

Veritas eDiscovery Platform™

Installation Guide

9.5

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: 2020-05-18

Legal Notice

Copyright © 2020 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 Drive
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	Installing Veritas eDiscovery Platform	9
	Overview	9
	Installation Prerequisites	9
	Machine Configuration	9
	Operating System	10
	Disk Space.....	11
	Software Requirements	11
	Guidelines for Domain User Accounts	12
	Install Prerequisite Checklist	17
	Installing eDiscovery Platform.....	19
	Optional: Setting Up Your System for Audio Processing	31
	Setting Up Your System: Server-Side.....	31
	Post-Installation Steps	34
	Post-Installation Checklist	34
	Validate Install.....	35
	Activate Microsoft Office Professional Plus 2013 SP1	35
	Validate if Outlook is enabled to connect to Office® 365 using MAPI/HTTP ..	37
	Apply the Latest V9.5 Patch (If Applicable).....	38
	Verify the Veritas eDiscovery Platform License	38
	Verify Veritas eDiscovery Platform Services	38
	Verify System Settings	38
	Verify Security Settings	39
	Verify Configuration Settings.....	41
	Verify Firewall Settings	41
	Configure Full Node Scheduled Backup Tasks	42
	Update Virus Scanning Software Exclusions (if applicable)	42
	Disable Adobe Automatic Updates	44
	Configure Browser Cache Security	44

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.
- 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.
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.

Document	Comments
Native Viewer Installation Guide	Describes how to install and configure the Brava Client for native document rendering and redaction for use during analysis and review.
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 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's QuickStart Guide	A reviewer's reference to getting started using the <i>Analysis & Review</i> 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
Audio Search User Guide	Describes how to use the Audio Search feature to process, analyze, and search and export search media content

Document	Comments
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 Transparent Predictive Coding feature to train the system to predict results from control 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, groups, and roles
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 information: <https://www.veritas.com/product/a-to-z.html>

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/>

Installing Veritas eDiscovery Platform

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

Note: The installation steps for eDiscovery Platform 9.5 using Windows Server 2016 or Windows Server 2012 R2 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

- Supported number of CPU cores: 16, 24, 32, 48, 64

Note: Veritas recommends using a minimum of 16 CPU cores for better performance. The “Supported number of CPUs” refers to the number of cores detected by the Windows operating system and not the physical CPU count.

It is possible that a physical CPU not only has multiple cores but can also have hyperthreading enabled (which doubles the number of CPUs detected by the Windows operating system).

- Supported RAM: 32, 64, 128, 144 GB
 - **C: Drive** – 80 GB minimum with recommended 10 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 TB or more of free disk space.

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 processing components, therefore a D: drive of at least 1 TB is recommended.

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

Operating System

Installed and activated:

- Windows Server 2016 (Standard or Data Center edition)
- Windows Server 2012 R2 (Standard or Data Center edition)

Note: 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 Error Reporting and the Problem Reports and Solutions, as well as the Disable Windows Memory dump options, to maximize space on the C: drive before continuing the installation. If these two features are not disabled, a pop-up window displays with the following text:

1. Disable Windows Error Reporting and the Problem Reports and Solutions.

"Windows Error Reporting and the Problem Reports and Solutions" 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 > Action Center > Maintenance > Settings** > select the option " **I don't want to participate, and don't ask me again**" > click **OK**.

2. Disable Windows memory dump.

"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.

- Internet Explorer 11, Google Chrome, Microsoft Edge, Safari - Mac

Note: In version 9.0 or later, if Internet Explorer 10 users are unable to establish an https connection, make sure that the **Use TLS1.2** check box is enabled. Go to the Internet Explorer's **Tools** menu > select **Internet Options** > click the **Advanced** tab > select the "**Use TLS 1.2**" check box > click **OK**.
If the appliance is running Internet Explorer 10, verify that the **Use TLS1.2**

check box is enabled. Starting with eDiscovery Platform 9.5, Internet Explorer is supported as the browser to be used for Native Review Mode

- Microsoft .NET Framework 3.5 SP1 and .NET Framework 4.7.2 (required)
- Microsoft Framework .NET 4.8.0 (recommended)

IMPORTANT! For Windows Server 2012 R2 and Windows Server 2016, you must install Microsoft .NET Framework 3.5 SP1. Click **Start > Administrative Tools > Server Manager > Features > Add Features**, and then expand **.NET Framework 3.5 Features** and select **.NET Framework 3.5**.

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.

Veritas eDiscovery Platform uses Image Helper (also referred to as Muhimbi Document Converter) Service to convert Microsoft Office documents to PDF files before passing them to IGC.

Service	Username (example)	Rules for Account Credentials
EsaPstCrawlerService	appadmin	
EsaPstRetrieverService	pstretriever	
EsaNsfCrawlerService	appadmin	
EsaNsfRetrieverService	appadmin	
EsaExchangeCrawlerService	appadmin	
EsaExchangeRetrieverService	appadmin	
EsaEvCrawlerService	appadmin	
EsaEvRetrieverService	Appadmin	
IGCBravaLicenseService		<ul style="list-style-type: none"> ● Use the same Administrator account that is used to login to the appliance. <p>The reason for this requirement is that IGC only prompts for a password and does not prompt for an account username. IGC</p>
IGCJobProcessorService		

Service	Username (example)	Rules for Account Credentials
		<p>assumes that the account you are logged into is the one which will run the IGC services.</p> <p>Note: Make sure that these two services are configured to use the same account. If you need to change service accounts, do not use the Windows Service Control Manager to change IGC accounts.</p> <p>For instructions see the <i>IGC Administration Notes</i> PDF section "Changing the IGC Service Account". <i>IGC Administration Notes</i> is found in the <i>IGC Admin Utility</i> folder on the appliance where the eDiscovery application is installed.</p>
EsaImageHelper	ESADocImager	<ul style="list-style-type: none"> • Use a separate "Log On As" account for this service which must not be used for other services. • The Image Helper Service Account should be a Network Administrator user account with minimum appropriate rights to access appliances, hard disks, etc. and it should have the ability to execute typical administrative tasks such as service rights. • The account must have local administrative rights on the appliance.
EsaClassifierService	appadmin	<ul style="list-style-type: none"> • Use the same account credentials used for EsaApplicationService <p>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 9.5.</p>

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 Lotus Notes client was initialized correctly. If at any time you modify the "Log On As"

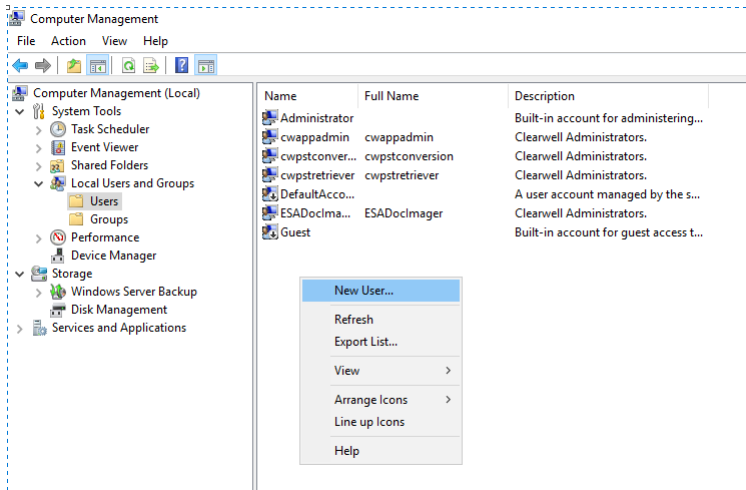
accounts for these services, be sure the Lotus Notes client is initialized for that particular account.

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 Administrators 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** (Windows Server 2012 and Windows Server 2016).
2. (Windows Server 2012) Under **System Tools**, click **Local Users and Groups**.
3. Click **Users**.



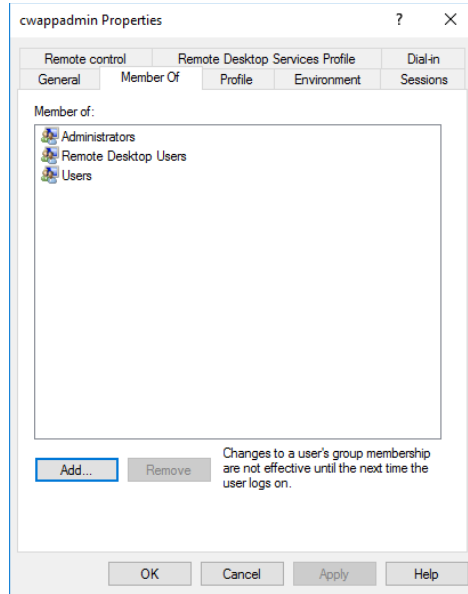
4. Under **Users**, click **More Actions**.
5. Click **New User**.

The image shows a 'New User' dialog box with the following fields and options:

- User name:** Text input field.
- Full name:** Text input field.
- Description:** Text input field.
- Password:** Text input field.
- Confirm password:** Text input field.
- User must change password at next logon**
- User cannot change password**
- Password never expires**
- Account is disabled**

Buttons at the bottom: **Help**, **Create**, and **Close**.

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



12. Click **Add**.
13. 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.
14. Click **OK**. The (Administrators) group will appear in the **Member of** list on the <user name> Properties dialog.
15. 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 <i>User Account Control (UAC)</i> 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 IGC install as well as other 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 Guidelines for Domain User Accounts.
7	Log in to the Administrator account (same for IGC installation) and enter account password. Set up the following security settings and user rights assignments for the Administrator account: <ol style="list-style-type: none"> 1. Act as part of the operating system 2. Log on as a Service 3. Allow log on locally <p>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.</p>

Step	Task
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 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 <i>Veritas eDiscovery Platform, Identification and Collection Guide</i> .
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.

Installing eDiscovery Platform

To perform a clean install of the platform and its 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. This must be the same user account that will be used for IGC services. Unzip the installer into a temporary directory (*D:\tmp\inst* 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**.

Name	Date modified	Type	Size
packages	2/7/2020 11:58 PM	File folder	
utilities	2/7/2020 9:12 AM	File folder	
_3rdPa~1	2/7/2020 9:11 AM	Cabinet File	1,336,752 KB
0x0409	2/7/2020 9:11 AM	Configuration sett...	22 KB
Clearwell 9.5	2/7/2020 9:11 AM	Windows Installer ...	11,079 KB
ClearwellSplash	2/7/2020 9:11 AM	Bitmap image	1,112 KB
CWServices	2/7/2020 9:11 AM	Text Document	1 KB
default	2/7/2020 9:11 AM	Cabinet File	21 KB
help	2/7/2020 9:11 AM	Cabinet File	69,990 KB
IGC	2/7/2020 9:11 AM	Cabinet File	22 KB
InstallClearWell	2/7/2020 9:11 AM	Windows Batch File	1 KB
InstallSubNode	2/7/2020 9:11 AM	Windows Batch File	1 KB
ISSetup.dll	2/7/2020 9:11 AM	Application extens...	2,710 KB
main	2/7/2020 9:11 AM	Cabinet File	393,722 KB
setup	2/7/2020 9:12 AM	Application	1,250 KB
Setup	2/7/2020 9:11 AM	Configuration sett...	6 KB
setup.isn	2/7/2020 9:12 AM	ISN File	55 KB
web	2/7/2020 9:12 AM	Cabinet File	223,700 KB

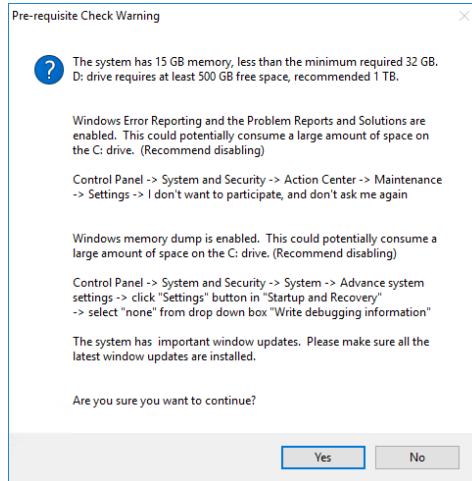
The Open File dialog appears.

2. Click **Run**.
3. If Microsoft .NET Framework 3.5 SP1, and .NET Framework 4.7.2 are not installed, then you will be required to install them before installation can proceed. At the prompt to begin installation, click **Install**.

You must reboot after installation of Microsoft .NET components.

4. 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**.

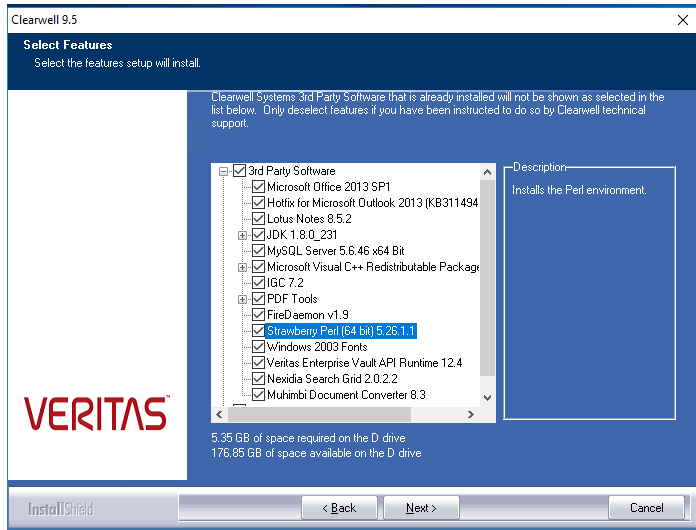
5. Read and acknowledge acceptance of the terms of the Veritas software license agreement. Click **Next**.
6. A warning will appear if the installer detects that the appliance doesn't meet the minimum requirements, or there are Windows features that should be disabled in order to maximize space on the 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 Error Reporting and Problem Reports and Solutions" feature to maximize space on the C: drive before continuing the installation.
See Disable Windows Error Reporting and the Problem Reports and Solutions for instructions.
 - c) 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.
7. On the Choose Destination Location screen, leave the default 9.5 installation directory as is, and click **Next**.
 8. For Setup type, leave the default selection, **Complete**, and click **Next**.

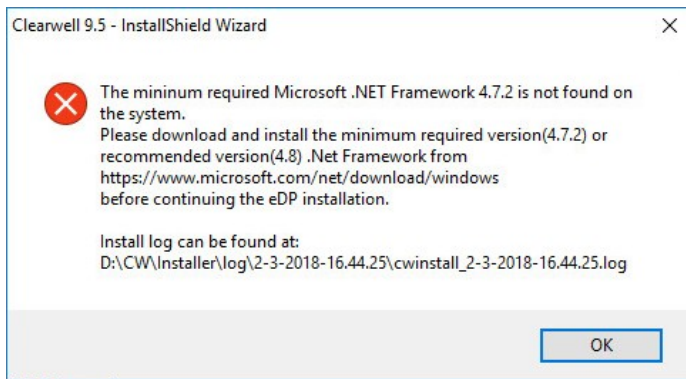
Select **"Custom"** only to view the individual software components that will be installed, but do not change any of the default selections which are required as part of the installation.

Selecting “Custom” displays the Select Features screen showing the third party components to be installed with 9.5. Click **Next**.



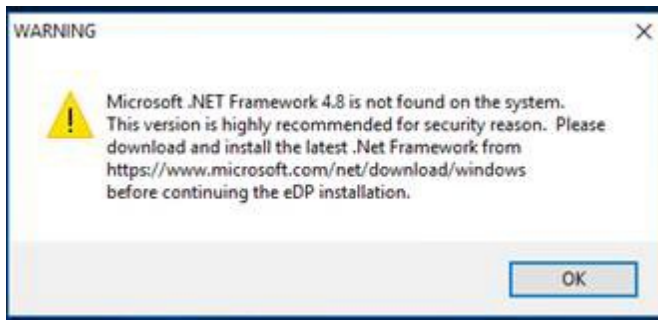
Note: Third party components are not configurable. Components may be installed on the C: or D: drive.

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**.

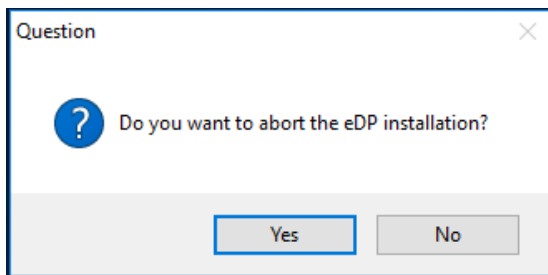


A warning is issued if .NET 4.8.0 is not installed on the system.

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



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



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 9.5.

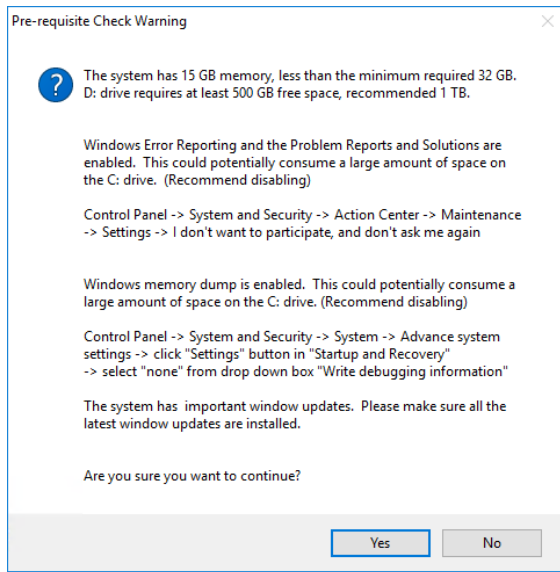
Important! If your environment requires Veritas Enterprise Vault API Runtime 11.x, or 12.x, then do the following:

- Select the custom install option
- Deselect the Veritas Enterprise Vault API Runtime 12.4 selection

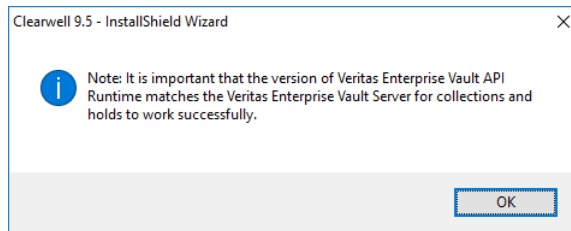
- Allow the Veritas eDiscovery Platform install to complete
- Install the required EV client runtime libraries to match the version of your Enterprise Vault server.

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**.



9. Choose a location for the IGC Installation and click **Next**.
IMPORTANT! You will need the password of an administrative account. The installation program will use the default IGC installation account to match the current logged on account. The two IGC services will be set up using this account as the "Log On As" Service account.
Do *not* select an account that will be removed from the "Logon As A Service" or "Logon Locally" rights when any domain policies take effect.
10. On the IGC User Credentials screen, enter the account password, and click **Next**.
11. Check that the time zone settings are correct, and click **OK**.

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

The screenshot shows the 'Clearwell 9.5' dialog box titled 'Clearwell Service Information'. It contains the following elements:

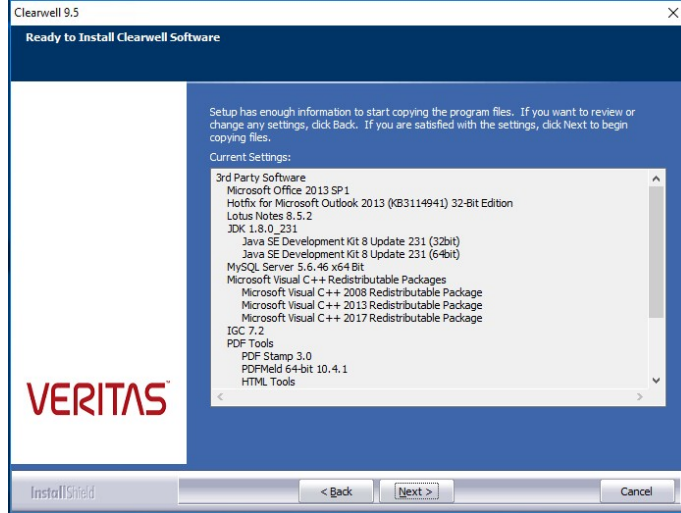
- Title Bar:** Clearwell 9.5
- Section Header:** Clearwell Service Information
- Instructions:** De-select the services you don't want to create. Provide logon username and password for each service.
- Buttons:** 'Apply EsaApplicationService logon credential to selected services' (top right), '< Back', 'Next >', and 'Cancel' (bottom).
- Service List:**
 - EsaApplicationService/EsaSubShellService (Required) - Logon As: \owappadmin, Password: [masked]
 - PST Services
 - Crawler - Logon As: \owappadmin, Password: [masked]
 - Retriever - Logon As: \owpstretreiver, Password: [masked]
 - NSF Crawler/Retriever services - Logon As: \owappadmin, Password: [masked]
 - Exchange Crawler/Retriever services - Logon As: \owappadmin, Password: [masked]
 - EV Crawler/Retriever services - Logon As: \owappadmin, Password: [masked]
 - Classifier service - Logon As: \owappadmin, Password: [masked]
 - EsaImageHelper (Muhimbi DocumentConverterService) - Logon As: \ESADocImager, Password: [masked]
- Firewall Option:** Let Clearwell manage Firewall? Yes No

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 overlaps with other service accounts or the IGC service account. 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.

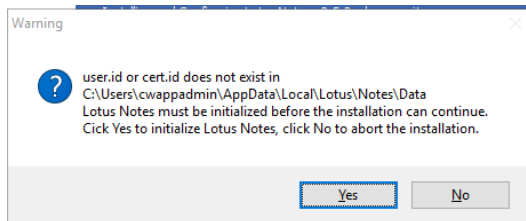
- The Installer will check the disk space on C: drive, ensuring that it has at least 10 GB available, and that D: drive has at least 30 GB available after installation, with memory at least 32 GB.
- The Ready to Install Clearwell Software screen displays the program files selected for installation. Click **Next**.



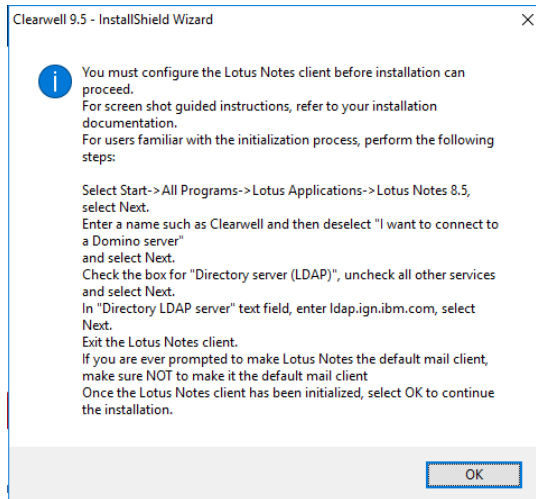
15. The installer will go through various steps – no intervention is required.

Note: IGC v7.2 installation takes a long time (approximately 10 to 15 minutes).

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



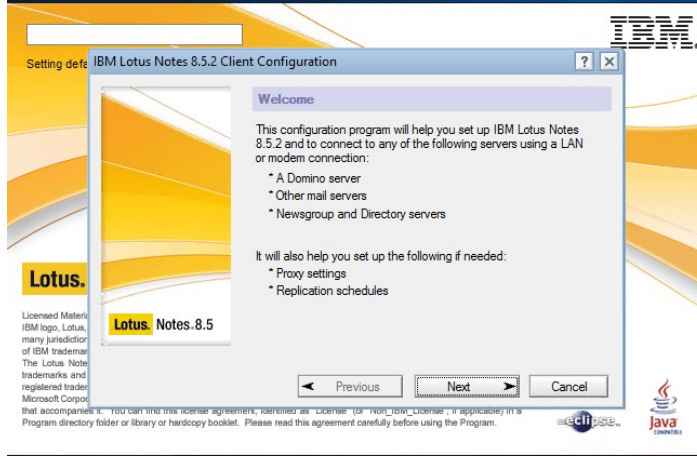
Initialization instructions and screenshots are documented in the next steps, but are also shown in the dialog message that displays.



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

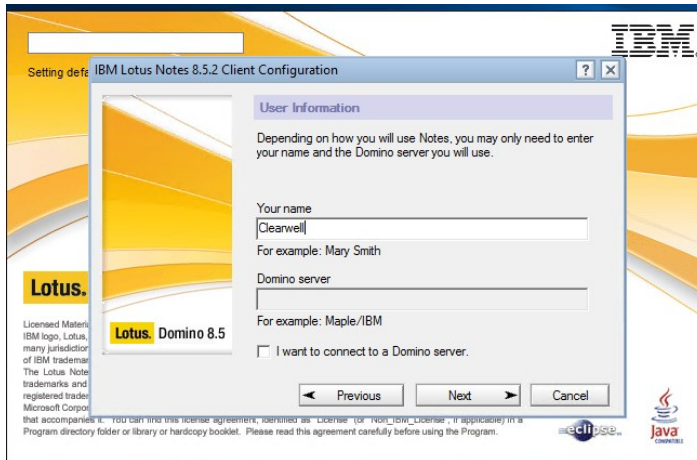
Note: Even if you do not have a Domino server, you must complete the Lotus Notes installation to complete the installation of Veritas eDiscovery Platform.

17. Use Remote Desktop to the server with a second connection in order to proceed with the initialization of Lotus 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 > Lotus Applications > Lotus Notes 8.5** to launch the Notes client. Click **Next**.

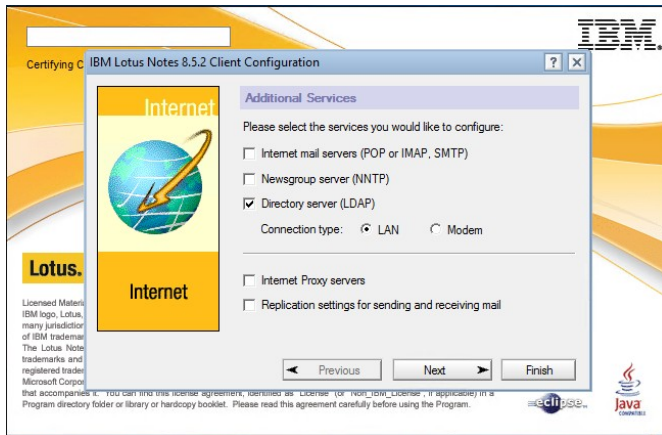


18. Enter "Clearwell" in the name field and clear (deselect) the option **I want to connect to a Domino server**. Click **Next**.

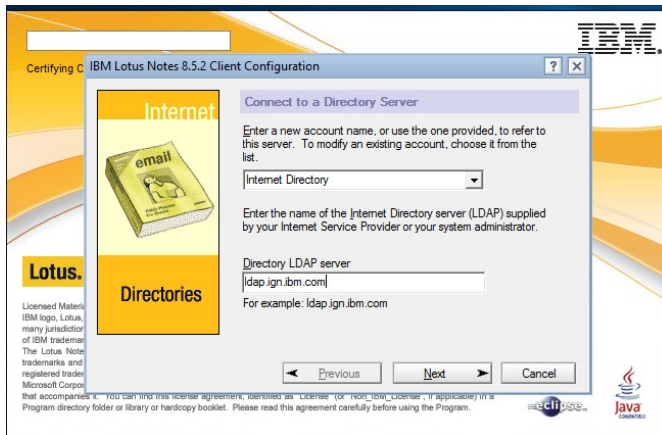
Note: If you are using a Domino server, then keep the option **I want to connect to a Domino server** selected and then enter the Domino settings on the following screens.



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



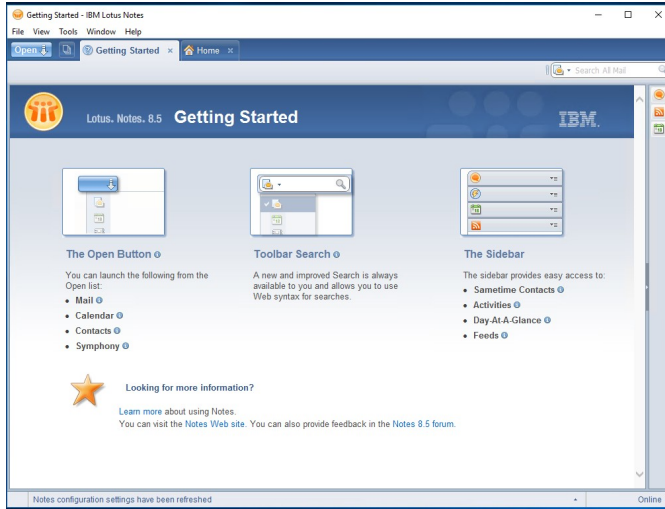
20. In the field for Directory LDAP server, type **"ldap.ign.ibm.com"**.



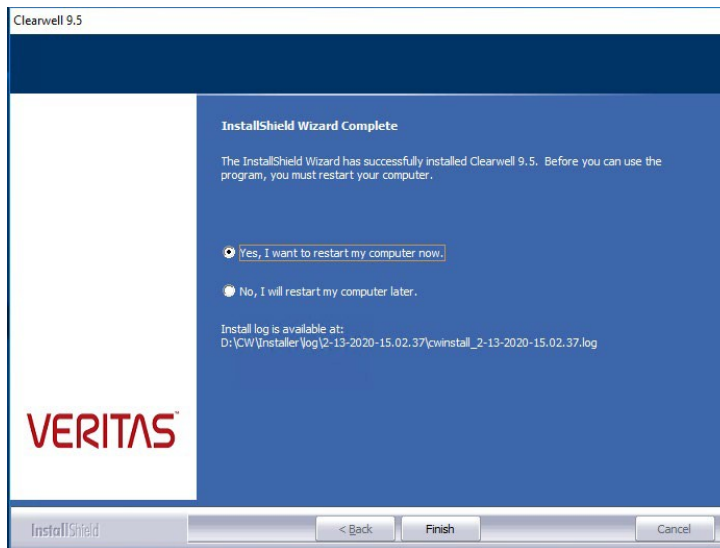
Click **Next** to complete Lotus Notes setup.

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

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



22. Go back to the InstallShield dialog and click **OK** to continue. The system continues the installation. After installation completes, select **Finish** to reboot the system.



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, Kasperky Endpoint Security, and Microsoft Security Essentials are known to interfere with media operations. Make sure to exclude these directories from antivirus scans:

Audio Search Directories

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 here:

Default TCP Ports

Component	Port #
esa.firewall.port.nexidiapublic.desc= Nexidia Search Grid Gateway Public Port esa.firewall.port.nexidiapublic.port=25002	25002
esa.firewall.port.nexidiamsgrkr.desc= Nexidia Search Grid Message Broker Port esa.firewall.port.nexidiamsgrkr.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.

EsaNxGridAgent	Searches phonetic indexes for Nexidia Search Grid	Started	Automatic
EsaNxGridBase	Manages data storage and communications for Nexidia Search Grid	Started	Automatic
EsaNxGridGateway	Provides the public interface to Nexidia Search Grid	Started	Automatic

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**.

Post-Installation Steps

The following steps should be performed *after* the 9.5 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 <ol style="list-style-type: none"> 1. Run cwpostinstall script using the icon located on the desktop 2. Resolve Microsoft Office Professional Plus 2013 SP1 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.9.5 patch (if applicable).
3	Verify the Veritas eDiscovery Platform license.
4	Verify Veritas eDiscovery Platform services started without errors.
5	After the Services in <i>services.msc</i> 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.

Step	Task
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 requires you to enter a valid license product key in order to activate the product. If you do not activate Office 2013 SP1 after you install it, the program cannot operate in a fully functional mode. For information on how to activate Office 2013, see [Activate Microsoft Office Professional Plus 2013 SP1](#).
- 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 9.5.0.0.0.

Activate Microsoft Office Professional Plus 2013 SP1

After installing the Veritas eDiscovery Platform 9.5, you must activate Microsoft Office Professional Plus 2013 SP1.

Note: You must obtain and install the Microsoft Office 2013 Service Pack 1 (SP1). For details, see <https://support.microsoft.com/en-us/help/2817430>.

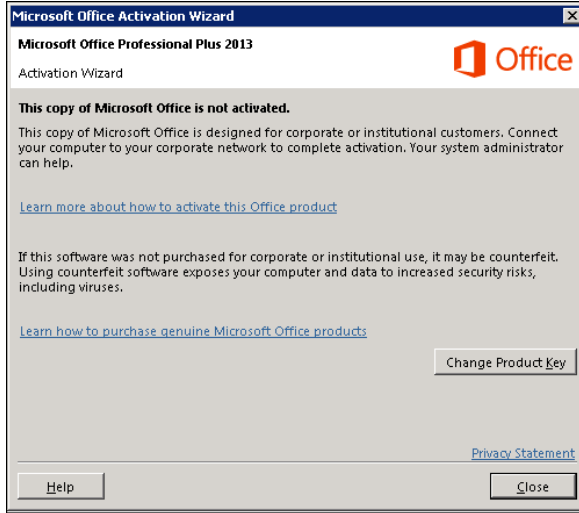
After installing Microsoft Office Professional Plus 2013 SP1, please install "Hotfix for Microsoft Outlook 2013 (KB3114941)", which is available at <https://support.microsoft.com/en-in/help/3114941/april-5-2016-update-for-outlook-2013-kb3114941>.

To activate Office 2013 SP1:

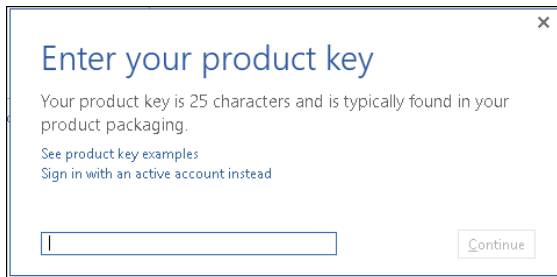
From **Start > All Programs > Microsoft Office 2013**, open Outlook 2013 or any other Microsoft Office application such as Word. The Microsoft Office Activation Wizard appears.

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..**

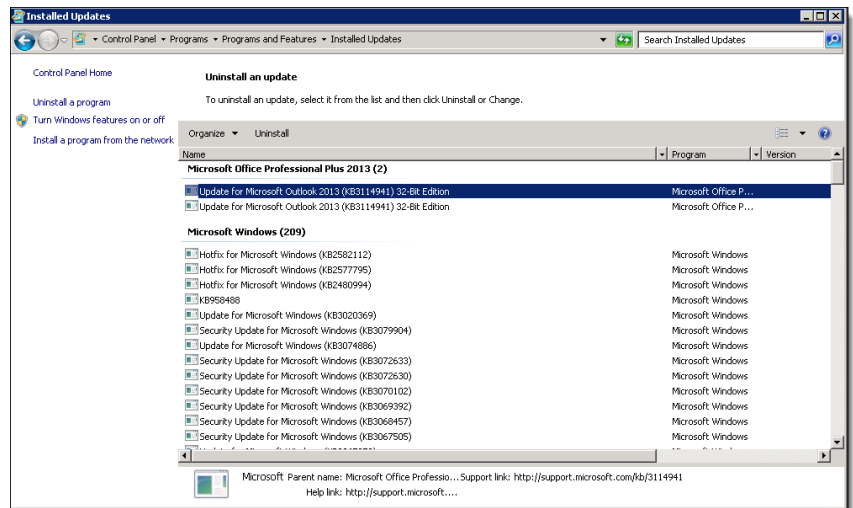


3. Your Office 2013 is activated.
4. To confirm the activation, open a Word file and then go to **File > Help**. You will see the Office 2013 activation status.

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

Starting with 9.0, eDiscovery Platform now connects to Office® 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 Office® 365 connection using MAPI/HTTP.

It is recommended to validate if the update (KB3114941) is installed before you start collection from Office® 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 V9.5 Patch (If Applicable)

Apply the latest version 9.5 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.

EsaClassifierService	Classifier portal daemon	Running	Automatic	\cswppadmin
EsaEvCrawlerService	Manages Clearwell EV Crawler Process	Running	Automatic	\cswppadmin
EsaEvRetrieverService	Manages Clearwell EV Retriever Process	Running	Automatic	\cswppadmin
EsaExchangeCrawlerService	Manages Clearwell Exchange Crawler Process	Running	Automatic	\cswppadmin
EsaExchangeRetrieverService	Manages Clearwell Exchange Retriever Process	Running	Automatic	\cswppadmin
EsaIGCBravaLicenseService	ClearwellIGCBravaLicenseService	Running	Automatic	\Administrator
EsaIGCJobProcessor	ClearwellIGCJobProcessor	Running	Automatic	\Administrator
EsaImageHelper	Manages Clearwell ImageHelper Process	Running	Automatic	\ESADocImager
EsaNsCrawlerService	Manages Clearwell NSF Crawler Process	Running	Automatic	\cswppadmin
EsaNsRetrieverService	Manages Clearwell NSF Retriever Process	Running	Automatic	\cswppadmin
EsaNsGridAgent	Searches phonetic indexes for Nexidia Search Grid	Disabled	Disabled	\cswppadmin
EsaNsGridBase	Manages data storage and communications for Nexidia Search Grid	Disabled	Disabled	\cswppadmin
EsaNsGridGateway	Provides the public interface to Nexidia Search Grid	Disabled	Disabled	\cswppadmin
EsaPstCrawlerService	Manages Clearwell PST Crawler Process	Running	Automatic	\cswppadmin
EsaPstRetrieverService	Manages Clearwell PST Retriever Process	Running	Automatic	\cswpstretreiver

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.

The screenshot shows the 'Security' tab of the Veritas eDiscovery Platform settings. The page includes a navigation bar with 'All Cases', 'Select a Case', 'All Legal Holds', 'All Collections', and 'All Processing'. Below this is a 'Settings' menu with options like 'Users', 'Appliances', 'Sessions', 'Backups', 'Directories and Servers', 'Known Files', 'Jobs', 'Schedules', 'License', 'Logs', and 'Support Features'. The 'Security' tab is active, showing fields for 'Administrator email address*' (admin@customer.com), 'SMTP server hostname/IP*' (mailserver@customer.com), 'SMTP server authentication' (user, password), 'Confirmation server hostname/IP', 'Auto-recovery' (checked 'Enable appliance auto-recovery'), 'Support web page URL' (https://www.veritas.com/content/support/en_US/dpp_eDiscoveryPlatform), 'Windows authentication for Clearwell appliance' (user, password, Change password), and 'Additional account for mail conversion'. A 'Save' button is at the bottom.

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.

The screenshot shows the login page for the Veritas eDiscovery Platform. It features the Veritas logo and the text 'Veritas™ eDiscovery Platform'. There are two input fields: 'Username' and 'Password'. A blue 'Sign in' button is positioned below the password field. At the bottom left, there is a 'Need Help?' link, and at the bottom right, the version number 'Version 9.5.0' is displayed. A copyright notice '© 2020 Veritas Technologies LLC.' is at the very bottom, followed by a warning: 'WARNING: Any unauthorized access to, or misuse of this system or data contained in it may result in civil and/or criminal prosecution, and employee discipline up to and including termination. System access and usage are monitored and audited.'

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*.

Settings | Users | Appliances | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | License | Logs | Support Features

General | Locations | Indexing | **Security** | Print | Time & Date | Branding | Legal Hold Authentication

Session timeout (5 - 90 minutes)*: 30
 Minimum password length (8 - 25)*: 8
 Password change interval (0 - 365 days)*: 0
 Failed logins allowed (1 - 5)*: 5
 Lockout message: Your account has been locked.
 User Logon Help Message: Please contact your eDiscovery Platform administrator for assistance.
 No additional text
 Email
 Address:
 Text:
 Link
 URL:
 Text:
 HTTPS
 Errors and warnings
 Browser Cache
 Requires secure connections (HTTPS) [Connect securely](#)
 Show full details
 Cache Enabled
 Save

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.

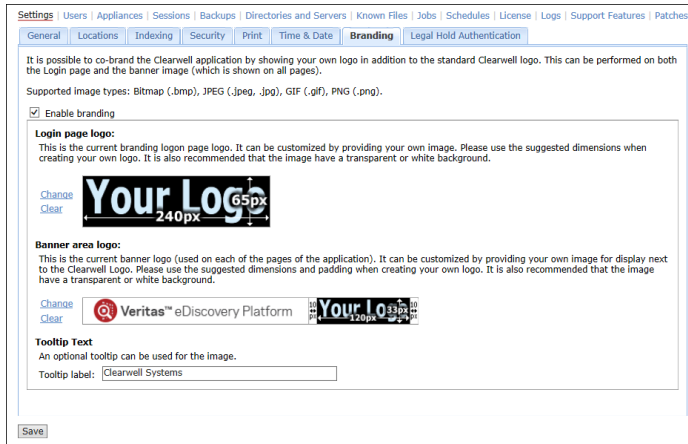
General | Locations | **Indexing** | Security | Print | Time & Date | Branding | Legal Hold Authentication

Items to Include in Processing	Exchange/PST	Notes/NSF	Archives
Contacts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Calendar Items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tasks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Journal Entries	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Posts (files)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Note: Email messages are always indexed for all document sources.
 Save

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 master 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

JDK Software

C:\jdk-8u231-windows-x32

C:\jdk-8u231-windows-x64

MySQL Database Software

D:\mysql

D:\MySQLData (Clearwell v7.1.4+)

D:\mysqltemp

D:\CW\

Note: D:\CW\

D:\CW\

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\\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
```

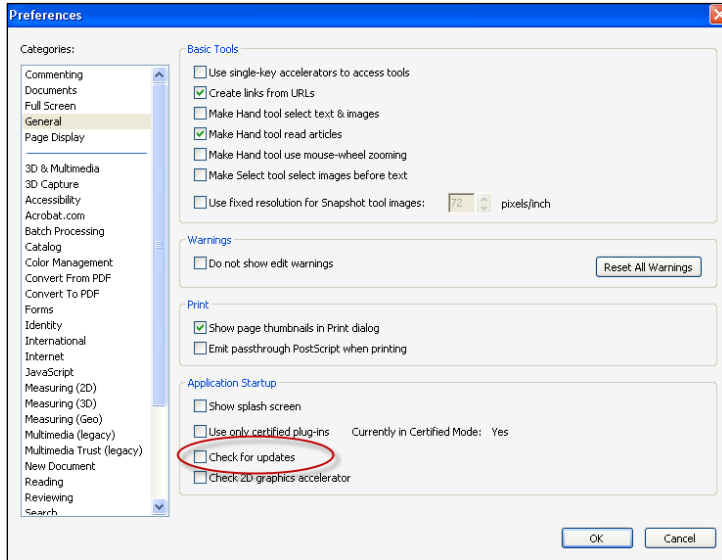
```
C:\Program Files\Nexidia\Search Grid 2.0
```

```
D:\Nexidia
```

```
C:\Users\\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, including Internet Explorer, 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**.

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