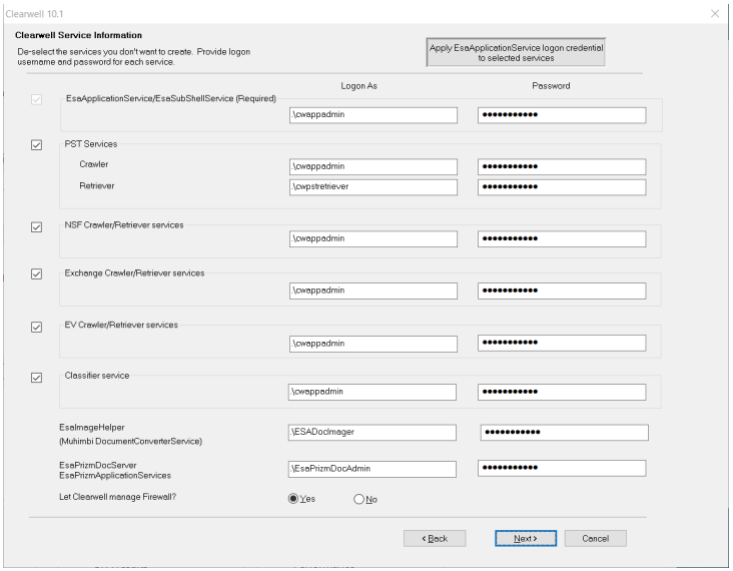
A warning about Veritas Enterprise Vault API Runtime version appears. Click **OK**.



A warning is issued about Windows Error Reporting. Click **Yes** to disable Windows Error Reporting and proceed with the installation.

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

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

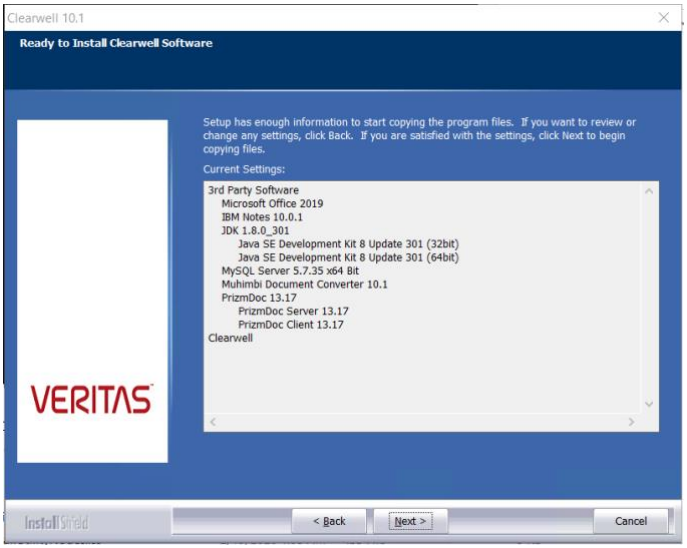


Note: Credentials can be changed on the Clearwell Service Information screen, if required. See Guidelines for Domain User Accounts.

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.

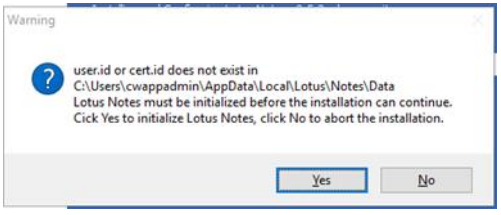
If correct "Log On As" service accounts are used, a message confirming the same appears. Click **OK** to continue the installation.

14. The Installer will check the disk space on C: drive, ensuring that it has at least 80 GB available, and that D: drive has at least 500 GB available after installation, with memory at least 32 GB.
15. The Ready to Install Clearwell Software screen displays the program files selected for installation. Click **Next**.

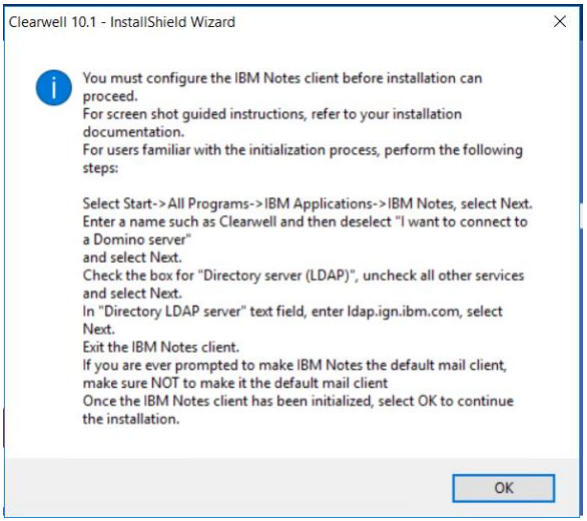


16. The installer will go through various steps – no intervention is required.

17. When the installer prompts for IBM Notes initialization, click **Yes** to initialize Lotus Notes.



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



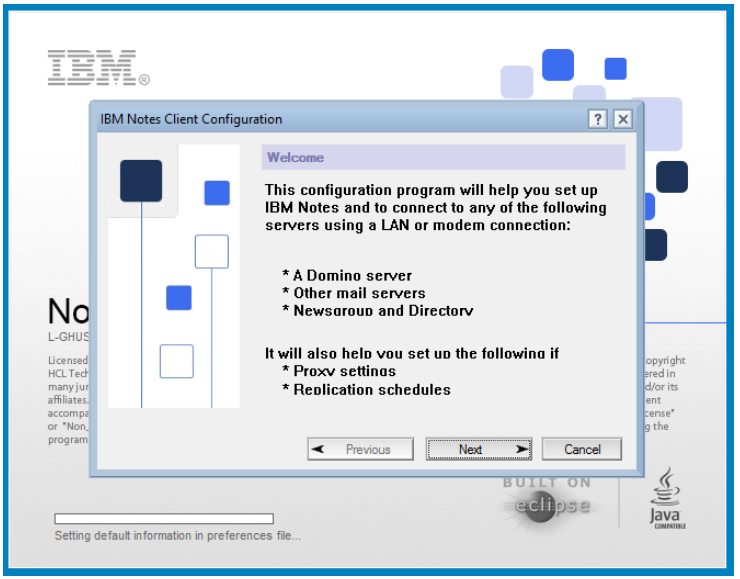
Click **OK** to continue. You must perform the next steps to manually initialize IBM Notes.

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.

---

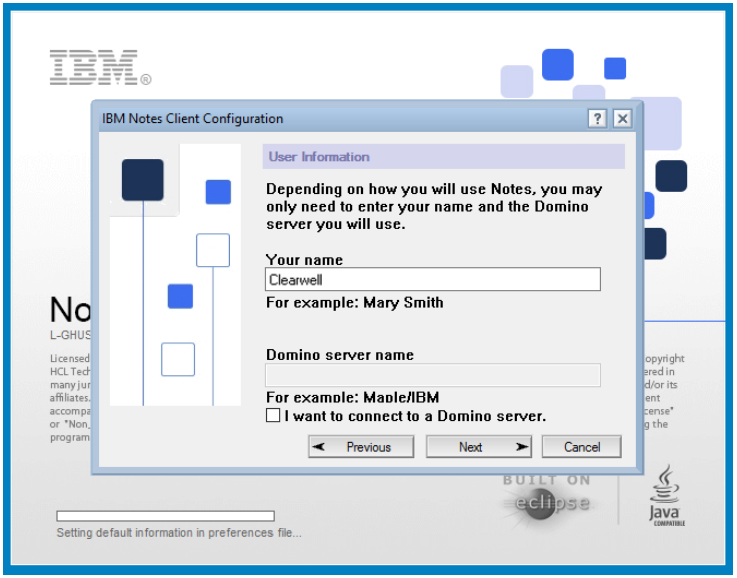
18. Use Remote Desktop to the server with a second connection in order to proceed with the initialization of IBM Notes. **Logon to the appliance with the account credential provided in the NSF Retriever or Crawler service (if not already done so).**

Go to **Start** > **(All) Programs** > **IBM Applications** > **IBM Notes 10.0.1** to launch the Notes client. Click **Next**.

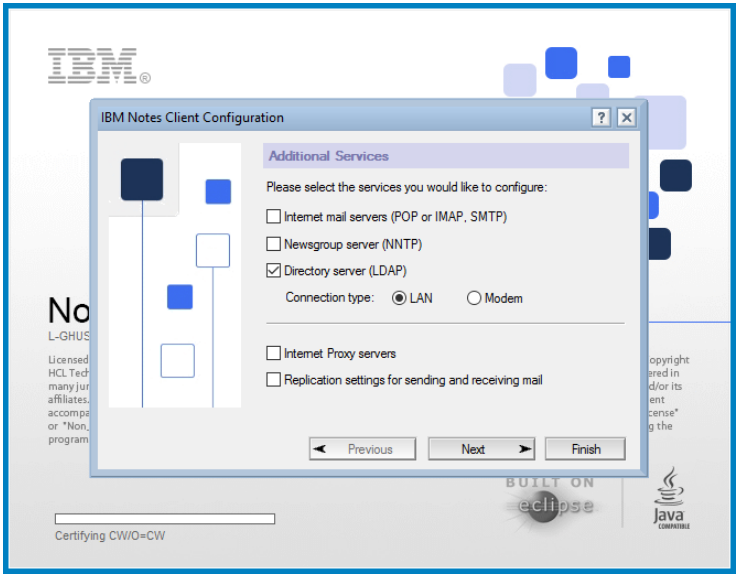


19. Enter "**Clearwell**" in the name field and clear (deselect) the option **I want to connect to a Domino server**. Click **Next**.

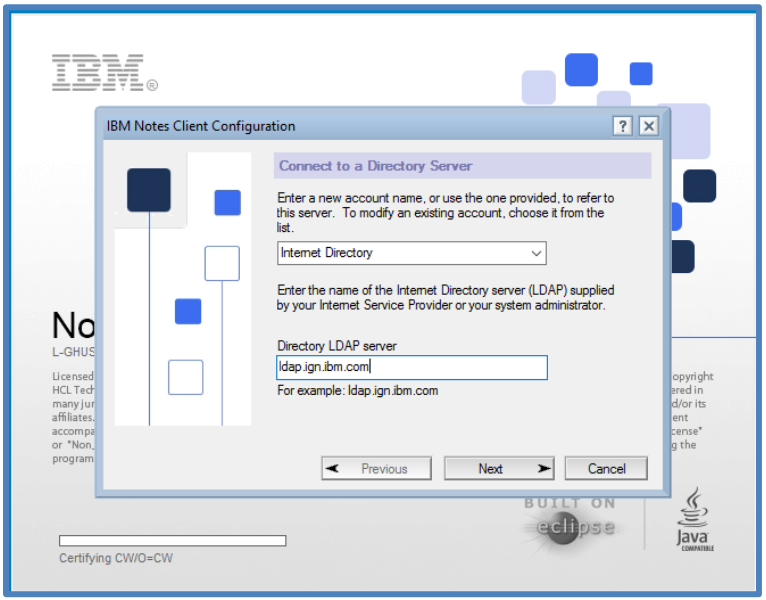
Note: If you are using a Domino server, then keep the option I want to connect to a Domino server selected and then enter the Domino settings on the following screens.



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



21. In the field for Directory LDAP server, type "**ldap.ign.ibm.com**".



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

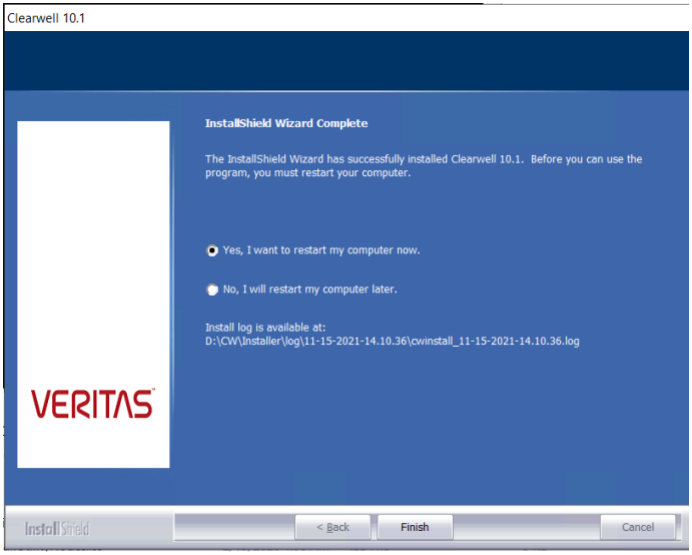
Note: You might receive a popup box stating: "IBM Notes is not currently set as your default email program. Would you like to set it now?" Make sure that IBM Notes is not set as the default mail client during the IBM Notes client installation. Microsoft Office Outlook should be the default mail client.

---

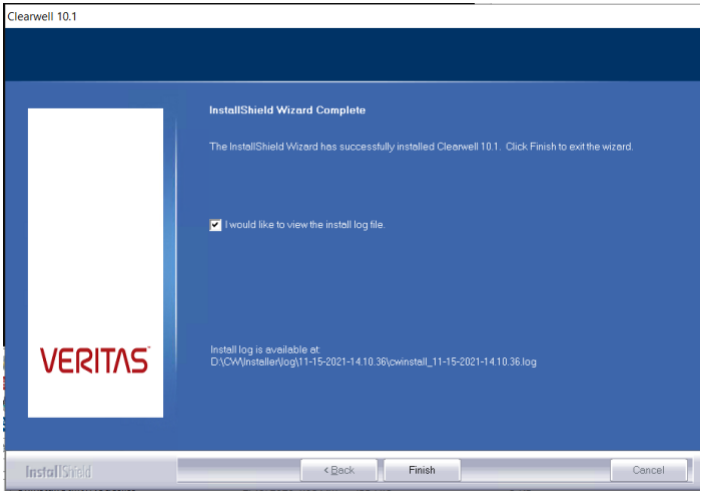
22. On the **Getting started** screen, close **IBM Notes** and select the option **In the future, exit without prompting**.

23. Go back to the Installer dialog and click **OK** to continue.

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.



Chapter 4

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 8.1.1 release or later. This section describes the prerequisites and the installation steps for installing the Audio Search tools.

After you complete the installation 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. See Audio License.
2. Exclude the Audio Search directories from antivirus scans. See Antivirus Exclusions.
3. Configure firewall software.
4. Firewall configuration and TCP Port Usage.
5. Start the start audio search services and then check if audio search services are running. See Audio Search Services.

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

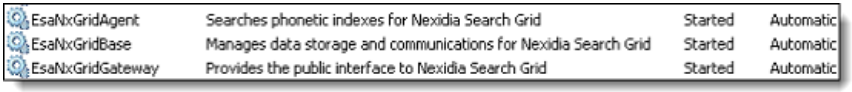
To stop and disable audio search services

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. For example, on Windows Server 2012 R2/2016, locate the Services control panel by selecting **Start** > **Control Panel** > **Administrative Tools** > **Services**.

Chapter 6

Post-Installation Steps

The following steps should be performed after the 10.1 appliance has been successfully installed.

Post-Installation Checklist

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

Step	Task
1	Validate install 1. Run **cwpostinstall** script using the icon located on the desktop 2. Resolve Microsoft Office Professional Plus 2013 SP1 (or 2019) license product key issues (if applicable) 3. Review install logs 4. Confirm correct Veritas eDiscovery Platform version (on all nodes if cluster environment)
2	Apply the latest v.10.1 patch (if applicable).
3	Verify the Veritas eDiscovery Platform license.
4	Verify Veritas eDiscovery Platform services started without errors.
5	After the Services in *services.msc* are created, enable the "Allow service to interact with desktop" option on the properties of the windows services.
6	Verify system settings.
7	Verify security settings.
8	Verify Indexing settings.

9	Configure custom logo.
10	Verify Veritas eDiscovery Platform configuration settings.
11	Verify firewall settings.
12	Configure full node scheduled backup tasks.
13	Update virus scanning software (if applicable).
14	Disable Adobe Reader Updates.
15	Configure Browser Cache Security

Validate Install

Run the ***cwpostinstall*** script using the icon on the desktop to set the customerID property, to indicate to technical support who is initiating a log upload.

Microsoft Office Professional Plus 2013 SP1 (or 2019) requires you to enter a valid license product key in order to activate the product. If you do not activate Office 2013 SP1 (or 2019) after you install it, the program cannot operate in a fully functional mode. For information on how to activate these Officeproducts, 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.

To verify that the correct version of Veritas eDiscovery Platform was installed, log on to the system and select **System** > **Appliances**.
Select the appliance and verify that it matches the Product Version 10.1.0.2.0.

Activate Microsoft Office Professional Plus 2013 SP1 (for Windows Server 2012 R2 and 2016)

After installing the Veritas eDiscovery Platform 10.1, you must activate Microsoft Office Professional Plus 2013 SP1.

Note: It is recommended to install latest patches of Microsoft Office Professional Plus 2013 SP1.

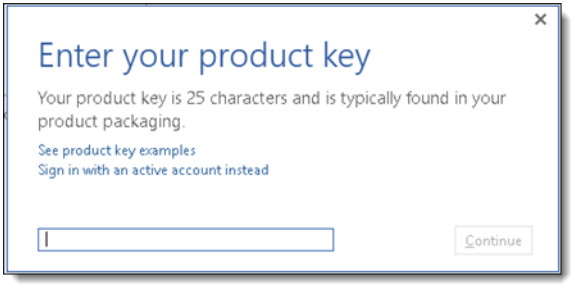
To activate Office 2013 SP1:

From **Start** > **All Programs** > **Microsoft Office 2013**, open Outlook 2013 or any other Microsoft Office application such as Word. The Microsoft Office Activation Wizard appears.

Alternatively, you can run the **cwpostinstall** script using the icon on the desktop and then follow the commands.

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 2013 is activated.
4. To confirm the activation, open a Word file and then go to **File** > **Help**. You will see the Office 2013 activation status.

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

After installing Veritas eDiscovery Platform 10.1, you must activate Microsoft Office Professional 2019.

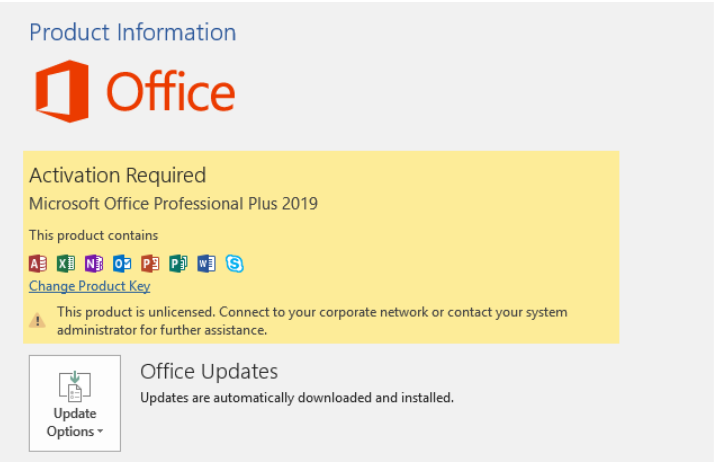
Note: It is recommended to install latest patches of Microsoft Office Professional Plus 2019

To activate Office 2019:

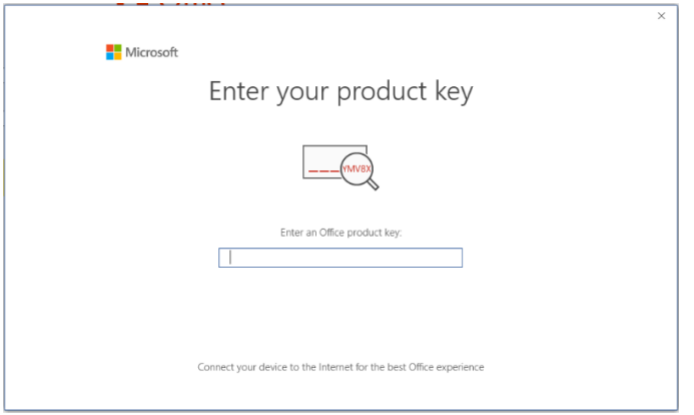
From **Start** > **All Programs** > **Microsoft Office 2019**, open Outlook 2019 or any other Microsoft Office application such as Word. The Microsoft Office Activation Wizard appears.

Alternatively, you can run the **cwpostinstall** script using the icon on the desktop and then follow the commands.

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..**



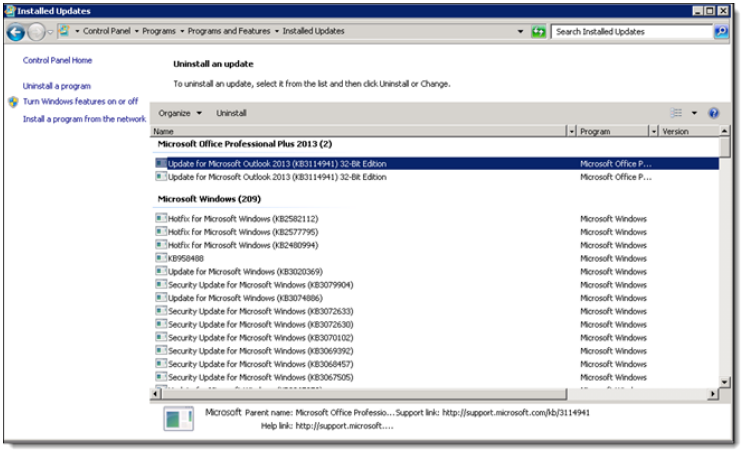
3. Your Office 2019 is activated.
5. To confirm the activation, open a Word file and then go to **File** > **Help**. You will see the Office 2019 activation status.
6. Update Microsoft Office Professional Plus 2019 to latest available version and Restart.

Validate if Outlook is enabled to connect to Microsoft 365 using MAPI/HTTP

Note: This section is applicable only for Windows Server 2012 R2 and Windows Server 2016.

Starting with 9.0, eDiscovery Platform now connects to Microsoft 365 using MAPI/HTTP protocol instead of RPC/HTTP. When you install or upgrade to 9.0 or later, the eDiscovery Platform installer installs the KB3114941 updates for Outlook 2013 32-Bit Edition that enables Microsoft 365 connection using MAPI/HTTP.

It is recommended to validate if the update (KB3114941) is installed before you start collection from Microsoft 365 mailboxes. To see the installed updates, go to **Control Panel** > **Programs and Features** > **View Installed Updates** > Search Installed Updates for KB3114941.



If you do not see the KB3114941 Outlook update installed, download it from https://www.microsoft.com/en-us/download/details.aspx?id=51720 and then manually install it.

Apply the Latest V100 Patch (If Applicable)

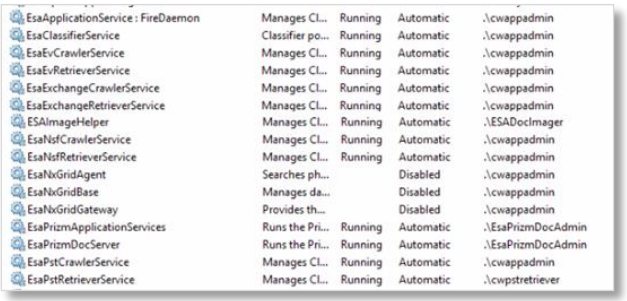
Apply the latest version 10.1 patch if applicable.

Verify the Veritas eDiscovery Platform License

Go to **System** > **License** to verify and, if needed, update your Veritas eDiscovery Platform license. 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.

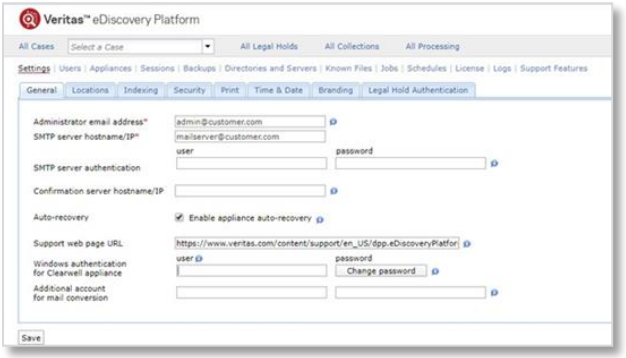


IMPORTANT! Make sure that you follow the guidelines described in the Guidelines for Domain User Accounts section.

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. Refer to the Administrator's QuickStart Guide for more information.

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.



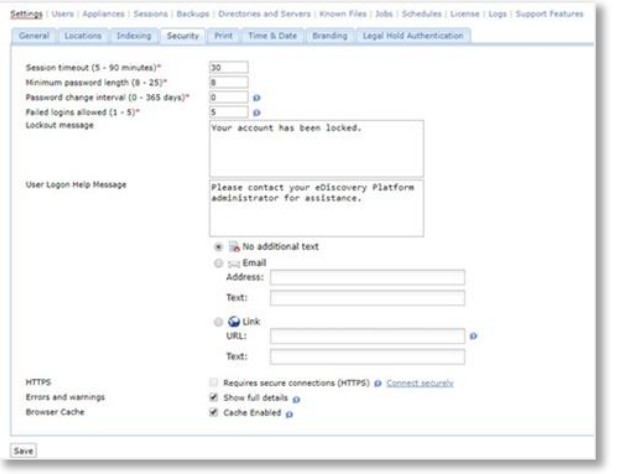
Verify Security Settings

If the system needs to be configured for HTTPS redirection you can enable it 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

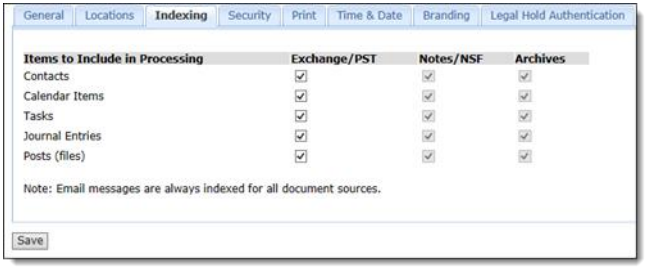
(HTTPS) option is enabled). For more information, refer to the *System Administration Guide*.



Verify Indexing Settings

Review if Contacts should be enabled by default. Contacts can be easily searched for in versions higher than Veritas eDiscovery Platform 5.0, for those who may want to index contacts and then exclude them with filtering if not relevant.

> **Note:** The Crawler services need to be restarted after making changes to these system-wide security settings. By default, Contacts is not enabled. If this is enabled, the Crawlers will need to be restarted.



Configure Custom Logo

If the system needs to be configured to use a custom logo, set up the custom branding after the install on the System > Settings > Branding tab. 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 Features** screen, select the "**Property Browser**" support feature, then select the primary appliance and click **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 set up to an appropriate location.

Refer to the *Veritas eDiscovery Platform System Administration Guide* for best practices on how to redirect backups to a location off the appliance.

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)".

Configure Full Node Scheduled Backup Tasks

As a best practice, configure a scheduled full node backup. For more information on how to perform backups, refer to the *Veritas eDiscovery Platform System Administration Guide*.

Update Virus Scanning Software Exclusions (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 eDiscovery Platform System Administration Guide*.

Make sure to 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-8u301-windows-x32

C:\ jdk-8u301-windows-x64

MySQL Database Software

D:\mysql

D:\MySQLData

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, Kasperky 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

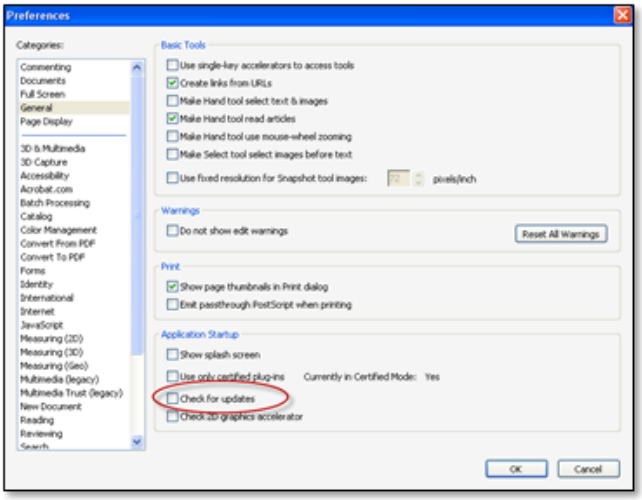
C:\Program Files\Nexidia\Search Grid 2.0

D:\Nexidia

C:\Users\<username>\AppData\Local\Temp

Disable Adobe Automatic Updates

If Adobe Reader is installed on your system, disable Adobe Reader automatic updates. To disable, launch Adobe Reader, then select **Edit** > **Preferences** > **General**. Ensure that the "Check for updates" option in the Application Startup section is not selected.



Configure Browser Cache Security

Browsers maintain a page repository (cache) that is used to expedite the process of 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**.

a. In the **System** view, click **Settings** > **Security**.
b. Clear the **Cache Enabled** checkbox (selected by default).
c. Click **Save**.