Veritas eDiscovery Platform™

System Administration Guide

10.0.1

VERITAS™

Veritas eDiscovery Platform™: System Administration 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: 2021-7-2.

Legal Notice

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

System Administration Guide

The System Administration Guide provides an administrator's view of the eDiscovery Platform, and describes how to perform basic and advanced system setup, account management, support, backup and restore, and troubleshooting tasks associated with managing and maintaining the appliance.

This section contains the following sections:

About This Guide

This guide is intended for, but not limited to, system administrators who are responsible for the configuration, installation and maintenance of the Veritas eDiscovery Platform. For information about the administration tasks regarding setting up cases, see *"Case Administration Guide"*.

Revision History

The following table lists the information that has been revised or added since the initial release of this document. The table also lists the revision date for these changes.

Revision Date	**New Information**
July 2021	• Updated the *Configuring Privacy Info items for Bulk Redaction* section. • Added the Managing FIPS mode for classification section • Update version: jdk 8u291 • Added information on how to enable encrypted connection with MySQL
May 2021	• Updated the *Configuring Privacy Info items for Bulk Redaction* section.
March 2021	• Added information related to case status report • Added information related to SAML-based authentication • Added information related to configuring minimum password length • Update version: jdk 8u251 • Added information related to BCFKS type keystores and truststores • Added information on generating activity reports for all cases
October 2018	• Update version: jdk 8u231 • Added information related to JDK and TOMCAT password management. • Minor edits
March 2018	• Added information related to IPv6 support • Added information related to case archives
December 2017	• Added “redaction” and “bulk redaction and deletion” to event history reports • Removed obsolete “prompt for reason code” right from Document Access Rights • Removed Telemetry opt-in/out instructions • Reference to Legal Hold User guide for Integrated Windows Authentication Sign-On for Legal Hold • Added classifier service account • Added DA-Setup-related note to virus scanning guidelines for modifying the attachments directory path • Updated version of jdk to 8u144

Revision Date	**New Information**
June 2017	• Browser version deprecation (IE9) • Clearwell Commander password changes • Certificates procedures updated in Appendix A • Enable browser cache • Index Repair added • Legal Hold Authentication setting instructions in LH guide • LDAP instructions update • Update version: jdk 8u121 • Update checksum for email added • Windows updates mentioned in security • Corrected to state requirement of TLSv1.2 protocol • Added port clarification to esa.ldap.connectionURL
October 2016	• Deleted FTP upload account information • Updated new LDAP setup method
July 2016	• CW Commander passwords management • CW Commander certificate generation changes • Changes to user management for access groups • Changes to support for OST conversion • Update JDK version: jdk-8u74 • Minor edits and rebranding
March 2016	• branding and minor edits
August 2015	• Secure Authorization features: access groups, locations • Corrected System Stats, LDAP Utility and Property Browser input • Delete Utility Node Resource Management Property Mode: CONVERSIONS • DTQS support feature renamed to Imaging Tools Management • No longer support IE8. Add IE11support • Remove “prompt for reason code” under redaction privileges for users • Update JDK version: jdk-8u45 • Updated AV exclusions with D:\MySQLData • Remove Rights Management Guide
March 2015	• Image accessibility • Updated list of eDiscovery services • Changes to “Setting Up A Virtual Appliance” • Added details for exposing tokenizer through property browser • Updated “Virus Scanning Guidelines” • Updated CW Commander image • Updated “SSL Configuration Details” with supported TLS version and provider generated certificate details if using TLSv1.2 • Updated Secure LDAP SSL/TLS Support root certificate details with JDK • Updated LDAP property configuration reference example for role search

Revision Date	**New Information**
October 2014	• Added user group management setting • Updated screenshots • Added jdk and Image Helper directory antivirus exclusions • Remove support feature setting for Slip Sheet reports • Corrected SSL certificate install syntax • Minor edits and branding
December 2013	• Clarified “allow support access” added functionality • Added update to In-product Notification, Clearwell Commander Utility, Using the Support Features • Added information on how to change MySQL credentials (including root) • Added new permission to allow playing of audio media files (requires Audio Search module) • Added audio search directories to be excluded from antivirus scanning. • Clarified recommendation: VMware vSphere ESXi 5.0 or later • Minor edits
June 2013	• Added Updates and Patches Management • Added more details about user roles: Case Admin rights, Legal Hold Access and Legal Hold Management • Updated DA screens showing appliance roles, provisioning, role assignment • Added additional details to System settings/items to include in processing • Changes to virus scanning procedures documented • Additional details: adding appliance to a cluster • Added Employee Attribute Mapping • Updated Using the Support Features • Added opt-in/opt-out for data telemetry • Added extracted files behavior during archive/restore • Added description of how system indicates backup migration is complete • Updated Scheduled Appliance Backups • Added Web Services Case Creation API appendix • Minor corrections throughout
Sept 2012	• Integrated Windows Authentication (IWA) and header-based authentication configuration
June 2012	• User Accounts section now has Document Access Rights for Transparent Predictive Coding.
May 2012	• Appendix: Web Access Interface Options; updated step 3 on page 120, in instructions for installing a certificate.

Revision Date	New Information
March 2012	• Branding • This guide incorporates content from the following (formerly stand-alone) documents: – *LDAP Active Directory Configuration Reference* – *Virus Scanning Guidelines* – *Web Access Interface Options (Appendix)* • Added *Discovering Archive Sources* content (also in the *Case Administration Guide*)
Feb 2012	• New Update License wizard in System > License
Nov 2011	• New top menu navigation, case selection, and System administration workflow • Integrated Dashboard for single view of status and activity for all cases and single cases • Additional options to control reviewer access to item notes and tag history comments • Distributed architecture mode using RDMS for distributed review.
May 2011	• Exception warning messages administration • Support Feature updates
Feb 2011	• Additional security and administrative options, including: – allow OCR processing (after initial case processing) • Relocate cache (on or off) the appliance • Export job enhancements • (Minor revisions, updates, and graphics enhancements throughout)
Dec 2010	• Updated Technical Support Contact Information • (Minor revisions and graphics enhancements throughout)

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 Clearwell 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:

eDiscovery.InfoDev@veritas.com

You can also see documentation information or ask a question on the Veritas community site.

https://vox.veritas.com/

Managing User Accounts

This section describes managing user accounts.

Defining a Local or Enterprise User Account

If your appliance is configured for LDAP Authentication (rather than the Veritas default authentication), you have the option of designating users as *Local* or *Enterprise*, depending on how each should be authenticated. This determines whether the eDiscovery Platform should authenticate users against the username and password stored in the eDiscovery Platform or an enterprise authentication solution. Three enterprise-level solutions are available: LDAP, Integrated Windows Authentication (IWA), and header-based authentication.

Local versus Enterprise Users

A *local* user will always be authenticated against the username and password stored for that user in the eDiscovery Platform database, regardless of whether the platform is configured for enterprise authentication. An *enterprise* user however, will be authenticated against one of the enterprise authentication mechanisms, after enterprise authentication is enabled. If not enabled, the enterprise user will be authenticated in the platform against their username and password in the same manner as a local user. For more information on enterprise authentication, see *"There are columns showing each event date, type, description, folder, and total number of documents." on page 35*.

To define local or enterprise users

1. From the **System** view, click **Users**.
2. At the bottom of the Users tab, Click **Add**.

   Under the **User Profiles** tab, (with appliances configured for LDAP authentication only), the user selections appear, along with *Identity Source* and *Search for user* fields.
3. Select **Local User** or **Enterprise** (default).
4. To search for the user, start typing the user's login name.
5. Complete the remaining fields as described in *"Defining User Accounts" on page 15*.

Access Groups and User Creation

In release 8.2, the optional Access Groups feature provides a significant level of access control. Case access can be granted individually, or by assigning users to Access Groups, across the entire workflow. For more about Access Groups, see *"Access Groups" on page 61*.

Assign Access Levels to Groups

You can restrict or assign levels to the following group entities:

- Users
- Cases
- Legal Holds
- Sources
- Locations
- Collection Sets

Case Authorized Operation

If you choose not to assign users to an Access Group, these users will be in a common pool and will have access to all cases not assigned to an Access Group. Users can then be assigned to specific cases. This is called **Case Authorized**. Restrictions on case access can then be further assigned on a user-by-user basis. Case Authorized operation is a less flexible alternative to Group Access. It is recommended for when a user should have access only to a small number of cases.

> **Note:** When users are created, they are either assigned to all Access Groups (the default) or, if the **Case** radio button is selected, authorized for all cases, unless you specifically limit either Access Groups assignment or case authorization.

Administering User Accounts

For information about how to manage user accounts and the roles that determine each user's access permissions, see the following topics:

- *"Defining User Accounts" in the next section*
- *"Defining User Roles" on page 20*
- *"Viewing System Sessions" on page 27*

Defining User Accounts

A user's account and its associated user role determine the system administration tasks the user can perform and the cases the user can search and administer.

A system manager can define accounts with system access to any case, and can define the accounts, roles, and access profiles for all users. If the group access feature is used, a system manager can create groups and assign users to them. Case administrators can define user accounts and access profiles for each of their authorized cases. Accounts created by a case administrator can have case administrative privileges, but not system administrative privileges (see *"Viewing Case Participants and Groups" in the Case Administration Guide*).

Note: For each case, an access profile can override the case privileges in a user's role, and limit visibility within a case to the documents in specific folders and/or a specific date range. The predefined super user account allows access to all administrative functions and cases.

Groups Considerations When Creating New Users

- When creating new users, you must choose Access Type when the user is created. You can assign them to an access **group**, or to authorize them only to specific **cases**.

  Note: You cannot give a user both group access and case authorization. For users with both in version 8.1.1: after an upgrade to 8.2, existing users will retain their case authorization but lose their group assignments. Changes that happen as a part of the upgrade process are reported in the upgrade logs. See the Upgrade Guide for more information on logging and reporting.

- Starting with version 8.2, only users with the **System Manager** role, the **Group Admin** role, or the **Case Admin** role can add users, assign them to roles, assign them to Access Groups, or assign them to cases. A **System Manager** can assign a user to any role, and to any access group. A **Group Admin** can only assign users to that group. A **Case Admin** can only assign users to that case.
- When you create a new user, they will have all of your group access rights by default.

  Note: If a System Manager creates a new user and does not authorize either specific cases or place the user in specific Access Groups, that new user has access to all cases.

- When creating new users, you can choose to place them in an access group, or to authorize them only for specific cases. If you do not do one or the other, the new user will have access to either the same access groups as you, or the same cases.

Note: In previous versions, when creating a new user the default was no visibility into cases until an explicit assignment was made.

- If you wish to create cases but keep them invisible temporarily, you can create an Access Group with few or no users, and place the case there. It can be moved later.
- When users are granted access on a case-by-case basis, this is called **Case-Authorized** operation. Users and cases function as described in *"Case Authorized Operation" on page 14*.

Note: If you are upgrading and are currently using Access Groups, you and other stakeholders should decide how to arrange user and case authorization to Access Groups before upgrading. At least one person must have the **System Manager** role to work with Access Groups. As a System Administrator, you should work with the System Manager, any other Case Administrators, and the workflow management team to define Access Groups, role assignments, and how to resolve related issues as part of any upgrade. Refer to the *Veritas Upgrade Overview* for more information.

To add or view user accounts

1. From the **System** view, click **Users**.
2. Use the **Show** menu to view all accounts or just the enabled, disabled, or expired accounts (enabled accounts are listed by default).
3. To add a new user account with system access:

   A. Click **Add** to open the Add User screen.

   B. Specify the following information. An asterisk (*) indicates a required field.

Field	Description
User Name*	Enter a login name for the user (up to 35 characters). The name is not case sensitive, but must be unique. Use only letters, numbers, and underscores.
Full Name	Enter the user’s full name (up to 255 characters).
Role*	Select a role to specify the user’s access. The predefined roles are: • **Group Admin.** New in 8.2. Allows the user to add and remove users, cases, and other items from the **group** to which they have access, and to perform other administrative tasks. • **Case Admin**. Allows access to all case administration, search, tagging, export, and reporting functions **for a case**, but no System Manager functions. • **Case Manager**. Allows access to one or more **cases**. It includes case admin rights, except for source setup, plus all case user rights. • **Case User**. Allows access to most case search, tagging, export, and reporting functions **for a case**, but provides no system or case administration functions. • **eDiscovery Admin**. Allows a user to manage the Identification Data Map, perform Collections, and Process, Analyze, and Review. System manager privileges are not included. • **Collection Admin**. Allows user to manage only the Identification Data Map and perform Collections. • **Legal Hold Admin**. Allows user administrative access and management of Legal Holds. • **System Manager**. Allows access to all system and case administration, search, and reporting functions. This role gives unrestricted rights to manage the entire system, including admin-level access to all groups and cases. **This role allows the user to manage users in different groups when the Group Access feature is used.** The predefined roles cannot be changed. To define new roles, see *“Defining User Roles” on page 20*. **Note:** Access Groups related changes to case administration roles in 8.2 should be considered when assigning Group Admin (new), Case Admin, Case Manager, Case User, or System Manager roles. See the Case Administration Guide “Case Administration Overview” for more information.

Field	**Description**
Access Type	Choose either **Group** access or **Case** authorization. • You can quickly add a user to one or multiple **groups** with the access group option. The **Available** column displays all the groups that you can add the user to. To add a user to a group, select the group from the **Available** column and click the arrow key to move the group to the **Included** column. Verify that the groups listed in the **Included** column are the ones that should be associated with the user. The **Groups** radio button is selected by default. For this Access Type, the **Authorize Cases** tab will be inaccessible. Users can access only those resources such as cases, legal holds, sources, locations (export and collections) and collection sets that are added in the groups to which the user belongs. • Assign **Case** Authorized users to specific cases only. This method offers less flexibility, but can be more efficient if the user requires access to only a few cases. Select the **Case** radio button and the Authorized Cases tab will become accessible. Any Authorized Cases appear in the **Included** column. Verify that the **Included** cases are the ones that should be associated with that user. If the user does not need access to that case, move it to **Available**. **Note:** You cannot give a user both group access and case authorization.
Account Status	Select whether the account is enabled, disabled (if not expired). Disabling or expired accounts prevent users from logging in, and the account is removed from the user lists.
Expires	Select **Never** or select **On** and click 📅 and select a month and day when the account expires (or enter the date as MM/DD/YYYY). The account expires at 12:01 AM on the selected date.
Password* Verify Password*	Enter and verify a case-sensitive password for the account.
Email Address	Enter the user's email address (up to 255 characters).
Show Info-bubbles	Select whether information icons ⓘ are displayed next to some fields. Moving the cursor over the icon opens a "bubble" describing the field.
Display Micros oft Office documents	Select whether a selected Micros oft Office document is opened in the browser (the default) or in a separate application window (requires Micros oft Office 2007 or later).
Comments	Enter additional comments about the account.

C. To override the case access rights specified in the user role, click the **Case Access Profiles** tab, and select an access profile for the appropriate cases. The following profiles are predefined:

- › **Case Admin.** Allows access to case administrative functions only (no search or report functions)
- › **Case Manager.** Allows access to all case search and report functions (no case administrative functions) for one or more cases.
- › **Case User.** Allows Search, tagging, and print dashboard rights.
- › **Case Reviewer**.

To define new access profiles, such as to limit document visibility to specific folders and/or dates, see *"Defining Case Access Profiles" on page 31*.

D. Click **Save** to submit the new account, or click **Cancel** to discard your changes.

4. To change or enable/disable an account, click the account name, change the account settings, and click **Save**.

5. To delete a user account, follow the steps in *"Disabling Case Access for User Account" on page 34*.

Defining User Roles

A user role specifies a set of access permissions that can be assigned to individual user accounts. Only a system administrator with the role management privilege can create and assign user roles. User roles apply system-wide, but case-specific access can be defined through case access profiles, which can override user role settings. For more information, see *"Defining Case Access Profiles" on page 31*.

To assign a role to an account, see *"Defining User Accounts" on page 15*. The following roles are predefined:

- **Case Admin**. Allows access to all case administration, search, tagging, export, and reporting functions.
- **Case Manager**. Allows access to one or more cases (includes case admin rights, except source setup) plus all case user rights.
- **Case User**. Allows access to most case search, tagging, export, and reporting functions (export, smart tagging, system and case administration functions are not accessible).
- **Collection Admin.** Allows user to only manage the Identification Data Map and perform Collections.
- **eDiscovery Admin.** Allows user to manage the Identification Data Map, perform Collections, and Process, Analyze, and Review. System administration privileges are not included.
- **Group Admin.** Gives the user, Legal Holds Rights, Document Access Rights, all Case Administration rights, and some System Administration rights, such as creating users and assigning them to tasks. System Management, administrative user and role management, and group management are not included unless explicitly granted.
- **Legal Hold Admin.** Allows user to manage all legal hold administrative tasks (except for collections, unless explicitly granted by a system administrator). If read-only access is preferred, the Legal Hold Management box should be unchecked.
- **System Manager**. Allows unrestricted access to all system, groups, and case administration, search, and reporting functions.

Note: If you are evaluating which role to assign a user for Group Access, view the user role to see the default rights. See *"User Role Details" on page 21* for more background. The **System Administrative Settings** section contains the privileges for **User Management**, **Admin User and Role Management**, and **Group Management** for each role.

To add or view user roles

1. From the **System** view, click **Users**.
2. Click the **Roles** tab to view the list of user roles.
3. To add a new user role:

   A. Click **Add**.

   B. Specify the following information. An asterisk (*) indicates a required field.

User Role Details

Field	Description
Role Name*	Enter a role name (up to 35 characters).
Description	Enter a description of the role (up to 255 characters).
General Rights	
	Select check boxes to allow general access rights: • **Allow integrated analytics access**—Allows the user to access the Analytics charts found on the **Case Home > Data Analytics** screen. • **Allow analysis tags dashboard access**—Permit viewing of tags on Review Dashboard. – **Allow access to management charts**—Permit viewing of case management-level charts on the Review Dashboard. • **Allow reports access**—Allows the user to access reports available on the **Processing > Processing Reports** screen. For this feature to be available, the customer needs a pre-processing license, which should be enabled for the case to see these reports. • **Allow mobile access**—Enable access to case information using mobile device.
Collection Rights	
	Select check boxes to allow collections access rights: • **Allow collections access**—Allow users read-only access to the **Identification and Collection screens** in the user interface. This includes **Collections**, C**ollection Templates**, **Collection Sets**, **Sources**, **Source Accounts**, **Source Groups**, **Custodians**, and **Locations**. (users can view Locations from **All Cases -> Locations**. If you select this check box, you can choose the following options: – **Data Map management**—Allows users to also add/modify data map objects. Includes: **Sources**, **Locations (**under **All Cases)**, **Source Accounts**, **Source Groups**, **Custodians**, and **Collection Templates**. – **Collections management**—Allows users to also add/modify collections. – **Clearwell collection sets management**—Allows users to also add/modify collection sets.
Legal Holds Rights	
	Select check boxes to allow legal hold access rights: • **Allow Legal Hold access**—Allow users **read-only** access to the Legal Hold screens in the user interface. If you select this check box, you can choose the following option: – **Legal Hold management**—Allows users to also add, modify, archive or delete legal holds and legal hold settings.

User Role Details (Continued)

Field	Description
Document Access Rights	
	Select check boxes to allow viewing and tagging rights: • **Allow viewing**—Permit viewing of documents. – **Allow tagging**—Select and assign values for one or more tag categories. (Tagging can be enabled only if viewing documents is enabled.) –**Allow moving or removing from folders**—Enable assignment/reassignment/removal of documents to/from folders. –**Allow bulk tagging**—Enable users to tag multiple documents at once. (Bulk tagging can be enabled only if access to item notes is enabled.) –**Allow smart tagging**—Allow user to apply a set of tag values and comments to all current and/or future documents that match the specified search criteria. (Smart tagging can be enabled only if bulk tagging is enabled.) –**Allow viewing of prediction ranks**—Enable viewing of prediction ranks under the **Analysis and Review** module. –**Allow predictive coding actions**—Allow user to apply and manage Transparent Predictive Coding actions. – **Allow access to tag event comments**—Enable viewing of, and adding tag event comments as part of tagging. (Tag event comments can be enabled only if viewing documents is enabled.) – **Allow access to item notes**—Enable viewing of, and adding item notes as part of tagging. (Item notes can be enabled only if viewing documents is enabled.) • **Allow redacting**—Enable redacting functions. This option appears only if the cluster is licensed for the redaction features. – **Prompt for reason code**—Enable user to enter a reason code for the redaction when prompted. This option is only available if redacting is enabled. • **Allow tag history viewing**—Enable viewing of tag history. – **Allow tag history searching**—Enable searching of tag history. • **Allow exporting**—Enable the export of documents from the platform. • **Allow printing**—Enable the printing of documents to PDF files. • **Allow native download**—Enable download of native documents. • **Allow media streaming**—Enable playing of audio media files (requires Audio Search module). • **Allow caching for review—**Allows user to cache case data in preparation for review. • **Allow searching and filtering by processing flags**

User Role Details (Continued)

Field	Description
Case Administration Rights	
Case Administration Rights	Allow users to perform case administration functions. If a user does not have case administration for any cases, the case management screens are not displayed. Select an option from the drop-down menu: • **No case admin rights**—The user cannot perform any case administration functions. • **All case admin rights**—The user can perform all case administration functions. • **Custom case admin rights**—Select from the following options to customize the use case rights: – **Allow case status access**—Allows full access to "View Case Status" screen, in addition to the error/warning logs and the remediation area. If you choose not to allow the role to access to case status, you can still individually configure the other administration rights shown below. If you choose to allow access, choose whether to allow case processing setup: –**Allow case processing source setup**—Allows access to the "Sources & Pre-Processing" screen for the case. (If the parent permission is not selected, this option is not available.)

User Role Details (Continued)

Field	Description
	– **Allow user management**—Allows user to access the **Manage Users** area within the case. User can enable/disable access for system admin users to the case. User can manage case admin users for all the same admin permissions also belonging to this user. However, with this permission, the user is not able to enable/disable permissions that they themselves do not have. – **Allow activity report access**—Allows user to view activity reports. – **Allow group and topic management**—Allows management of groups and topics – **Allow tag definition**—Allows the user to define tags. – **Allow folder Setup**—Allows the user to configure folders and batch documents into multiple review sets using the Batch interface. Select from the following sub-options: –**Allow folder check-out management**—Allows the user to enable reviewers to check in and check out review set folders and to stop or complete a review begun by another reviewer. –**Allow production folder management**—Allows the user to configure production folders. This option appears only if the cluster is licensed for the production feature and is selectable only if **Allow Folder Setup** is selected. –**Allow unlocking of production folders after export**. – **Allow custodian management**—Allows the user to administer custodians. – **Allow participant management**—Allows the user to define aliases and add, delete and edit the list of participants in an alias. – **View exceptions**—Allows access to view processing exceptions associated with a case. –**Manage exceptions**—Allows access to view and manage the processing errors and warnings for the case. User can also search and filter on warnings in the end-user administrator interface. **– Allow OCR processing**—Allows user to process (or resubmit) documents for conversion to OCR after the case has initially processed. (For user procedures, see *"Viewing Documents Processed for OCR" in the Case Administration Guide*.) **– Allow image management**—Enables the image remediation feature. Enables users to access the **Case Home > Images & Rendering** tab, where they can run native cache jobs, import images, and manage existing images. Allows user to access image overlay and remediation options in the Analysis & Review module. This feature replaces prior TIFF import functionality. **– Allow access to automation rules**—Allows the user to create and edit automation rules. – **Other case management functions** (e.g. jobs, batches, etc.)

User Role Details (Continued)

Field	Description
Legal Hold Admin	
General Rights	– **Allow Integrated analytics access**—Allows the user to access the Analytics charts found on the **Case Home > Data Analytics** Screen. – **Allow mobile access**—Enable access to case information using mobile device.
Legal Holds Rights	– **Allow Legal Hold access**—Allows **read-only** access to Legal Holds module unless the Legal Hold management box is checked. –**Legal Hold management**—With access to Legal Holds module, legal hold management includes creation and administration of Legal Holds and Legal Holds notices. **Note:** These rights are the default Legal Hold Admin rights for holds and notices management. A System Administrator with the role management privilege can customize access privileges for a user's rights in all areas. For more information about how this can affect a user with the Legal Hold Admin role, see "Viewing/ Editing the Legal Hold Admin Role" in the Legal Hold User Guide.
System Administrative Settings	– **Allow Case Home and All Cases Dashboard Access**—Allow user to view the overall status (Dashboard) for both single cases (Case Home), and all cases across the system (All Cases) for the cases to which access is granted, **except for the following rights, which must be explicitly granted**: – support access, – case creation, backup, and restore, deletion and template creation – collections and data map backup and restore – user management

User Role Details (Continued)

Field	Description
System Administrative Settings	
	• **Allow Case Home and All Cases Dashboard Access**—Enables user to view all activity for a single case from the **Case Home** view, as well activity across all cases from the **All Cases** > **Dashboard** view. • **Allow system management—**Allow all system management functions, **except for the support, case, and user functions listed below**. • If none of the system management functions are allowed, the System view does not display. If case management also is not allowed for any cases, case management modules are not displayed. **Note:** The System Management privilege allows users to manage jobs and schedules for ALL cases (see *"Managing Schedules and Jobs" on page 71*). – **Allow support access**—Allow access to the support functions, such as uploading logs to support. (For full details, see *"Using the Support Features" on page 118.*) • **Allow new case creation, case backup, restore, deletion, template creation**—Allow the user to create and manage cases and case templates, and back up and restore cases. • **Allow collections and data map backup, restore**—Allows the user access to the Data Map and Collections Backup tab in the Backups screen under the **System** view. Users will be able to create new collection backups and restore existing backups of collections. This option does not effect system level or case level backups and only pertains to the Collection Evidence Repository. • **Allow user management**—Allow the user to add or edit non-system administrative accounts. **Note:** A user who has **Allow User Management** checked but not **Allow group management** will not be able to manage users that are outside his assigned group or create new groups. If the **allow user management** check box is selected, you can also select: – **Allow admin user and role management—**Allows the user to add or edit user roles and system administrative user accounts. – **Allow group management—**Enables user to create and manage user groups including assigning access to cases, legal holds, and collections.

C. Click **Save** to submit the new role, or click **Cancel** to discard your changes.

4. To change a role, click the role name, change the settings, and click **Save**.

   Note: You cannot change the **Case Admin**, **Case User**, or **System Manager** roles.

5. To delete a role, click 🗑 for the role.

Viewing System Sessions

The Sessions screen lists the users who are currently logged in to each appliance in the cluster, and lets you terminate user sessions. The appliance name, login time, session duration, and the client name or IP address are shown for each active user. You may want to terminate user sessions when:

- A user’s access permissions are changed (the changes are not applied to existing sessions)
- An appliance must be backed up, renamed, or deleted

To view the active user sessions

1. From the **System** view, **Sessions**.
2. To view the user sessions for just a single appliance, select the appliance from the **Appliance** menu (all appliance sessions are listed by default).

- To terminate a user session, click the trash icon placed in the user’s row.

  Note: Terminating a user's session does not cancel any of their jobs, the results of which are accessible from the Jobs window found above the navigation bar and the Jobs screen found in the System view.

Managing User Accounts For a Specific Case

For information about how to manage user accounts and access profiles for a specific case, see the following topics:

- *"Defining Case User Accounts" in the next section*
- *"Defining Case Access Profiles" on page 31*
- *"Disabling Case Access for User Account" on page 34*
- *"Viewing User Activity Reports" on page 34*
- *"Viewing Global Activity Reports" on page 35*
- *"Viewing Case Status Report" on page 36*

Defining Case User Accounts

System and case administrators can define user accounts limited to the currently selected case. These accounts default to the "Case User" role, with no administrative access. Case administrators cannot change the role, but they can assign an access profile to the account to override the role's case access privileges, and to limit document visibility by folder and/or date. Also, case access can be disabled for any account, except for accounts that have the System Manager role.

Disabling User Accounts

When you want to ensure security and/or restrict previous user access, you can disable a user account. For example, when a user has left the company, changed roles, or had their access revoked, their user account can be disabled from any cases to which the user had access, and then disabled in the system. For information on how to disable a user, see *"Disabling Case Access for User Account" on page 34*.

Change Password Protection

To ensure security, case administrators cannot change passwords for case users, according to two use cases: 1) If you access to the **Case Home > Users** screen, you can change your own password or the password of any user having access to a subset of the cases to which you have access. 2) If you have access to the **Case Home > Users** screen, you cannot edit users, roles, or change passwords, unless if you have the permission to "Allow admin user and role management".

User accounts added for a specific case are added to the list of user accounts, where they can be modified by a system administrator (see *"Defining User Accounts" on page 15*).

To add or view case user accounts

1. From the **All Cases** view, select a case.
2. Click **Users** to view user accounts with access to the selected case.
3. Use the **Show** drop-down menu to view all accounts or accounts without access to this case.

4. To add a new case user account:

   A. Click **Add**.

   B. Specify the following information. An asterisk (*) indicates a required field.

Case User Profile

Field	Description
User Name*	Enter a login name for the user (up to 255 characters). The name is not case sensitive, but must be unique. Use only letters, numbers, and underscores.
Full Name	Enter the user's full name (up to 255 characters).
Case Access Profile*	Select an access profile if you want to override the case access privileges in the default "Case User" role. The predefined roles are: • **Case Admin**. Allows access to case administrative functions only (no search or report functions). • **Case Manager.** Allows Manager-level access to one or more cases. Includes case admin capabilities (except source setup rights) plus all case user rights. • **Case User**. Allows access to all case search and report functions (no case administrative functions). The predefined access profiles cannot be changed. To define new profiles, such as to limit document visibility to specific folders and/or dates, see *"Defining Case Access Profiles" on page 31*.
Account Status	Select whether the account is enabled or disabled. Disabling an account prevents users from logging in and removes the account from user lists.
Expires	Select **Never** or select **On** and click 📅 and select a month and day when the account expires (or enter the date as MM/DD/YYYY). The account expires at 12:01 AM on the selected date.
Password* Verify Password*	Enter and verify a case-sensitive password for the account (up to 17 characters).
Email	Enter the user's email address (up to 255 characters).
Show InfoBubbles	Select whether information icons ⓘ are displayed next to some fields. Moving the cursor over the icon opens a "bubble" describing the field.
Display Microsoft Office documents	Select whether a selected Microsoft Office document is opened in the browser (the default) or in a separate application window (requires Microsoft Office 2007 or later).
Comments	Enter additional comments about the account.

   C. Click **Save** to submit the new account, or click **Cancel** to discard your changes.

5. To import user information from a file:

   A. Click **Import** to open the Import File dialog box.

   Note: Veritas strongly recommends checking the sample CSV file to ensure your file contains all required columns and data before import. Click the **Download example CSV file** link.

The following table shows the required entries in the CSV file.

CSV File Contents

Item	Comment
User Name	User's name
Full Name	Complete name to identify the user
Identity Source	Local or Enterprise **Note:** This is required for appliances configured for LDAP authentication. For more information about local versus enterprise users, see *"Defining a Local or Enterprise User Account" on page 13*.
Access Profile	System manager, case administrator, case user
Account Status	Enabled or disabled
Expire Date	Date that the user information expires
Password	User password
Confirm Password	User password (must match Password)
Email Address	User email address
Show Info Bubbles	Yes or No
Display MS Office docs in application	Yes or No
Comments	Text comment
Access to all cases	(User has access to all cases, current and future) TRUE or FALSE
Cases	(Provide the names of cases the user will have access to) Example: Case1|Case2|Case3

B. Click ... to select the file to upload using the following format, with one record per line.

C. Click **Next** to upload the selected file. The uploaded items are displayed.

D. Click the **Use first row as column header** check box to maintain a separate header row that is not imported as data.

E. Click **Finish**.

The users are added to the list on the Manage User screen.

6. To change an account, click the account name, change the account settings, and click **Save**.

7. To enable or disable case access for one or more accounts, select the check box next to the appropriate accounts, select the menu option at the bottom of the screen, and click **Go**.

Defining Case Access Profiles

An access profile overrides the default access privileges for a specific case. Only system administrators can create and assign access profiles. The following predefined access profiles can be used for any case (they cannot be changed):

- **Case Admin**. Allows access to case administrative functions only (no search or report functions).
- **Case Manager**. Allows access to one or more cases (includes case admin rights, except source setup) plus all case user rights.
- **Case User**. Allows access to all case search and report functions (no case administrative functions).

If you add a new access profile, it can be used only for the current case. To assign a new access profile to an account, see *“Defining Case Access Profiles” on page 31* or *“Defining Case User Accounts” on page 28*.

To add or view access profiles

1. From the **All Cases** view, on the top navigation bar, select a case.
2. Click **Users**.
3. Click the **Access Profiles** tab.
4. To view an access profile, click the profile name, or click **Add** to add a new access profile for this case.

   A. Specify the following information. An asterisk (*) indicates a required field.

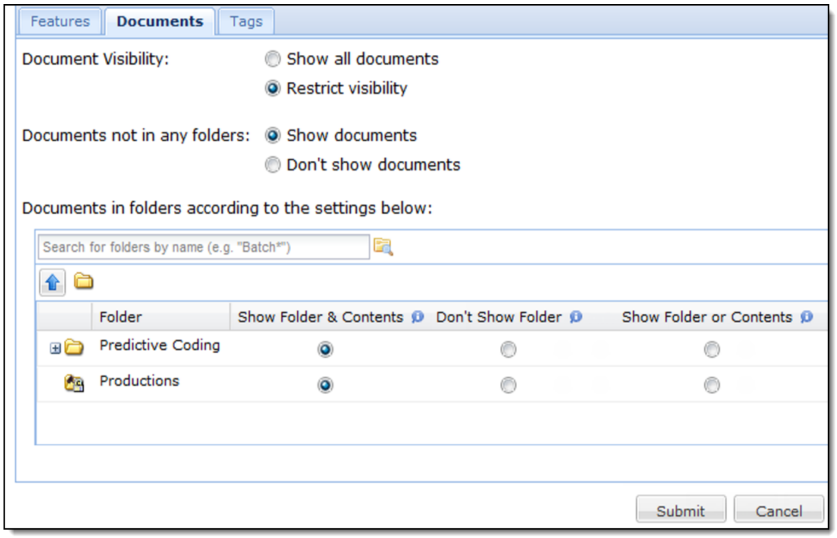
Access Profile Details

Field	Description
Profile Name	Enter a profile name (up to 255 characters).
Description	Enter a description of the profile (up to 255 characters).
Features Tab	
General Rights	Select check boxes to allow general access rights: • **Allow integrated analytics access**—Permit viewing of documents. • **Allow analysis tags dashboard access**—Permit viewing of tags on Review Dashboard. – **Allow access to management charts**—Permit viewing of case management-level charts on the Review Dashboard. • **Allow reports access**—Enable access to the reports shown on the Review Dashboard screens. **Allow mobile access**—Enable access to case information using mobile device.

Access Profile Details (Continued)

Field	Description
Document Access Rights	Select check boxes to allow viewing and tagging rights: • **Allow viewing**—Permit viewing of documents. – **Allow tagging**—Select and assign values for one or more tag categories. (Tagging can be enabled only if viewing documents is enabled.) –**Allow moving or removing from folders**—Enable assignment/reassignment/removal of documents to/from folders. –**Allow bulk tagging**—Enable users to tag multiple documents at once. (Bulk tagging can be enabled only if access to item notes is enabled.) –**Allow smart tagging**—Allow user to apply a set of tag values and comments to all current and/or future documents that match the specified search criteria. (Smart tagging can be enabled only if bulk tagging is enabled.) – **Allow access to tag event comments**—Enable viewing of, and adding tag event comments as part of tagging. (Tag event comments can be enabled only if viewing documents is enabled.) – **Allow access to item notes**—Enable viewing of, and adding item notes as part of tagging. (Item notes can be enabled only if viewing documents is enabled.) • **Allow redacting**—Enable redacting functions. This option appears only if the cluster is licensed for the redaction features. • **Allow tag history viewing**—Enable viewing of tag history. – **Allow tag history searching**—Enable searching of tag history. • **Allow exporting**—Enable the export of documents from the eDiscovery Platform. • **Allow printing**—Enable the printing of documents to PDF files. • **Allow native download**—Enable download of native documents. • **Allow caching for review—**Allows user to cache case data in preparation for review. • **Allow searching and filtering by processing flags** • **Case Administration Rights**—No case administration, all case administration, or custom case administration rights. For custom rights, you can select additional custom rights, including the ability to manage production folders. The production option appears only if the cluster is licensed for the production feature.

Access Profile Details (Continued)

Field	Description
Documents Tab	 Features · Documents · Tags Document Visibility: ○ Show all documents ● Restrict visibility Documents not in any folders: ● Show documents ○ Don't show documents Documents in folders according to the settings below: Search for folders by name (e.g. "Batch*") Folder · Show Folder & Contents · Don't Show Folder · Show Folder or Contents Predictive Coding · ● · ○ · ○ Productions · ● · ○ · ○ Submit · Cancel
Show all documents	Select to make all documents visible for the access profile. **Note:** Settings are selected here, but the user will view the documents from within the context of a case, not from the **All Cases** view. What the user will see will also be based on their role and access.
Restrict visibility	Select options to restrict folder rights. Click the + icons as needed to expand the listing. • **Documents not in any folders**—Specify whether to show or not show documents that are assigned to any folder. • **Documents in folders according to the settings below**—Specify the visibility for specific folders. – **Show folder and contents**—Allow users to view and search the selected folder and the documents within the folder. – **Don't show folder**—Prevent users from viewing and searching the folder. This option has no effect on document visibility. – **Don't show folder or contents**—Prevent users from viewing and searching the folder and any of the documents within the folder. If a document is assigned to both a visible and non-visible folder, the document is visible and can be viewed and searched. To hide a document completely, make sure it is assigned only to non-visible folders.
Tags Tab	Click the tag set and set the visibility by selecting the Show or Hide options on the right.

B. Click **Submit** to submit the new access profile, or click **Cancel** to discard your changes.

5. To change a profile, click the profile name, change the settings, and click **Save**.

   Note: You cannot edit the default profiles from the System Admin page. From within a case, the System Administrator can edit and assign case-specific privileges.

6. To delete a profile, click 🗑 for the profile.

Disabling Case Access for User Account

To disable case access for the user account

1. From the **All Cases** view, select a case.
2. Click **Users** to view user accounts with access to the selected case, then click to select the user you want to disable.
3. Select **Disable Case Access** then click **Go**.

Viewing User Activity Reports

Activity reports list all events for specific users, specific events for all users, or tagging events for specific folders. The events include login, logout, searches, and the tagging, redaction (including bulk redaction and deletion), exporting, and printing of search results. A one-line summary of the search results is shown for each search. All activity reports are limited to the selected case.

To generate an activity report for all cases, see *"Viewing Global Activity Reports" on page 35*.

To view activity reports

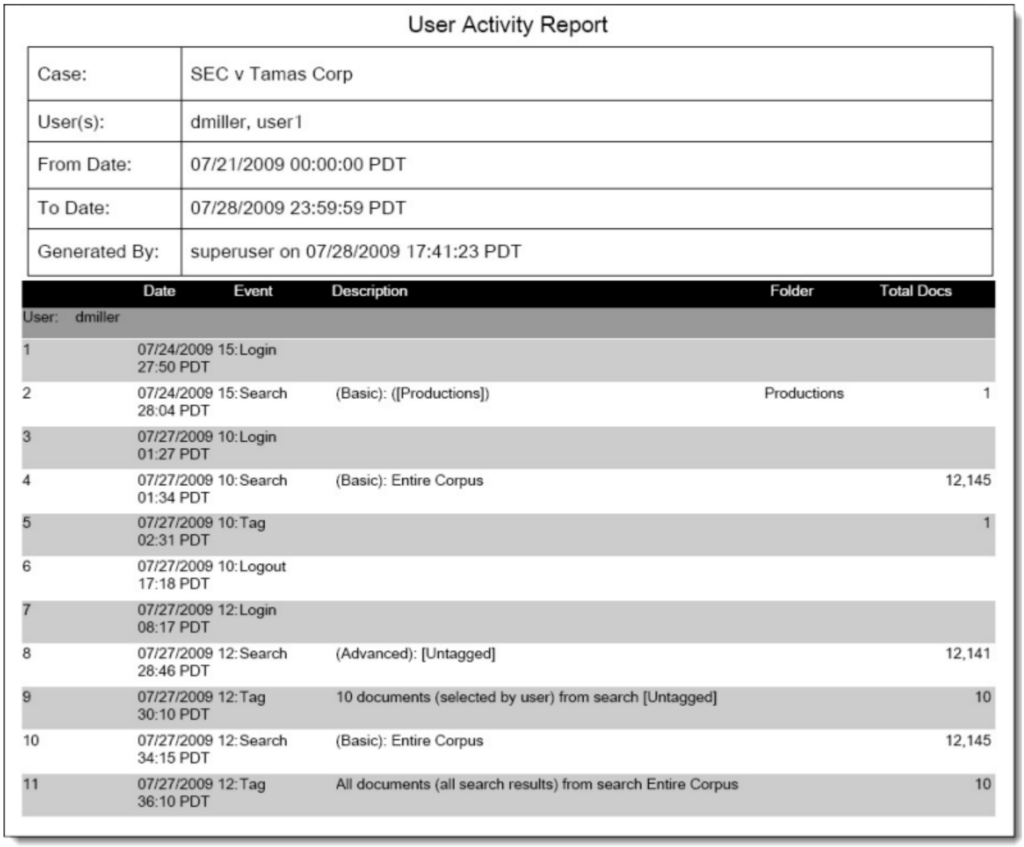
1. From the **All Cases** view, select a case and click **Activity Reports** to open the View Activity Report screen.
2. Specify the following information.

Generating Activity Reports

Field	Description
Type	Select the report type: • **Users**. Displays all events for one or more case users. Click **Users**, and select the users to be included in the report. • **Events**. Displays selected events for all case users. Click **Events**, and select the events to be included in the report.
Format	Select whether the report is in PDF or comma-separated value (CSV) format.
Date Range	Select a report for the last 7 or 30 days, or click 📅 and specify start and end dates for the report.

3. Click **Generate**, and then follow the prompt to open or save the file.

   The following example shows all search, export, and print events for the case for a given user. The **Folder** column indicates whether the search was limited to a specific folder. The **Total Docs** column indicates the number of documents in the search results or the number of documents exported or printed.



User Activity Report

Case:	SEC v Tamas Corp
User(s):	dmiller, user1
From Date:	07/21/2009 00:00:00 PDT
To Date:	07/28/2009 23:59:59 PDT
Generated By:	superuser on 07/28/2009 17:41:23 PDT

	Date	Event	Description	Folder	Total Docs
User: dmiller					
1	07/24/2009 15:27:50 PDT	Login			
2	07/24/2009 15:28:04 PDT	Search	(Basic): ([Productions])	Productions	1
3	07/27/2009 10:01:27 PDT	Login			
4	07/27/2009 10:01:34 PDT	Search	(Basic): Entire Corpus		12,145
5	07/27/2009 10:02:31 PDT	Tag			1
6	07/27/2009 10:17:18 PDT	Logout			
7	07/27/2009 12:08:17 PDT	Login			
8	07/27/2009 12:28:46 PDT	Search	(Advanced): [Untagged]		12,141
9	07/27/2009 12:30:10 PDT	Tag	10 documents (selected by user) from search [Untagged]		10
10	07/27/2009 12:34:15 PDT	Search	(Basic): Entire Corpus		12,145
11	07/27/2009 12:36:10 PDT	Tag	All documents (all search results) from search Entire Corpus		10

   There are columns showing each event date, type, description, folder, and total number of documents.

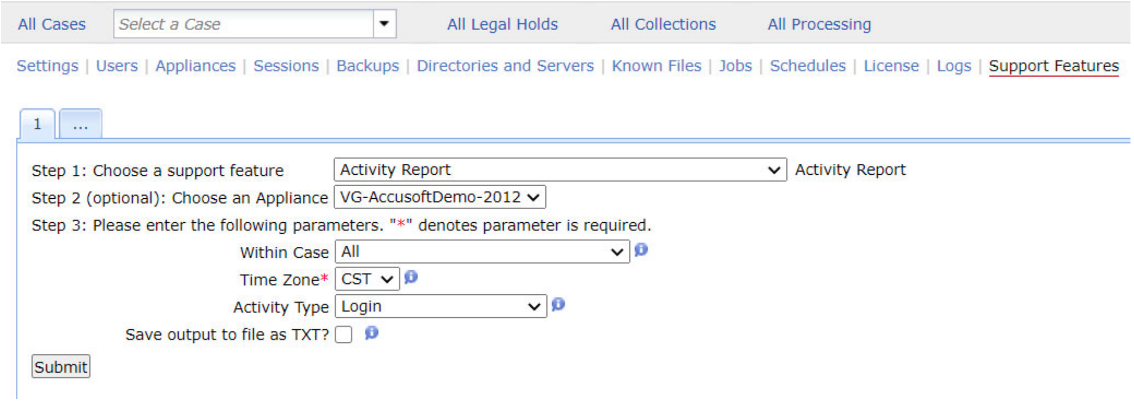
Viewing Global Activity Reports

Starting with release 9.5.1, users can generate the Global Activity Report either for a specific case or for all cases. Users can select the time zones in which the last activity time should be reported, and generate reports based on the activity type.

To generate a global activity report

1. Using an account with System Management permissions, log onto the eDiscovery Platform web interface.

2. From the **System** > **Support Features**, select **Activity Report**.


All Cases
Select a Case
All Legal Holds
All Collections
All Processing
Settings | Users | Appliances | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | License | Logs | Support Features
1
...
Submit

Step 1: Choose a support feature Activity Report Activity Report

Step 2 (optional): Choose an Appliance VG-AccusoftDemo-2012

Step 3: Please enter the following parameters. "*" denotes parameter is required.

Within Case All

Time Zone* CST

Activity Type Login

Save output to file as TXT? □

3. Optionally, choose an appliance to which the feature will apply.

4. Specify the following information:
   - **Within Case**: Select a specific case or All to generate the activity report for.
   - **Time Zone**: select the time zones in which the last activity time should be reported.
   - **Activity type**: Select the user activity on which the report to be based on.

5. Select the save output to file as TXT check box to redirects the output to a unique TXT file.

6. Click **Submit**. The report details are displayed on the screen.

Viewing Case Status Report

Starting with release 10.0, users with the **`Allow Support Access`** permission can generate a case status report using the "Case Status Report" support feature. This report helps administrators to see active and inactive cases, and decide on when to archive an inactive case.

A user with the **`Allow Support Access`** permission can generate a xlsx report for all available cases in the system with following columns:

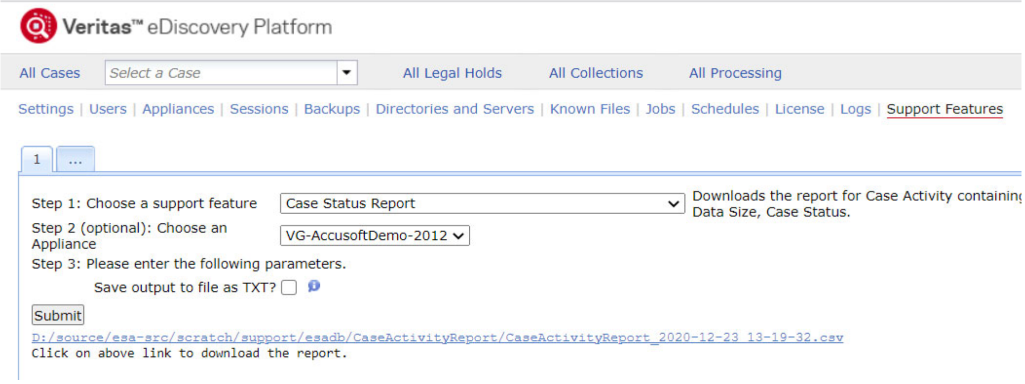
- **Case** – The name of the case.
- **Created By** – The name of the user who created the case. If the full name of the user is not available, then the username is displayed.
- **Creation Date** – The date (MM-DD-YYYY) and time (HH:MM:SS) when the case was created. The time zone is also displayed.
- **Days Open** - The number of days from the case creation date to the current date in days.
- **Last Activity Date** -The date on which the last processing or search was performed on the case.
- **Days Inactive** - The number of days from the "Last Active Date" to the current date in days.
- **Processed Data Size** – The size of the processed data for the case.
- **Status** – The status of the case, it can be **Active** or **Inactive**.

When a case has no processing or search activity for 30 days, it is marked as an inactive case by default. This duration can be configured using the **`esa.support.caseactivityreport.threshold.days`** property. The default value for this property is set as 30 days.

The case status is Active when the Days Inactive is less than or equal to the days defined for the above mentioned property, and Inactive when the Days Inactive is greater than the days defined for the above mentioned property.

To generate a case status report

1. Using an account with System Management permissions, log onto the eDiscovery Platform web interface.
2. From the **System** > **Support Features**, select **Case Status Report**.


Veritas™ eDiscovery Platform
All Cases
Select a Case
All Legal Holds
All Collections
All Processing
Settings | Users | Appliances | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | License | Logs | Support Features
1
...

Step 1: Choose a support feature: Case Status Report
Downloads the report for Case Activity containin
Data Size, Case Status.

Step 2 (optional): Choose an Appliance: VG-AccusoftDemo-2012

Step 3: Please enter the following parameters.

Save output to file as TXT? □

Submit

```
D:/source/esa-src/scratch/support/esadb/CaseActivityReport/CaseActivityReport_2020-12-23_13-19-32.csv
Click on above link to download the report.
```

3. Optionally, choose an appliance to which the feature will apply.
4. Click **Submit**. A download link appears on successful execution of the feature.
5. Click the link to save the report on your computer.

Managing Security of eDiscovery Platform

For information about how to authorize, authenticate and secure, see the following topics:

Secure Windows Server

The Veritas eDiscovery Platform runs on the following operating systems:

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

Veritas recommends that you follow standard practices for securing these operating systems. Install all Windows updates.

You should change the default Windows Server password that ships with the appliance to one that meets your security policies. You should also change the default password of the superuser account used to access the eDiscovery application. See *QuickStart Guide*.

Additional security issues to consider:

- **Firewall**. The Windows firewall is enabled by default, and eDiscovery applications are registered by name (rather than by port) to communicate through the firewall. To view the firewall settings or to configure a third-party firewall, see the *"Using the Support Features" on page 118*.

  Note: On utility nodes, the Windows firewall is disabled by default.

- **Data Security**. By default, documents are indexed where they currently reside, and are not copied to the appliance. Users can retrieve and view indexed documents, but cannot change them. When the user logs off, any documents fetched during the session are flushed from the system. Note the following:
  - Printed and exported documents ARE copied to the appliance, so users should delete their print and export jobs after they download the files. For added security, users can flush the browser cache after a session.

    To configure the confidentiality footer for printed reports, from the **System** view, click **Settings > Print** tab. Type the new confidentiality footer text in the field provided. (See *"Defining System Settings" on page 90*).
  - The eDiscovery Platform does not scan documents for viruses. If you want to install anti-virus software on an appliance, contact Technical Support for configuration instructions.

- **Network Security**. Veritas recommends using Secure Sockets Layer (SSL) encryption to secure access to the appliances from any untrusted network. The appliance uses port 443 for SSL and recommends that only this port should be accessible from an untrusted network.

- **Access to Network Shares**. Starting with eDiscovery Platform 9.5, only the SMB2 Windows Network Share access protocol is supported, which replaces the less secure SMB1 protocol that was supported in earlier versions of eDiscovery Platform. Advise your system administrator to enable the SMB2 protocol on all the servers on which eDiscovery Platform is installed as well as on the file shares that are accessed by eDiscovery Platform for various functions.

- **Enhancements in password** . The eDiscovery Platform release 9.5 provides enhanced security by increasing the minimum requirements for user passwords in terms of password length and complexity.

- **Ability to change AES Key and AES key password**. The eDiscovery Platform release 9.5 provides a security enhancement where system administrators can use the Password Manager option of the Clearwell Commander to generate a new AES key or to change the password associated with the AES key.

  Note: You must not change the AES key while any job is running.

The eDiscovery Platform is certified to work with the browser's default security settings. If you use custom security settings, contact Technical Support for guidance on known security issues.

For additional security, you can force redirection to HTTPS for all access attempts. See *"Defining System Settings" on page 90*.

Changing Database Root and User Passwords

For security reasons, some organizations require that the MySql and User passwords be changed to conform with their own standards for passwords. MySQL passwords can only be edited with Clearwell Commander or through the property browser.

Important: This function is password protected. These passwords should only be managed with assistance from Support, or by someone in Support. Changing these passwords without understanding the effects can be disastrous, such as permanent loss of access to the data. This tech note contains the list of passwords managed by Clearwell Commander: 000114500.

For more about Clearwell Commander's functions, see *"Clearwell Commander" on page 105*.

Managing the JDK and TOMCAT password

System administrators can now use the **Password Manager** option of the Clearwell Commander on the Appliance desktop to periodically change the password for TOMCAT and Java Certificates store.

When the password for TOMCAT and JDK Certificates store is changed on the Primary node (Admin server), the changes are applied to all secondary nodes in the cluster, but not to the Utility node. System administrators can change these passwords for the Confirmation server by using the Clearwell Commander on the Confirmation Server appliance's desktop. This enhancement is currently not available for the Utility nodes.

To change the JDK and TOMCAT password

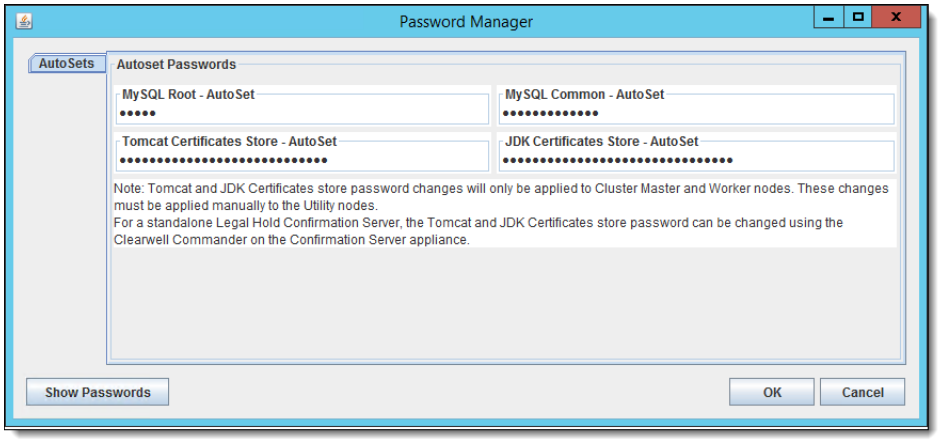
1. On the appliance's Windows desktop, double-click the Clearwell Commander icon. A user with System Manager rights can access Clearwell Commander from the icon on an appliance's desktop.

2. From **Action**, select **Stop Appliance Services**. Also stop PrizmDoc services.

3. From **Action**, select **Password Manager**.

4. This function is password protected. Enter your System Manager (superuser) account password and click **OK**.

5. The Password Manager screen appears. Click **Show Passwords**.



Password Manager

AutoSets

Autoset Passwords

MySQL Root - AutoSet: •••••

MySQL Common - AutoSet: •••••••••••••

Tomcat Certificates Store - AutoSet: •••••••••••••••••••••••••••••

JDK Certificates Store - AutoSet: ••••••••••••••••••••••••••••••••

Note: Tomcat and JDK Certificates store password changes will only be applied to Cluster Master and Worker nodes. These changes must be applied manually to the Utility nodes.
For a standalone Legal Hold Confirmation Server, the Tomcat and JDK Certificates store password can be changed using the Clearwell Commander on the Confirmation Server appliance.

6. Change the required TOMCAT and JDK password.

7. Click **OK**.

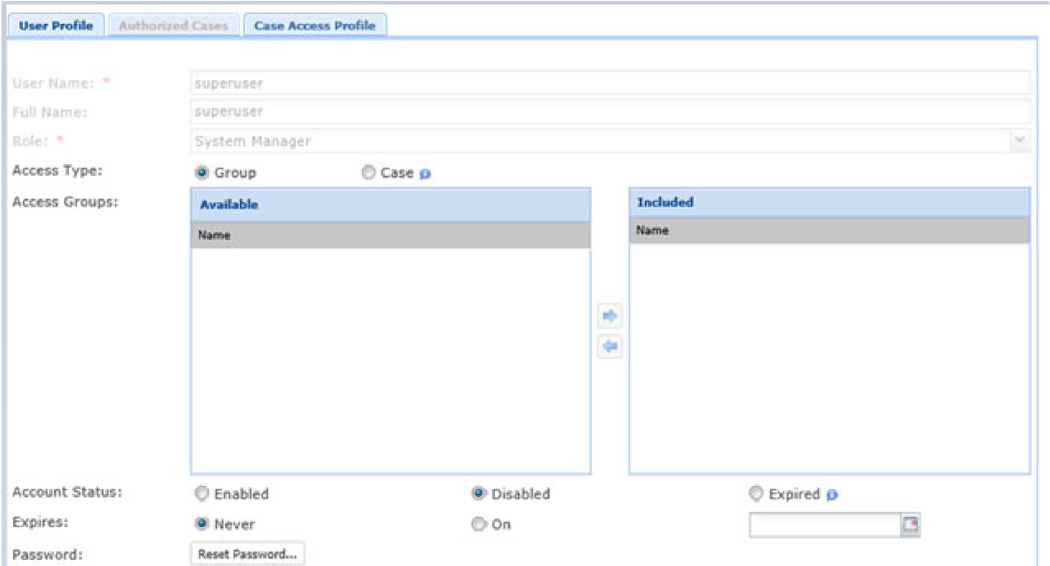
For a clustered deployment, you need to perform these steps only on the Primary node. It will change password for both Primary and secondary nodes in the cluster.

Ability to disable the superuser account

Starting with eDiscovery Platform 9.5, the capability to disable the superuser account is provided. This feature is enabled by default.

To delete the superuser account

1. Log in as a user who has the System Manager role (other than superuser).
2. Navigate to **System** > **Users**.
3. Click on the **superuser** row from the users list.
4. Open the **User Profile** tab.
5. Select the **Disabled** option from the **Account Status** values.



User Name: * superuser

Full Name: superuser

Role: * System Manager

Access Type: ● Group ○ Case

Access Groups:

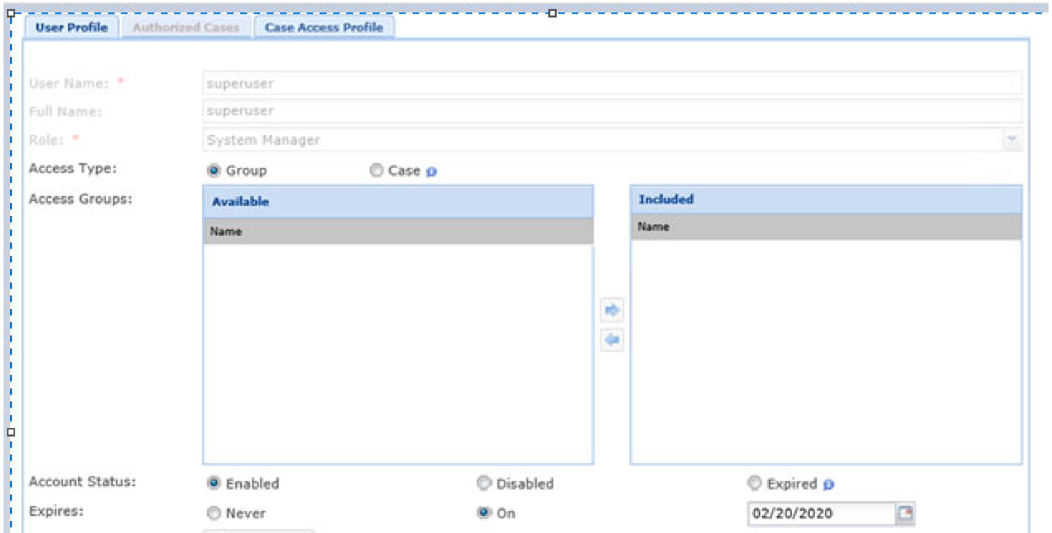
Account Status: ○ Enabled ● Disabled ○ Expired

Expires: ● Never ○ On

Password:

To expire the superuser account

1. Log in as a user who has the System Manager role (other than superuser).
2. Navigate to **System** > **Users**.
3. Click on the **superuser** row from the users list.
4. Open the **User Profile** tab.
5. Select the **On** option from the **Expires** values and set an expiration date.



User Name: * superuser

Full Name: superuser

Role: * System Manager

Access Type: ● Group ○ Case

Access Groups:

Account Status: ● Enabled ○ Disabled ○ Expired

Expires: ○ Never ● On 02/20/2020

To enable or disable the feature that lets you disable or expire the superuser account

1. On the **Support Features** screen, select the **Property Browser** support feature, and then select an appliance.
2. To change the name of the property, type the following case-sensitive value: `esa.disable.superuser.feature.enabled`

   Note: The system properties are case-sensitive. When checking the value of a property or updating an existing property, be sure to check for case-sensitivity.

   > **Tip:** If you accidentally set a property with the incorrect case, first remove it, and then set its value again with the correct case.

3. For the **New Value** specify, `type:true`.
4. Select both the check box options to confirm your changes and to save your settings to a text output file.

Known limitation

A lockout may occur if all the users with the System Manager role are marked to expire at a future date and the superuser is also disabled. Such a lockout situation can only be resolved over a Support call. To avoid such a lockout situation, before you disable the superuser, ensure that at least one user with the System manager role is not marked as disabled or is marked to never expire.

Enterprise Authentication

The eDiscovery Platform supports two types of authentication: local authentication and enterprise authentication. With regular local authentication, users are authenticated against a user name and password stored in the eDiscovery Platform database. With enterprise authentication, users are authenticated against an enterprise authentication solution using their log on name.

The following enterprise-authentication mechanisms are currently available.

- LDAP
- Integrated Windows Authentication (IWA)
- Header-based authentication
- SAML 2.0 based authentication with trusted Identity Provider

When the eDiscovery Platform is configured to use enterprise authentication, system administrators have the ability to create users as local or enterprise users. Enterprise users will be authenticated against the enterprise-authentication mechanism and local users (such as *superuser*) will always be authenticated against the username and password stored in the eDiscovery Platform database.

System administrators may want to create local users for users who do not have access to the internal domain (such as external contractors using the system). However, in most cases users will be added as enterprise users and authenticated against the configured methods of enterprise authentication.

Moving to an Enterprise Authentication Environment

Until enterprise authentication is enabled, all users are local users, meaning that they must have an eDiscovery Platform username and password to log in. Depending on the method of enterprise authentication that is used, the way newly created and converted enterprise users log on may change. When using LDAP, the login page will remain unchanged and users will continue to use a username and password. With IWA and Header methods, the login page will change to one that facilitates automatic login.

Note: The superuser account will always be a local user and will require a password to log in.

After IWA or Header authentication is enabled, local users must use the following link to log in.

```
http://CW_appliance_server/esa/public/login.jsp
```

Configuring User Authentication for LDAP

When the 's LDAP feature is enabled, all user authentication is performed via LDAP except Local accounts.

Note: Once Enterprise authentication is enabled, only system administrators can create new local users. Users created by the Case Admin will always be enterprise users.

To set up authentication via LDAP

The properties to enable LDAP authentication are set using the **Property Browser** Support Feature. All property changes related to enterprise authentication should be made using the Property Browser. The Property Browser automatically updates the appliance each time you add a new property.

1. Using an account with System Management permissions, log onto the eDiscovery Platform web interface.
2. From the **System > Support Features**, select the **Property Browser**.
3. Using the Property Browser, configure the required set of properties to enable LDAP authentication. See the *List of Required LDAP Configuration Properties*.
4. Verify the LDAP configuration properties are set correctly by running the **LDAP Configuration Tester** Support Feature without entering a username and password. This will list all currently set LDAP configuration properties and their values. You cannot test user authentication until LDAP is enabled and an enterprise user is added.
5. Enable LDAP authentication by setting **`esa.ldap.enabled`** to true.

List of Required LDAP Configuration Properties

```
esa.ldap.connectionName
esa.ldap.connectionPassword
esa.ldap.connectionURL
esa.ldap.enabled
esa.ldap.userBase
esa.ldap.userSubtree
esa.ldap.userSearch
esa.ldap.referrals
```

LDAP Property Configuration Reference

LDAP integration is controlled by a set of configuration properties that are shared among all appliances in a cluster.

`esa.ldap.enabled`
Enable or disable LDAP authentication.
Default: `false`
Syntax: `true/false`

`esa.ldap.connectionURL`
URL and port of the LDAP directory server. Supplied by the network administrator.
Default: N/A
Syntax: `ldap://<ldapserver>:<port>`
Example: `ldap://server1:company.com:389`

`esa.ldap.connectionAltURL`

URL of failover LDAP directory server. Will only be used if first server is inaccessible.
Default: N/A
Syntax: **`ldap://<ldapserver>:<port>`**
Example: **`ldap://server1:company.com:389`**

`esa.ldap.connectionName`

User account used to connect to LDAP Directory Server. Password should not change. Using one of the service accounts is recommended.
Default: N/A
Syntax: **`<user>@<domainFQDN>`** or **`<domain\<user>`**
Example: **`company\administrator`**

`esa.ldap.userBase`

Base DN used to search for users. For best results, try to be as selective and specific as possible. Restrict the query to the minimally required branch of the tree or forest. Must be set in conjunction with **`esa.ldap.userSearch.`** Must be removed if using **`esa.ldap.userPattern.`**
Default: N/A
Example: **`ou=Clearwell, dc=foo, dc=com`**

`esa.ldap.userSearch`

Pattern used to search for users when using anonymous binding. Cannot be used in conjunction with **`esa.ldap.userBase`**. Must be removed if using **`esa.ldap.userPattern`**. Does not typically need to be changed.
Syntax: Standard LDAP query format.
Default: **`(&(objectClass=user) (sAMAccountName={0}))`**

`esa.ldap.userPattern`

DN Pattern to use for binding after an anonymous connection. Cannot be used in conjunction with **`esa.ldap.userSearch`** or **`esa.ldap.userBase`**. Must be removed if using **`esa.ldap.userPattern`**. Does not typically need to be changed.
Default: N/A
Example: **`cn={0}, ou=Clearwell, dc=foo, dc=com`**

`esa.ldap.userSubtree`

Determines if search for users is recursive to the **`esa.ldap.userBase`** DN.
Default: **`true`**
Syntax: **`true/false`**

`esa.ldap.roleBase`

Base DN used to identify roles. See *"Automatic User Creation and Role Assignment" on page 56*.
Default: N/A
Example: **`ou=Clearwell, dc=foo, dc=com`**

`esa.ldap.roleSearch`

Search pattern used to identify roles. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: Standard LDAP query format.
Example: **`(memberOf={0})`**

`esa.ldap.roleName`

Name of LDAP attribute used to determine role. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: **`attributeName`**
Default: N/A
Example: **`name`**

`esa.ldap.roleSubtree`

Determines if search for roles is recursive to **`esa.ldap.roleBase`** DN. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: **`true/false`**
Default: **`true`**

`esa.ldap.createUnknownUsers`

Enables automatic user creation if a successfully authenticated LDAP user does not have a user account in eDiscovery Platform. User will be assigned role and case access based on other properties. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: **`true/false`**
Default: **`false`**

`esa.ldap.useLDAPRoles`

Enables automatic user role change based on LDAP role. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: **`true/false`**
Default: **`false`**

`esa.ldap.newUserCaseList`

List of cases that automatically created users are assigned access to. Special value of **`'<all-cases>'`** gives access to all cases. Empty gives access to none. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: Comma separated list of all case names.
Default: N/A
Example: **`Case1, Case2, Case3`**

`esa.ldap.defaultRole`

Default role that LDAP users will get, when no matching role is found when using automatic role assignment. Required to be set when using **`esa.ldap.createUnknownUsers`** without automatic role searching. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: **`RoleName`**
Default: N/A
Example: **`Case User`**

`esa.ldap.newUserEmailDomain`

Email domain appended to user name for automatically created users. See *"Automatic User Creation and Role Assignment" on page 56*.
Syntax: Domain FQDN
Default: N/A
Example: **`company.com`**

`esa.ldap.userComment`

Comment applied to profile for automatically created users. See *"Automatic User Creation and Role Assignment" on page 56*.
Default: **`LDAP User`**

`esa.ldap.referrals`

Determines method used when LDAP directory server gives a referral response. This is usually required when using an Active Directory domain controller as the LDAP directory server. In most instances the correct setting will be **`'follow'`**.
Syntax: **`follow/ignore/throw`**
Default: N/A

`esa.ldap.user.distinguishedName`

LDAP attribute used to populate user information when creating new users.
Syntax: Attribute Name
Default: **`distinguishedName`**

`esa.ldap.user.email`

LDAP attribute used to populate user information when creating new users.
Syntax: Attribute Name
Default: **`mail`**

`esa.ldap.user.fullname`

LDAP attribute used to populate user information when creating new users.
Syntax: Attribute Name
Default: **`displayName`**

`esa.ldap.user.username`

LDAP attribute used to populate user information when creating new users. Must match LDAP property used in **`esa.ldap.userSearch`**. Usually **`sAMAccountName`** in Active Directory implementations.
Syntax: Attribute Name
Default: **`sAMAccountName`**

`esa.ldap.userPrefixSearch`

Search pattern used when adding new users manually. Affects the **Search** field in the **Add User** screen. Usually does not need to be changed.
Syntax: Standard LDAP query
Default: (&(objectClass=user)(|(sAMAccountName={0}*)(displayName={0}*)(mail={0}*)))

Untested Properties

`esa.ldap.protocol`
`esa.ldap.authentication`
`esa.ldap.derefAliases`

Configuring Integrated Windows Authentication (IWA)

The eDiscovery Platform supports enterprise authentication via Integrated Windows Authentication (IWA).

To set up authentication via IWA

Before you begin: LDAP must be configured and enabled against the Active Directory domain from which Windows users will be authenticating. This is required to permit selection of domain users for access to the eDiscovery application.

1. Using an account with System Management permissions, log onto the eDiscovery Platform web interface.

2. From the **System > Support Features**, select the **Property Browser**.

   Note: All property changes related to enterprise authentication should be made using the Property Browser. The Property Browser automatically updates the appliance each time you add a new property.

3. Configure the set of properties to enable IWA authentication.

   – **`esa.iwa.enabled`**
   Required. Set value to **`true`**.

   – **`esa.iwa.allowLdap`**
   Optional. To enable LDAP form authentication, set to **`true`**.

   – **`esa.iwa.allowNtlm`**
   Optional. To use NTLM authentication between hosts, set to **`ALL.`**
   To use IWA authentication from the local machine to itself, set to **`LOCAL`**.

4. For Active Directory configurations, set the Service Principal Name (SPN) for each system in the cluster.

   Note: The **`setspn`** command can be run by a domain administrator from any system in the domain. The command must be run for each node in the cluster.

   ```
   setspn -A HTTP/cw.server.fqdn customer-domain\user-running-esa
   ```

   `edp.server.fqdn`
   The fully-qualified domain name (FQDN) for each server in the cluster. For example: **`ClearwellAppServer.corp.com`**

   `customer-domain`
   The fully-qualified domain name. Example: **`corp.local`**

   `user-running-esa`
   The user account running the application service. Example: **`esaAdmin`**

5. Add the fully-qualified domain name (FQDN) to the browser's list of secure websites.

Configuring Header-based Authentication

The eDiscovery Platform supports authentication in an environment with an existing header-based, single sign-on (SSO) solution.

Note: You must be able to configure applications to be accessible through reverse proxy.

To set up header-based authentication

Before you begin: If user accounts are stored in a company LDAP directory, configure LDAP so that the accounts can be added to the eDiscovery application.

1. Using an account with System Management permissions, log onto the eDiscovery platform web interface.
2. From the **System > Support Features**, select **Property Browser**.

   Note: All property changes related to enterprise authentication should be made using the Property Browser. The Property Browser automatically updates the appliance each time you add a new property.
3. Configure the set of properties to get authentication working.
   - **`esa.auth.header.enabled`**
     Required. To enable header-based authentication, set to **`true`**.
   - **`esa.auth.header.headerName`**
     Optional. Name of the HTTP header, which specifies the username to authenticate.
   - **`esa.auth.header.loginURI`**
     Optional. URL of the webpage that the user should be sent to upon logging out.
   - **`esa.auth.header.allowedHosts`**
     Optional. Space or comma-separated list of host names or IP addresses to be accepted. This is the list of expected reverse-proxy servers. If a list is supplied, any host not on the list will be denied access.

   Note: Earlier, eDiscovery Platform only supported IPv4 address format. Starting with 9.0.1, eDiscovery Platform supports IP addresses in IPv4 and IPv6 formats. If IPv6 format is used, then it must be enclosed in square brackets as shown in this example: [fd74:128f:f0b1:901f:1111:2222:3333:4444].

Next Steps

- To verify header-based authentication is set correctly, add a user account to the eDiscovery Platform and then attempt to access the eDiscovery application through the reverse-proxy SSO server using this account. You should be granted access.

Configuring SAML 2.0 based authentication with trusted Identity Provider

Starting with release 10.0, eDiscovery Platform supports a new way for enterprise Single Sign-On (SSO) authentication with SAML 2.0 compliant Identity Providers (IdPs).

With SAML protocol, an Identity Provider (IdP) authenticates users and provides the authenticated user identity information to a Service Provider (SP). The IdP authenticates the users once and then allows access to multiple applications and services without additional sign-ins. Most modern IdP also support multi-factor authentication (MFA). Support for SAML 2.0 is more commonly used to help enterprise users sign in to multiple applications using single login.

Note: For enhanced security, eDiscovery Platform Server forces the user to authenticate again from IdP by default. This behavior can be customized to not force a user to re-authenticate again for eDiscovery Platform Server if they have already authenticated with the IdP once.

The Service Provider does not directly interact with the Identity Provider as a browser carries out all the redirections. A user presents the authentication details directly with the trusted IdP, and those will never be shared with the Service Provider at any stage.

Note: eDiscovery Platform Server does not need to have direct access to the Internet, to be able to integrate with trusted IdP.

To set up SAML 2.0 based authentication with trusted Identity Provider (IdP):

The properties to enable SAML-based authentication are set using the Property Browser Support Feature. All property changes related to enterprise authentication should be made using the Property Browser. The Property Browser automatically updates the appliance each time you add a new property.

Perform the following steps to set up the SAML-based authentication:

- Step 1: Register a new application in Identity Provider with the details about eDiscovery Platform Server
- Step 2: Configure the required properties in eDiscovery Platform

Note: In case of a clustered eDiscovery Platform environment, all of these steps must be performed on each eDiscovery Platform server.

Step 1: Register a new application in Identity Provider with the details about eDiscovery Platform Server

eDiscovery Platform works with several Identify Providers, such as okta, Microsoft Azure, AWS, and so on. The following steps use the okta IdP; the steps to register a new application in Identity Provider vary based on the IdP you use.

1. Sign in to the Identity Provider administrator portal.
2. Register New Application. During the application registration, if asked, provide the following details:

   A. Name of the App: Veritas eDiscovery Platform

   B. Platform: Web based

C. Sign On Method: SAML 2.0

D. Single sign on URL OR ACS URL: **`https://<your-eDP-server-name-here>/esa/public/SamlSpAssertionConsumer`**

Note: The URL specifies the location where the SAML assertion is sent by the IdP with a HTTP POST. This is often referred to as the SAML Assertion Consumer Service (ACS) URL of the application. This value is needed when you set the esa.saml.sp.acsUrl property as listed in Step 2.

E. Audience URI (SP Entity ID) or Issuer: **`https://<your-eDP-server-name-here>/`**

Note: It specifies the application-defined unique identifier that is the intended audience of the SAML assertion. This is most often the SP Entity ID of the application. This value is needed when you set the **`esa.saml.sp.entityid.issuer`** property as listed in Step 2.

F. Application username or User name in assertion’s subject Statement. It indicates the email address of the user.

Note: Ensure that the Response configuration is such that the “SAML Response” and the “Assertion in the response” must be signed using Signature Algorithm "RSA-SHA256".

Note: eDiscovery Platform currently does not support automatic configuration for SAML using MetaData URL. All the configuration details need to be configured manually.

3. Once the application is registered, note down the following values of the registered application:

   A. **Identity Provider Single Sign-On URL value**: The location where the SAML request will be sent to the IdP with a HTTP POST. This value is needed when you set the **`esa.saml.idp.ssoDestUrl property`** as listed in Step 2.

   B. **Identity Provider Issuer value**: The unique identifier of the registered application in IdP, that is the intended source who sends the SAML assertion. This is most often the IdP Entity ID of the application. This value is needed when you set the **`esa.saml.idp.entityid.issuer`** property as listed in Step 2.

   C. Download the certificate of your registered application, and save the cert file somewhere on your eDiscovery Platform server. If multiple formats of the certificate are presented for download by the IdP, then choose the Base64 Certificate format for download.
   For example: **`D:\eDP\IDPCert\okat.cert`**

   The path of IdP Cert file, located on eDiscovery Platform server.
   This value is needed when you set the **`esa.saml.idp.certificate-CerFile.Path`** property as listed in Step 2.

4. Assign permissions to all the required users who should be allowed to access eDiscovery Platform.

   Note: A matching user account with the same user name must exist in the eDiscovery Platform server for the SSO to work.

Step 2: Configure the required properties in eDiscovery Platform

1. Using an account with System Management permissions, log onto the eDiscovery Platform web interface.

2. From the **System** > **Support Features**, select the **Property Browser**.

3. Using the Property Browser, configure the required set of properties to enable SAML 2.0 based authentication with trusted Identity Provider (IdP).

   – Property: **`esa.saml.sp.acsUrl`**
   Value: The value for this property must be the same as the value mentioned in step 2d above.

   – Property: **`esa.saml.sp.entityid.issuer`**
   Value: The value for this property must be the same as the value mentioned in step 2e above.

   – Property Name: **`esa.saml.idp.ssoDestUrl`**
   Value: The value for this property must be the same as the value mentioned in step 3a above.

   – Property Name: **`esa.saml.idp.entityid.issuer`**
   Value: The value for this property must be the same as the value mentioned in step 3b above.

   – Property Name: **`esa.saml.idp.certificateCerFile.Path`**
   Value: The value for this property must be the same as the value mentioned in step 3c above.

   You might need to configure the following optional properties in specific scenarios:

   – Property Name: **`esa.saml.sp.samlAuthRequest.forceAuthentication`**
   Value: By default, the value is set to **`true`**, which indicates that the user should be forced to authenticate every time with IdP when they access the eDiscovery Platform web application.
   If the value is set to **`false`**, the user will be asked to login only once with IdP to access all supported application including eDiscovery Platform.
   For example, if the user has already authenticated with IdP once to access some application, and now when that user opens another tab in the same browser, and try to access eDiscovery Platform web application, the user will not be forced to log-in again with IdP, and will be signed in to eDiscovery Platform directly.

   – Property Name:
   `esa.saml.idp.samlResponse.useridAssertion.AttributeName`
   Value: IdP lets the SP know who the authenticated user is under the “subject” section of SAMLResponse XML data.
   The value of the subject is generally in text format. In this case, it is not required to set the value of this property explicitly, as the default value is “subject”.
   However, some IdP send the asserted user identity in non-text format; for example, in “transient” or “persistent” name-ID format. Such value cannot be used by eDiscovery Platform to map that user with eDiscovery Platform user. In such a case, IdP can be configured to return additional information about the authenticated user using

"attribute statements". Under such a scenario, the value of this property should be set with the exact "AttributeName" string, using which eDiscovery Platform matching username value is being sent by the IdP. Contact Veritas Support for more help.

Note: Once these properties are set, the eDiscovery Platform services must be restarted to take effect.

4. Enable SAML authentication by setting **`esa.saml.enabled`** to **`true`**.

   By default, the value is set to **`false`** which sets SAML disabled by default.

   Note: Before you set the value to true to enable SAML authentication, ensure that all properties listed in the step 3 are set. Also, eDiscovery Platform server must be configured to be accessed via HTTPS protocol.

Automatic User Creation and Role Assignment

See the following topics in this section:

- *"Automatic User Creation" on page 56*
- *"Automatic Role Assignment" on page 56*

Automatic User Creation

This feature is not enabled by default. When eDiscovery Platform LDAP integration is configured to create unknown users automatically:

- Created users are stored with empty passwords. Should LDAP be disabled, these eDiscovery Platform accounts will still exist, but they will not be accessible because you cannot log in with an empty password. Should an administrator desire to modify or edit these accounts while LDAP is disabled, they will need to provide the user with some non-empty password.
- By default, the eDiscovery Platform will set case access for the user to all cases. This can be controlled via a comma-separated list of case names like:
  `esa.ldap.newUserCaseList=case1, case2`
- Newly-created users will always be assigned their role based on the same logic that is described below for automatic role assignment.

Automatic Role Assignment

This feature is not enabled by default. When configured, LDAP-authenticated users are assigned a role based on their first matching LDAP role that starts with the prefix 'Clearwell ' (note the space at the end).

```
esa.ldap.useLDAPRoles=
```

The prefix can also be modified by using:

```
esa.ldap.rolePrefix=
```

When LDAP is enabled, if there is no LDAP matching role, the user will be given a configured default Role. If there is no matching role and no default role, login will be denied.

```
esa.ldap.defaultRole=
```

Secure LDAP SSL/TLS Support

The eDiscovery Platform can be configured to communicate over SSL/TLS while performing LDAP authentication. Starting with eDiscovery Platform 9.5, TLS 1.0 is no longer supported, and TLS 1.2 must be enabled.

To enable LDAP communication over SSL/TLS, set the `connectionURL` property (URL to the LDAP server) to: `ldaps://host:636`. The format is *ldaps://hostname[:port]*) and, in this example, the connection to the host is over the default secure LDAP port 636.

A valid certificate must be exported from the Domain Controller that is being used for LDAP authentication. Please consult your IT department for more information.

Starting with release 10.0, the keystores and truststores of BCFKS type are used instead of JDK cacerts truststore. The cacerts.bcfks file and the JDK's cacerts file are available in the same directory.

- The host's root CA certificate
- The host's intermediate certificate (if applicable)
- The host's SSL/TLS certificate

Note: Re-installation of these certificates may be required during a platform upgrade that modifies the version(s) of the JDK/JRE.

Tip: Save backup copies of the cacerts keystore before modifying them with the keytool.

Example Certificate Import

To import the root certificate

1. Go to the JDK directory.
   `cd c:\jdk-8u291-windows-x64\jre\lib\security`
2. Run the keytool command.

```
> c:\jdk-8u291-windows-x64\bin\keytool.exe

-import -trustcacerts -alias rootCA

-file c:\temp\LDAP_rootCA_cert.der -keystore cacerts
```

3. Enter the keystore password.
4. If the certificate already exists in the keystore under alias <rootCA>, you will be prompted whether to add it. Enter **`no`**.

To import the intermediate certificate

1. Go to the JDK directory.
   `cd c:\jdk-8u291-windows-x64\jre\lib\security`
2. Run the keytool command.

```
> c:\jdk-8u291-windows-x64\bin\keytool.exe
```

```
-import -trustcacerts -alias LDAPintermediateCA

-file c:\temp\LDAP_intermediateCA_cert.der -keystore cacerts
```

3. Enter the keystore password.

To import the ldapssl certificate

1. Go to the JDK directory.
   `cd c:\jdk-8u291-windows-x64\jre\lib\security`
2. Run the keytool command.

   ```
   > c:\jdk-8u291-windows-x64\bin\keytool.exe

   -import -trustcacerts -alias ldapssl

   -keystore cacerts -file c:\temp\LDAPhost_cert.der
   ```
3. Enter the keystore password.

Additional Configuration Examples

Because Active Directory (AD) exposes an LDAP listener, it is possible to communicate with AD via LDAP.

- Access for all Corporate Accounts
- Access via a Corporate Domain
- LDAP Configuration Property Example

Managing encrypted connection with MySQL

eDiscovery Platform 10.0 and later comes with an updated version of MySQL 5.7.xx that supports encrypted connections between clients and the server using the TLS (Transport Layer Security) protocol. By default, the connection between the eDiscovery Platform and MySQL server is not encrypted. The system administrators can enable encrypted communication by performing additional configuration steps. Please note that encrypted communication between the eDiscovery Platform and MySQL results in performance degradation in some eDiscovery workflows. So the decision to enable or disable encryption should be based on your business requirements.

To enable encrypted communication, you need to perform the following steps:

1. Configurations on the MySQL server
2. Configurations on the eDiscovery Platform server

Configurations on the MySQL server

You need the following files for enabling TLS on the MySQL server:

- **ssl_ca**: The path name of the Certificate Authority (CA) certificate file.

- **ssl_cert**: The path name of the server public key certificate file. This certificate is presented to the client to be validated against the CA certificate that it has in its truststore.
- **ssl_key**: The path name of the server private key file.

When you have these three files, update the MySQL's config file (***my.ini***) to include the following settings under the [***mysqld***] section, and then restart the MySQL server.

```
ssl-ca = "C:\mysqlCerts\ca-cert.pem"
ssl-cert = "C:\mysqlCerts\server-cert.pem"
ssl-key = "C:\mysqlCerts\server-key.pem"
```

Auto-generated certificates and keys created by the MySQL server are self-signed. These certificate files are present in *D:\MySQLData\data*. If you want to use your self-signed certificates, you must provide those in MySQL's config file.

Verify if TLS has been configured on the MySQL server. To do this:

1. Open command prompt.
2. Run the command: ***mysql -u root -p***
3. Enter password when prompted.
4. Run a query ***show global variables like '%ssl%';***

   The output should show ***have_openssl*** and ***have_ssl*** as ***YES***.

Configurations on the eDiscovery Platform server

The configuration steps on the eDiscovery Platform varies depending on whether you use a CA certificate or a self-signed certificate.

When a CA certificate is used:

Perform the following steps:

1. ***Using a CA certificate***: If no additional configurations are made regarding the server authentication, Java verifies the server certificate using its default truststore (*$JAVA_HOME/lib/security/cacerts*).
   You only need to configure the MySQL server using the *ssl_ca*, *ssl_cert*, and *ssl_key* parameters in its config file as described in *"Configurations on the MySQL server" on page 58*.
2. Set the system property ***esa.common.db.useSSL*** to ***true*** using **System** > **Support Features** > **Property Browser**. By default, this property is set to ***false***, disabling the encrypted communication.

When a self-signed certificate is used

Note: When using the eDiscovery Platform in the Distributed Architecture environment, you must perform the following steps in the primary node and all secondary nodes.

To verify the server certificate, eDiscovery Platform must be able to read the certificate that signed itself or the self-signed CA certificate. This can be accomplished by either importing the certificate (ca-cert*.pem* or any other certificate) into the Java default truststore or importing it into a custom Java truststore file and then configuring the eDiscovery Platform accordingly. You must import the CA certificate for both the truststore's cacerts and cacerts.bcfks.

To import the CA certificate (ca-cert.pm) file in java truststore for both cacert and cacert.bcfks, do the following:

- Run the keytool command:

```
keytool -importcert -alias <certificate alias name (user friendly name)> -
file <path of certificate file> -keystore <path of cacerts> -storepass
<keystore password usually changeit>
```

- Run the keytool command:

```
keytool -importcert -alias <certificate alias name (user friendly name)> -
file <path of certificate file> -keystore <path of cacerts.bcfks> -
storepass <keystore password usually changeit> -storetype bcfks -
providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -
providerPath <path of ccj jar>
```

For example:

```
keytool -importcert -alias MySQLCACert -file ca.pem -keystore C:\jdk-
8u291-windows-x64\jre\lib\security\cacerts.bcfks -storepass changeit -
storetype bcfks -providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -
providerPath C:\jdk-8u291-windows-x64\jre\lib\ext\ccj-3.0.1.jar
```

After importing the CA certificate (ca-cert.pm) file in java truststore for both cacert and cacert.bcfks, set the system property ***esa.common.db.useSSL*** to ***true*** using **System** > **Support Features** > **Property Browser**. By default, this property is set to ***false***, disabling the encrypted communication.

Access Groups

The eDiscovery Platform provides access groups as a way to organize users and control resources and functions. One of the prime reasons to organize users into specific access groups is as a security measure.

Access groups are collections of users that can be collectively assigned privileges associated with the group for easy security maintenance. For example, you can create different access groups for different departments or types of reviewers and give the users in each access group appropriate access to the data they require for their work.

An administrator can use access groups to help control and restrict user access to Cases, Legal Holds, Sources (Collections), Collection Sets (Collection Destinations in 8.1), and Locations (access to physical location on server for exports, collections or both). Your organization should create and add unique access groups in accordance with specific access and security needs.

For details on access group setup for legal hold and collection sets (sources), see the Legal Hold User Guide and Identification and Collection Guide.

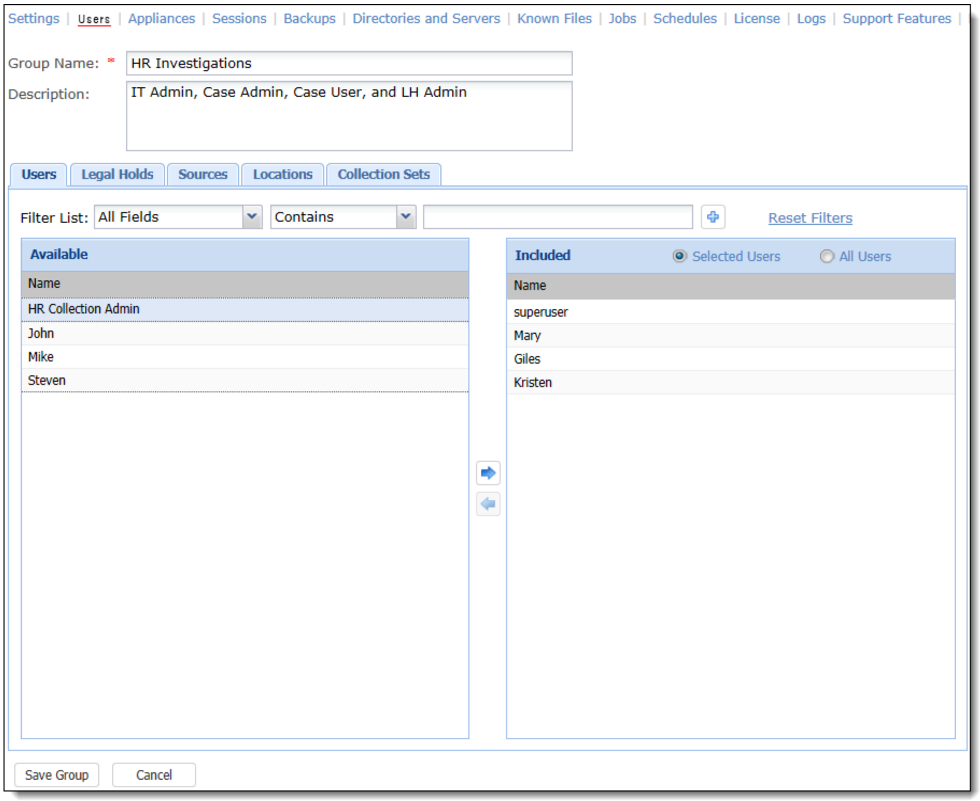
Considerations

- When a user is not added in any access group, then all cases, Legal Holds, sources, locations and collection sets that are not added in any access group are available to the user. Users, sources, locations, and Legal Holds are considered as open to all resources when they are not associated with any access group.
- When a new case, Legal Hold, source, locations and collections sets are created, they become a member of all Access Groups. If you have upgraded Veritas eDiscovery Platform from an earlier release, then all Legal Holds, sources, locations and collection sets are open to all users until the Access Groups permissions are enforced.

  Note: After upgrade from 8.1.1 to 8.2, Case Authorized users will not be affected unless they are also associated with an Access Group. In that case, their group association will be removed. Changes that happen as a part of the upgrade process are reported in the upgrade logs. See the Upgrade Guide for more information on logging and reporting.
- Consider access group naming conventions to allow for easy searches and to identify an access group’s purpose. If the purpose of your access group is to allow members of a particular work group, agency or department to have access to certain locations and not to others, it may be useful to create access groups along departmental lines or according to a particular business need and access mode for the work need (for example, type of reviewer: lead, temporary or contractor).

Creating and configuring a new access group

To create an access group, you must have the role of administrator with the System Administrative Settings of **Allow user management** and **Allow group management**. See *“Allow user management—****A****llow the user to add or edit non-system administrative accounts.” on page 26*.


Settings | Users | Appliances | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | License | Logs | Support Features |
Users
Legal Holds
Sources
Locations
Collection Sets
Reset Filters
Save Group
Cancel

Group Name: * HR Investigations

Description: IT Admin, Case Admin, Case User, and LH Admin

Filter List: All Fields Contains

Available
Name
HR Collection Admin
John
Mike
Steven

Included ● Selected Users ○ All Users
Name
superuser
Mary
Giles
Kristen

To add an access group

1. In the System view, click **Users**

2. Click the **Access Groups** tab to view the list of access groups

3. (Optional) Consider using the Search filter to locate existing access groups by name and description. It may be useful to search for existing access groups to help you determine how to name your access group.

4. Click **Add** to open the **Add Access Group** menu.

5. Specify the following information. An asterisk (*) indicates a required field.

Access Group Options

Field	Description
Group Name*	Enter a name for the new group. The group name must be unique (up to 35 characters). Consider using a consistent access group naming convention for easy group name searches and for quickly identifying the type or purpose of the access group.
Description	Enter a description for the group. (up to 255 characters)
Users	All existing Group Access users are listed in the **Available** column. To include specific users, select the **Selected Users** option, and then select the appropriate users in the **Available** column, and click the right arrow to move them to the **Included** column. **Note:** Take care to only add users that are authorized to access the resources that are associated with the group. A user created with **Group** Access can access only the cases, legal holds, sources, and locations that are added in the access groups to which the user belongs. By contrast, Users who are created with **Case** Authorization cannot be a part of a group. For more information about user creation with Group Access or Case Authorization, see *"Defining User Accounts" on page 15*.
Cases	All cases are listed in the **Available** column. To add a case to the group, move it to the Included column. **Note:** Group Access users can access only those cases that are added in the access groups to which they belong.
Legal Holds	All existing legal holds are listed in the **Available** column. To include specific legal holds, select the Selected Legal Holds option, and then select the appropriate legal holds in the **Available** column, and click the right arrow to move them to the **Included** column. **Note:** Group Access users can access only those legal holds that are added in the access groups to which they belong.
Sources	All existing sources are listed in the **Available** column. To include specific sources, select the **Selected Sources** option, and then select the appropriate sources in the **Available** column, and click the right arrow to move them to the **Included** column. **Note:** Group Access users can access only those sources that are added in the access groups to which they belong.
Locations*	All physical locations are listed in the **Available** column. If you need to add a physical location to those listed in the column, see *"Adding a location" on page 66*". To include specific locations, select the **Selected Locations** option (upper right corner of the **Included** pane), and then select the appropriate locations in the **Available** column, and click the right arrow to move them to the **Included** column. **Note:** Group Access users can only access locations that are added in the access groups to which they belongs.

Access Group Options

Field	Description
Collection Sets	By default, all existing collection sets for which the user has access and any global collection sets appear in the **Available** column. You must manually move the collection sets to the **Included** column so the collection sets are only used by the users who are members of this access group. If you do not specify a collection set for an access group, then the users from this access group will not have access to any of these collection sets. This means that these users will have access to the global collection sets which are not part of any access group. For details on how to work with collection sets for access groups, see *"Managing Collection User Accounts" in the Identification and Collection Guide*.

6. Click **Save Group**.

Deleting an access group

1. In **System** view, click **Users** and then click the **Access Groups** tab.

2. Click the trash icon for the access group and then in the **Delete confirmation** dialog, click **Yes** for. The access group is removed.

   Note: Roles created by an administrator can be deleted from the **Roles** tab, but not the system default roles. For more about roles, see *“Defining User Roles” on page 20*.

Locations

Both collection and export operations have the ability to store data to a physical location on disk. You can manage data security for these operations by controlling which users have access to which locations. Access to locations depends on the access group privileges that you grant users. Before you set up a user with location privileges, you must add the location and specify a location type.

For details on collection (sources) locations, see Identification and Collection Guide.

Export Locations Control

You can create export locations and allocate access groups to them, so that you can restrict access to a number of user accounts all at once.

The eDiscovery Platform uses the locations of type Export Only feature for the following operations:

Note: Locations are also used in the collection side as “Collection Destination”.

Production

- Metadata Exports
- Production Export
- Native Only Export

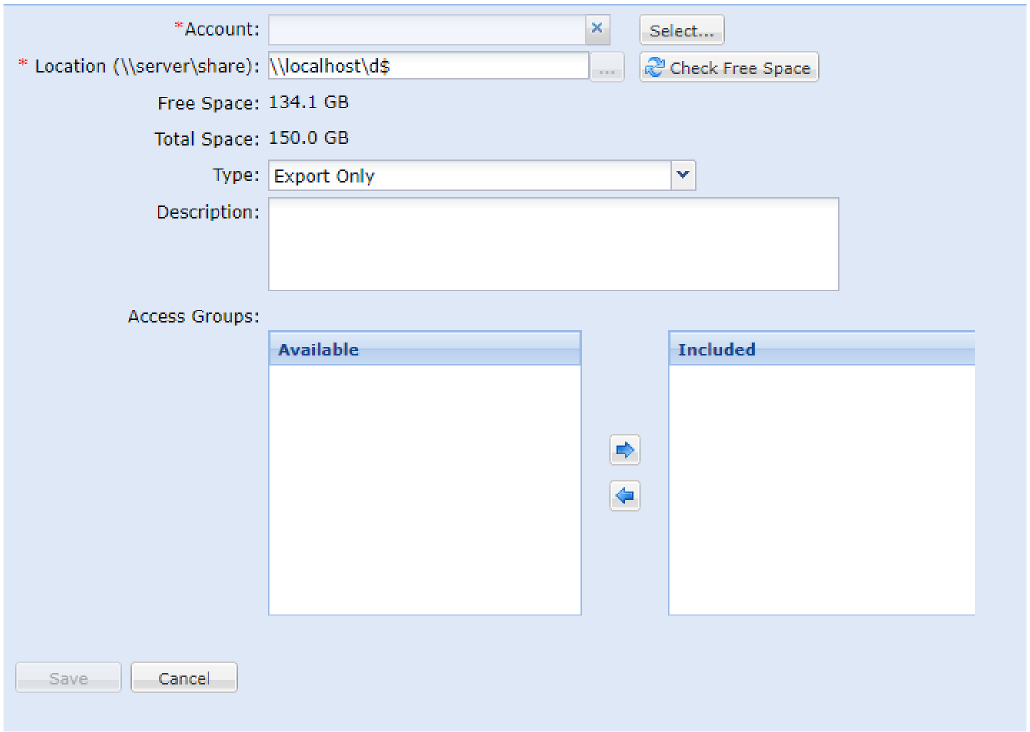
Processing

- Imaging & Rendering
  - Export Natives
- Exceptions
  - Export Current Documents
  - Export All Documents

Analysis & Review

- Print (Search results)

Adding a location


*Account:

* Location (\\server\share): \\localhost\d$

Free Space: 134.1 GB

Total Space: 150.0 GB

Type: Export Only

Description:

Access Groups:

To add a location

1. From the **All Cases** view, click **Locations**.
2. In the add location pane, specify the following information. An asterisk (*) indicates a required field.

Location Options

Field	Description
Account	Enter the name of the source account you created or click **Select...** to open the Account dialog box to choose an account and click **Save** to close the Account dialog box and return to main Location menu dialog.
Location*	Enter the path to the location where the collected data or export will be stored. Click the **...** button to open the **Directory Browser** dialog box to select a File Share directory or enter a remote directory. Click **OK t**o close the **Directory Browser** and return to the Location menu dialog**.** **Check Free Space** — Collections (sources) and exports are stored on disk. You can check the free space of the selected path to make sure there is enough room for the collection, export or collection and exports. The total space and available free space values appear after the Path entry.

Location Options

Field	Description
Type	Enter the type of source that you want to restrict for this location: • **Collect and Export** — This type of Location is used for both Collection and Export. • **Export Only** — This type of Location is used for Export operations only. • **Collect Only** — This type of Location is used for Collection operations only.
Description	Enter a description for the source account (up to 255 characters). The description should clearly identify and distinguish the purpose of the source account for easy administration purposes.
Access Groups	All Access Groups are listed in the **Available** column. To move an access group to the **Included** column or between columns, highlight the access group and click the Right or Left single arrow. Keep only those groups in the **Included** column in which you want to add the location and move all the remaining groups to the **Available** column If a location is not added to any group, then that location will be available to all users

3. Click **Save**.

Editing a location

To edit a location

1. In the **All Cases** view, click the **Locations** tab.
2. Under the **Actions** column, click edit ✎ icon for the location.
3. Modify the location settings and then click **Save**.

Deleting a location

To delete a location

1. In the **All Cases** view, click the **Locations** tab.
2. Under the **Actions** column, click the trash icon for the location.
3. In the **Delete confirmation** dialog, click **Yes**. The location is removed.

Introduction of Processing Only location type

A new **Processing Only** location type is introduced, which is used for processing a case. This location type can be used to add a collection set, a case source folder, or an LFI source. With this enhancement, the access to browse the directories can be restricted.

To enable the Processing Only location type

1. Navigate to **System** > **Support Features** > **Property Browser**.
2. Add the `esa.enable.processingonly.location` property and set it to `True`.

For more details, please contact Veritas Support.

Discovering Archive Sources

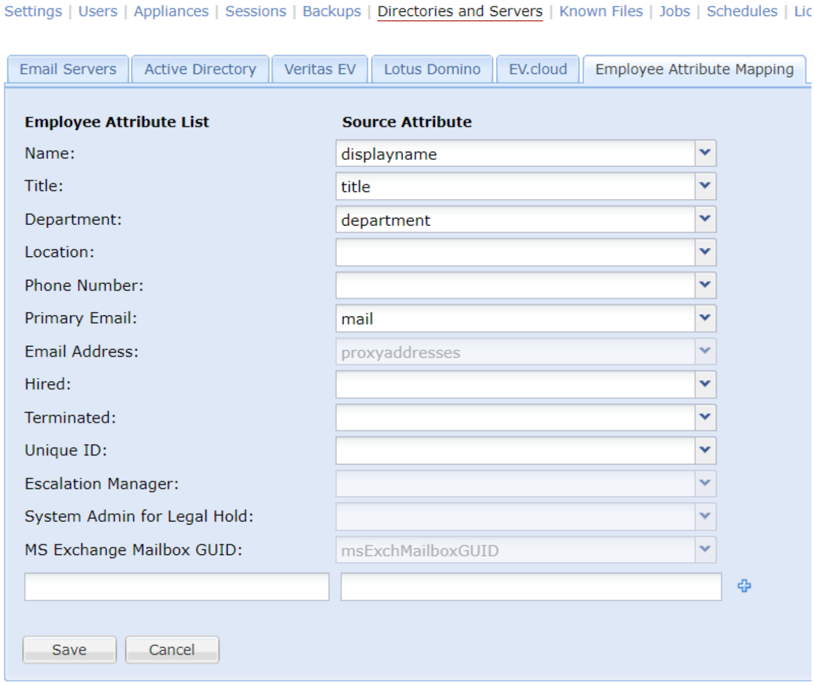
Note: You must have system administrator privileges, with access across all cases to perform all system configurations and archive discovery tasks on the appliance.

For information about how to discover and manage archive document sources, refer to the following topics:

- *"Employee Attribute Mapping" on this page*
- *"About Active Directory Discovery" on page 70*
- *"About Discovering Veritas Enterprise Vault Sources" on page 70*
- *"About Discovering Lotus Domino Sources" on page 70*

Employee Attribute Mapping

Accessed from **System > Directories and Servers > Employee Attribute Mapping**, the functionality on this tab allows the user to map the specific Active Directory Employee Attributes for import into the appliance. The values defined here will control what is pulled in from the active directory.


Settings | Users | Appliances | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | Lic
Email Servers
Active Directory
Veritas EV
Lotus Domino
EV.cloud
Employee Attribute Mapping
Save
Cancel

Employee Attribute List	Source Attribute
Name:	displayname
Title:	title
Department:	department
Location:	
Phone Number:	
Primary Email:	mail
Email Address:	proxyaddresses
Hired:	
Terminated:	
Unique ID:	
Escalation Manager:	
System Admin for Legal Hold:	
MS Exchange Mailbox GUID:	msExchMailboxGUID

- Enter the source attributes here by typing in the relevant fields as they are defined in the active directory.
- Additional Employee Attribute List - Source Attribute pairs can be added and defined by clicking on the plus sign.

- When you import the custodians their employee attributes will be preserved.

Note: Attribute mapping can be used to import data from other sources of employee data through CSV or Script Imports. The fields which will be referenced in the CSV/script import are the ones present on the Employee Attribute Mapping page.
For details about Employee attribute mapping, see *"Setting up Data Sources" in the Identification and Collection Guide*.

About Active Directory Discovery

The Active Directory (AD) crawler discovers your Microsoft Exchange servers, the mailboxes on each server, and your organizational data, such as physical locations and departments (groups). The appliance must belong to a Windows domain for the AD crawler to run. To schedule the AD discovery to be run periodically, see *"Managing Schedules" on page 71*.

To index the documents on a discovered Exchange server, the server must be added to a case (see *"Defining New Cases" Case Administration Guide*).

For details, see "Securing Source Credentials" and *"Setting up Data Sources" in the Identification and Collection Guide*.

About Discovering Veritas Enterprise Vault Sources

To schedule the EV discovery to be run periodically, or to limit the appliances that can access a discovered archive, see *"Managing Schedules and Jobs" on page 71*. To index the documents on a discovered vault, the vault must be added to a case (see *"Defining New Cases" Case Administration Guide*).

For detailed information on performing EV discovery, see *"Setting up Data Sources" in the Identification and Collection Guide*.

About Discovering Lotus Domino Sources

To schedule discovery on the Lotus Domino source to be run periodically, or to limit the appliances that can access a discovered archive, see *"Managing Schedules and Jobs" on page 71*. To index the documents on a discovered source, the source must be added to a case (see *"Defining New Cases" in the Case Administration Guide*).

For details, see "Securing Source Account Credentials" and *"Setting up Data Sources" in the Identification and Collection Guide*.

Managing Schedules and Jobs

For information about how to manage schedules and jobs, refer to the following topics:

- *“Managing Schedules” in the next section*
- *“Viewing Jobs and Accessing Exported Files” on page 74*

Managing Schedules

On the **Schedules** screen you can schedule several types of tasks depending on your view:

- From **System > Schedules** view, you can schedule the discovery tasks for Active Directory, Enterprise Vault, Lotus Domino, and EV.cloud sources. You can also schedule a bulk source, custodian import task or a system backup task. For more information about system and case backups, see *“Backup and Restore” on page 127*.
- From **Case Home > Schedules** view, you can schedule case jobs (including change, disable, or delete any schedule, such as document processing schedules for specific cases), and a case custodian email digest task. For more information, refer to *"Managing Case Schedules and Jobs" in the Case Administration Guide*.

To manage schedules from System view

1. From the **System** view, click **Schedules**.
2. Use the **Show** menu to view all schedules, just the system schedules, or schedules for a selected case.

   Note: By default, all schedules display.

3. To enable or disable a schedule, select the check box next to the schedule(s), and click the **Enable** or **Disable** button.

   The **Scheduled Time** column shows the first scheduled run time. The **Case or Source** column shows a name only for document processing or discovery schedules. If a task has never been run, the **Last Run** column will be blank.

   Note: To select all jobs, click the check box in the header row.

4. To change a scheduled job, select the job type (the job type cannot be changed).

   Note: For a document crawler job, you can change the maximum job duration and the document sources to be crawled.

5. To delete a schedule, click the delete icon, 🗑 , associated with the schedule.

To create a new schedule

1. Click **Add**.

2. Specify the following information. An asterisk (*) indicates a required field. (The Scope will always be “System” in System view.)

Schedule Properties

Field	Description
Description	Enter a description of the job (up to 255 characters).
Task Type	Select the **Backup** task or a discovery job for an Active Directory, Lotus Domino, or Veritas Enterprise Vault or EV.Cloud site. You can also select Bulk Source Import or Bulk Custodian import options.
Initial Run Date*	Specify the date of the first execution of the job: • Click 📅, and select a month and day. or • Enter the date directly as: MM/DD/YYYY. **IMPORTANT**: The first time the Active Directory discovery job is run, the job must be allowed to finish before a document processing job is run for any case. In general, run the discovery and processing jobs daily or weekly— first the discovery jobs, then the document processing jobs for each case. To ensure that all new documents are processed, do not schedule the discovery and document processing jobs to run at the same time.
Start Time*	Enter the start time in 24-hour format (HH:MM).
Frequency	Select a recurring schedule (**Once**, **Daily**, or **Weekly**).
Backup tasks **Note:** Files requiring conversion during processing are not automatically backed up or restored by this backup. These files should be backed up separately. For more information about system and case backups, see *“Backup and Restore” on page 127*.	
Cases to backup	For a backup job, select one of the following options: • **All cases at the time of the backup**. Backs up all cases (the default). • **Selected currently available cases**. Allows you to select zero or more cases to be backed up.
System backup	Select the check box to back up the primary appliance system files after the cases are backed up (recommended). The cluster will be unavailable while the system backup is running.
Collections, Data Map backup	Select the check box to back up collections and sources in the data map for all cases, or selected case(s) on the appliance.
Backup name*	Enter a name for the backup (up to 100 characters).
Bulk Import tasks (Source or Custodian)	
Import Script File*	Enter, or click **Browse** to assign the script file to be used for either a scheduled bulk Source or Custodian import.

3. Click **Save** to submit the new schedule, or click **Cancel** to discard your changes.

Scheduling Case Custodian Email Digest and Document Processing Tasks

- Create a case custodian email digest or document processing task from **Case Home >Schedules** using the “Add” button.
- Modify or reschedule an existing case custodian email digest or document processing task by selecting it from **System > Schedules.**

To schedule an email digest or process documents task

1. Click **Add**.
2. Specify the following information. An asterisk (*) indicates a required field. (The Scope will always be the selected Case in Case Home view.)

Schedule Properties

Field	Description
Description	Enter a description of the job (up to 255 characters).
Task Type	Select **Process Documents** or **Case Custodian Email Digest**.
Initial Run Date*	Specify the date of the first execution of the job: • Click 📅, and select a month and day. or • Enter the date directly as: MM/DD/YYYY. • If you choose a start date, you will need to choose a stop date.
Start Time*	Enter the start time in 24-hour format (HH:MM).
Frequency	Select a recurring schedule (**Once**, **Daily**, or **Weekly**).
Max Duration* (**Process Docs** Only)	Choose limited or unlimited. Default is unchecked = limited. Checking “Unlimited” removes the **Stop Date** field and requires choosing a number of occurrences.
Stop Date (**Process Docs** Only)	Choosing “Limited” for **Max Duration** requires choosing a **Stop Date**.
Stop Time (**Process Docs** Only)	Enter the stop time in 24-hour format (HH:MM).
End After (**Process Docs** Only)	Number of occurrences entry is available only if the **Max Duration** “Unlimited” box is selected.
Sources (**Process Docs** Only)	Highlight the source locations. Hold down the shift key to select multiples.
Send To (**Case Custodian Email Digest** only)	Enter an email address to receive the case custodian digest email for the case.
Enabled	Deselect the box to disable the rule.

3. Click **Save** to submit the new schedule, or click **Cancel** to discard your changes.

Viewing Jobs and Accessing Exported Files

On the Jobs screen, you can stop jobs that are still running, and delete jobs that are completed or stopped. You can access jobs in different ways, in one of two views: From the System, or Case Home view.

From the System view, you can see backup and restore jobs; those that pertain to all cases across the system. From there, if you select a case, or navigate to Case Home > Jobs, you will see jobs specific to that case. System, or case-specific jobs (depending on your view) are visible from the Jobs window while the job is currently running.

Case specific jobs can include all jobs for that case, such as exporting, and printing documents, plus any legal hold or identification and collections jobs. (Scheduled jobs are created and managed either from the System > Schedules, or Case Home > Schedules view.) For information on viewing case jobs, refer to *"Managing Case Schedules and Jobs" in the Case Administration Guide*.

For export jobs, users normally download the exported documents from the Jobs window as a single zip file. If the exported documents exceed the specified maximum size (see *"Defining System Settings" on page 90*), you must access the files directly on the appliance. Click ℹ in the Jobs window to view the export job ID. The exported files can be accessed from: `<esa_root>\data\filemanager\<username>\jobRun-<jobid>` For more information about running and producing export jobs, refer to *"Performing Exports" in the Export and Production Guide*.

To view/manage current jobs:

1. To view jobs from either the System view (across all cases), or within a selected case:

   A. On the top navigation bar, from **All Cases** view, click **System > Jobs**.

   B. On the top navigation bar, with a case selected, click **Case Home > Jobs**. (For more information, refer to *"Managing Case Schedules and Jobs" in the Case Administration Guide*.)

2. To view the job log for a job, from the Jobs window, click 📋 in the status column.

3. To limit the list of jobs displayed, select a user, case, or update time from the **User**, **Context**, and **Jobs updated** menus. Select **System Jobs** from the **Context** menu to view just the backup/restore jobs and email server/archive source discovery jobs. The Jobs window shows system jobs when you are in System view, and shows only case jobs when you are in Case Home view, or search screen.

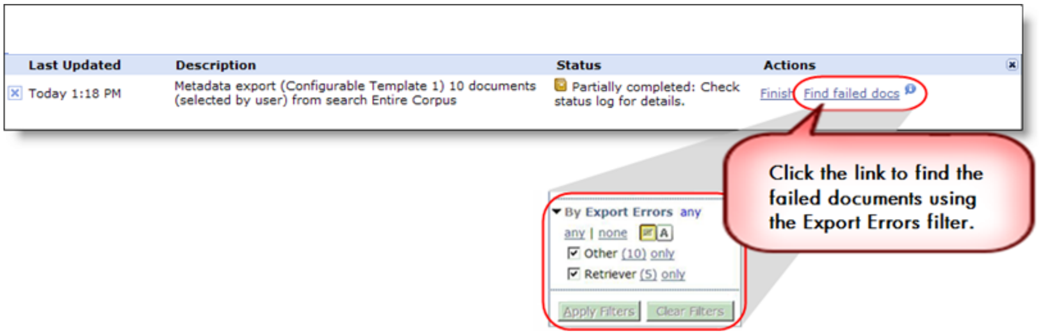
4. To stop a running job, select the check box next to the job, and click **Stop Jobs**.

   When a job is stopped, users can see the status change in the Jobs window. To open the Jobs window, click **Jobs** above the navigation bar. Only users with one or more system administrative privileges can view system jobs in the Jobs window.

5. To delete a completed or stopped job, click 🗑 for the job, or select the check box next to the job, and click **Delete Jobs**. Note that all files associated with a deleted job are also deleted, such as PDF reports and PST zip files, and will no longer be accessible from the Jobs window found above the navigation bar.

6. To view errors, click **Jobs** at the top of the screen.

   If an error occurred while running the job, a warning indicator is shown next to the **Jobs** link. The status of your job displays, with a link to **Find failed docs** under the Actions column. Click to view details for the errors that occurred to each document.



Last Updated	Description	Status	Actions
☒ Today 1:18 PM	Metadata export (Configurable Template 1) 10 documents (selected by user) from search Entire Corpus	Partially completed: Check status log for details.	Finish Find failed docs

Click the link to find the failed documents using the Export Errors filter.

When you click the link, the Export Errors filter appears in the Filter list, displaying the errors by type. This allows you to address the issues before re-running the job. For more information about filtering the export errors by problem type, refer to the section *"Filtering Search Results" in the Veritas eDiscovery Platform User's Guide*.

Managing the eDiscovery Platform

This section describes managing the eDiscovery Platform.

- *“Summary of Additional Administrative Tasks” on page 116*

About the eDiscovery Platform

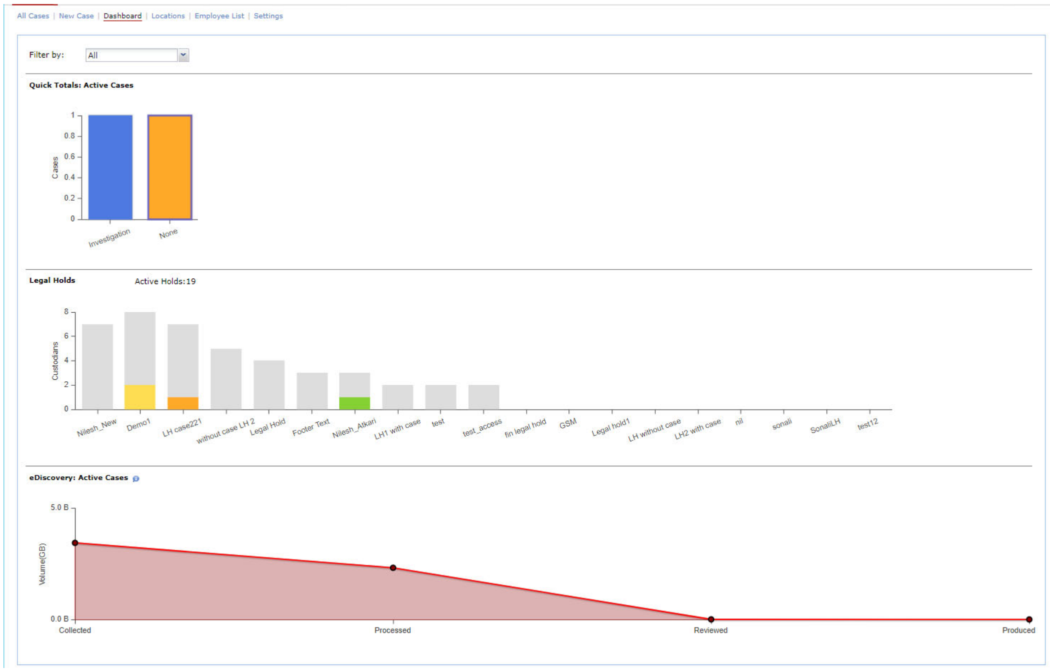
The eDiscovery Platform automates the analysis and review of information stored in Microsoft Exchange servers, email archives, Personal Information Store (PST) files, Lotus Notes Files (NSF), and other information stores.

The platform manages documents by *case*. To define a case, you specify the sources of the documents that you want to index and analyze. The scope of a case can be as broad or narrow as required, and can be updated dynamically as new content is added to the specified sources. You can have many cases active at one time, and each case can be managed independently of other cases, with its own discrete set of documents and access controls.

The Administration User Interface

The 7.x versions employ an enhanced user interface designed to improve case management with an end-to-end workflow within each case. (For more information about mapping 6.x menu items to the newest version, refer to the *Navigation Reference Card*.

From the **All Cases** view, system administrators can also see a single Dashboard view displaying status and activity for all cases across your eDiscovery Platform lifecycle.

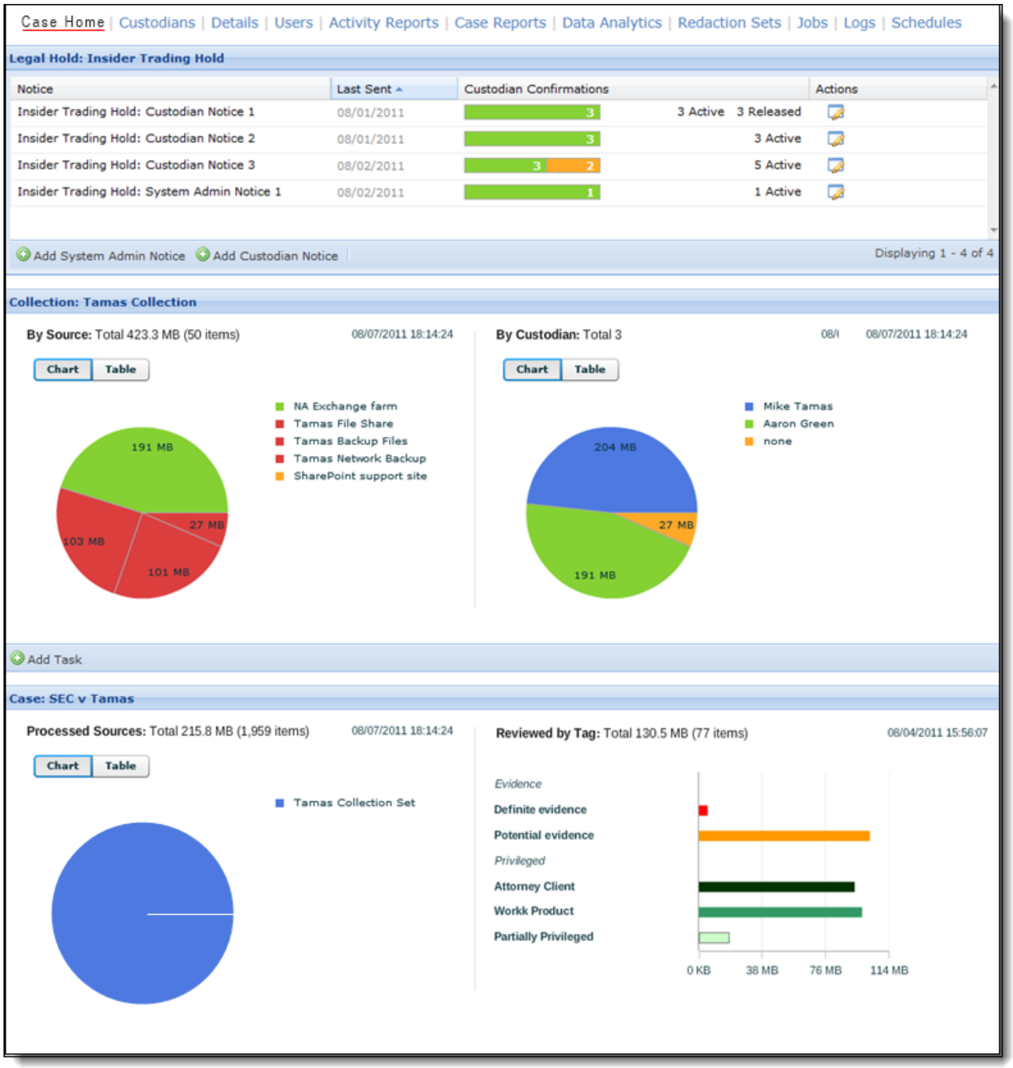


Dashboard status can be filtered by All Cases, or a type of case, and provides the number of cases, active legal holds, and data volumes that have been collected, processed, reviewed, and produced.

Note: The System Manager role has privileges to perform and access case management tasks as well as system management tasks which affect not only the selected case, but all cases (such as the **All Cases**, **All Processing**, and **System** views).

When a case is selected on the top navigation bar, from the **Case Home** view, system administrators can see case details, plus manage all activity for a selected case.

The following example shows three main areas of case activity, starting with the Legal Hold "Insider Trading Hold" for the SEC v Tamas case.



Legal Hold: Insider Trading Hold

Notice	Last Sent ▲	Custodian Confirmations		Actions
Insider Trading Hold: Custodian Notice 1	08/01/2011	3	3 Active 3 Released	✎
Insider Trading Hold: Custodian Notice 2	08/01/2011	3	3 Active	✎
Insider Trading Hold: Custodian Notice 3	08/02/2011	3 2	5 Active	✎
Insider Trading Hold: System Admin Notice 1	08/02/2011	1	1 Active	✎

Add System Admin Notice Add Custodian Notice Displaying 1 - 4 of 4

Collection: Tamas Collection

By Source: Total 423.3 MB (50 items) 08/07/2011 18:14:24

By Custodian: Total 3 08/(08/07/2011 18:14:24

Case: SEC v Tamas

Processed Sources: Total 215.8 MB (1,959 items) 08/07/2011 18:14:24

Reviewed by Tag: Total 130.5 MB (77 items) 08/04/2011 15:56:07

There are a total of four notices for this case, displaying the current status of custodian confirmations. This view also allows the option of adding new legal hold notices, or performing actions on the existing ones.

Collection data displays tasks by source and by custodian, showing the total volume of data collected for each. The bottom box shows the total data volume of sources processed by batch, and review/analysis tags associated with this case.

For more information about mapping administrative functions within the new user interface, refer to the 3-page *Navigation Reference Card*.

Managing Appliances

The appliances can be managed as standalone systems or in cluster configurations.

- **Standalone**. An appliance managed individually requires no additional setup related to other appliances, and the various appliance menus can be ignored.
- **Cluster**. A designated primary appliance can be used to manage multiple appliances. After you define the appliances in a cluster, you can use any appliance in the cluster to administer the other appliances and search any case on any appliance, provided the primary appliance is active and accessible from the appliance where you log in. Cluster operation requires the primary appliance to be available at all times.

  Note: Some cluster configurations may be set up with primary and secondary nodes that share a single database. Refer to the Distributed Architecture Deployment Guide for details.

Initial Configuration of the eDiscovery Platform

Overview: Setting Up an Appliance

This list describes the process of bringing an appliance online.

1. Connect the appliance to your network and configure the network settings and services.
   See *"Configuring the eDiscovery Platform Services" on page 83*.

2. (Optional) Configure the platform to use a Remote Database Management System. See *"Using a Distributed Architecture Deployment" on page 86* for more information.

3. Log in as an administrator.
   See *"Logging In and Out as an Administrator" on page 88*.

   Note: To create a cluster, see *"(Optional) Adding Appliances to a Cluster" on page 89*.

4. Configure the system settings.
   See *"Defining System Settings" on page 90*.

5. Specify an external location where case and system backups are stored.
   See *"Configuring the Backup Location" on page 96*.

6. Review the appliance security issues.
   See *"Secure Windows Server" on page 39*.

7. Install or check your anti-virus software according to platform guidelines.
   See *"Virus Scanning Guidelines" on page 98*

8. Configure the Windows firewall.
   See *"Summary of Additional Administrative Tasks" on page 116*.

Note: Starting in 8.0, if the users need to allow searches for punctuation marks, it needs to be enabled through the property browser. If the users require it, the property needs to be changed before any data is processed. The property is disabled by default.

1. Go to **System > Support Features**, and select **Property Browser**.

2. Enter the name of the property: esa.customtokenizer.display

3. In New Value, enter `True` to display.

4. Click Submit to save your settings. Once enabled, the property can be disabled by entering `False` for the new value.

Setting up a Virtual Appliance

The application can either run on a dedicated appliance, or as a guest operating system on a virtual appliance using VMware. While a number of options are available for running VMware images, Veritas recommends using VMware vSphere ESXi 5.0 or later.

Note: All servers require licensing. Contact your Sales representative to purchase a license, and to discuss additional information depending on your intended use and requirements.

The platform software optimizes the use of resources by dynamically tuning processing speeds based on the amount of memory and number of CPUs available. The following is a typical configuration for a VMware virtual guest.

Important: It is not recommended to run a virtual machine with less than the indicated memory, hard drive, and CPU specifications. This would cause some operations to fail to run. For details on the required hardware configurations, refer to the *Distributed Architecture Deployment Guide*.

Configuring the eDiscovery Platform Services

The following list describes the services that run on the Veritas eDiscovery Platform. Each service must run under a login user account in your Windows domain, and each account must have the appropriate permissions and belong to the local Windows Administrator group.

For detailed information on configuring accounts, see the *QuickStart Guide*.

To configure the eDiscovery services

1. On the appliance, right-click on **My Computer** and select **Manage**.
2. To change a service logon account, select **Services and Applications > Services**, right-click on the service, and select **Properties**.
3. To add an account to the Windows Administrator group, select **Local Users and Groups > Groups**, select **Administrators**, and add the account.

List of eDiscovery Services

`EsaApplicationService:Firedaemon`

Controls the eDiscovery Platform Application Server, which is responsible for indexing the incoming documents and processing search requests. This service depends on the MySQL service. No configuration is required, except in the following cases:

- To crawl PST files or loose files on a network share that requires a username and password, this service must run under a login account with those permissions. The login account must also be a part of the local administrator's group.
- To crawl an Active Directory domain other than the domain of the platform, this service must run under a login account in that domain.

`EsaEvCrawlerService`
`EsaEvRetrieverService`

Responsible for crawling and retrieving documents on Veritas Enterprise Vaults. The login user name must match the name used by the Veritas services (generally the "Vault Service Account").

Note: For more information about collecting data from Enterprise Vault, refer to ""Setting up Data Sources: Veritas Enterprise Vault" in the "Identification and Collection Guide.**EsaExchangeCrawlerService**
EsaExchangeRetrieverService
Responsible for crawling and retrieving documents on Exchange servers. The login user must have the following permissions:

- Read
- Execute
- Read permissions
- List contents
- Read properties
- List objects

- Open mail send queue
- Read metabase properties
- Administer information store
- Create name properties in the information store
- View information store status
- Receive As

`EsaPstCrawlerService`
`EsaPstRetrieverService`

Responsible for crawling and retrieving PST data stores. Note the following:

- If the PST files are on a network share that requires a username and password, these services must run under a login account with read and write access to the network share. The login account must also be a part of the local administrator's group.
- If the PST files are on a storage device attached to the platform, then only local permissions are required.

  Tip: The platform requires different accounts but similar privileges for each of the PST crawler, and retriever services. Setting up separate accounts avoids potential memory contention and management issues with Microsoft's MAPI interface which could result in sub-optimal performance.

`EsaNsfCrawlerService`
`EsaNsfRetrieverService`

Responsible for crawling and retrieving NSF data stores. These services must be configured with the permissions needed to access NSF files over the network, must also be a part of the local administrator's group, and the services should run under the account that installed the eDiscovery application. Note the following:

- If the NSF files are on a network share that requires a username and password, these services must run under a login account with read and write access to the network share.
- If the NSF files are on a storage device attached to the platform, then only local permissions are required.

`EsaPrizmDocServer`
`EsaPrizmApplicationServices`

The service for the PrizmDoc that is invoked to image documents during review, export, and production. These services must be configured with administrative access to the machine.

If Image Helper +Document Converter Service is enabled:

`EsaImageHelper`

The Image Helper service expedites document conversion and handling of typical Microsoft Office documents in native view.

Tip: 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.

Optional for Audio Search License owners:

`EsaNxGridAgent`
`EsaNxGridBase`
`EsaNxGridGateway`

The Grid Agent Service performs search and other CPU-intensive operations like phonetic index creation.

The Grid Base Service manages data storage and communications for Nexidia Search Grid.

The Grid Gateway Service provides the public interface to Nexidia Search Grid.

Optional for Veritas Information Classification users:

`EsaClassifierService`

The Classifier Service allows the eDiscovery Platform to access Veritas information classifier policies using the common interface. The credential for this service is configured at the time of installation or upgrade.

Note: The Case Administration Guide has information on how to set up a case so Information Classification policies will be applied to case data: see *"Information Classification" in the Case Administration Guide*. The User Guide shows how reviewers use classification information in eDiscovery: see*"Classification Information" in the Veritas eDiscovery Platform User's Guide*.

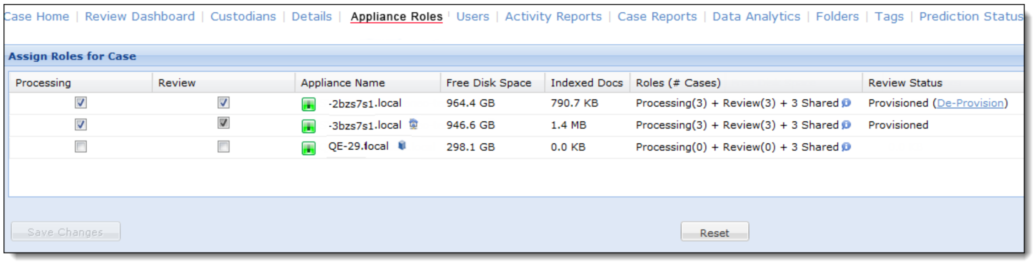
Using a Distributed Architecture Deployment

The appliance can be configured to run in a distributed environment. In a distributed configuration, The eDiscovery Platform uses a dedicated MySQLdatabase located on a separate machine for the underlying database server component which, when coupled with proper assignment and provisioning of appliances, efficiently spreads the review and processing workload across multiple appliances.

Appliances and their roles are viewed and managed from two locations:

- With a case selected, in **Case Home** > **Appliance Roles**.
- In **All Cases** view, in **System** > **Appliances** > [*selected appliance*] > **Appliance Roles**.

Case-Level: Review and Processing Assignment



Case Home | Review Dashboard | Custodians | Details | Appliance Roles | Users | Activity Reports | Case Reports | Data Analytics | Folders | Tags | Prediction Status
Assign Roles for Case
Save Changes
Reset

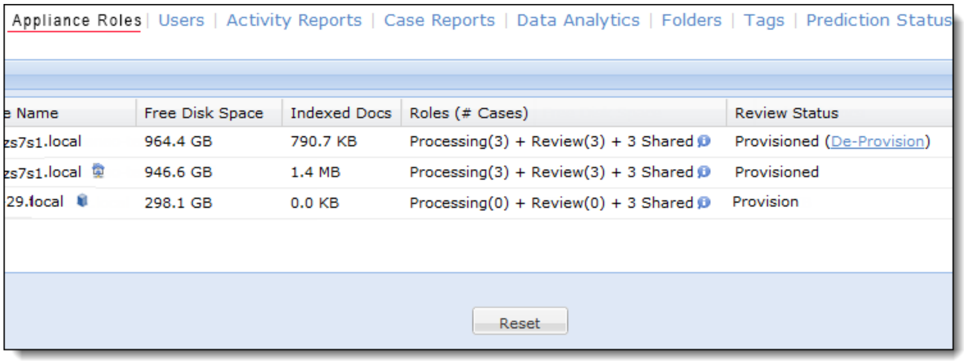
Processing	Review	Appliance Name	Free Disk Space	Indexed Docs	Roles (# Cases)	Review Status
☑	☑	-2bzs7s1.local	964.4 GB	790.7 KB	Processing(3) + Review(3) + 3 Shared	Provisioned (De-Provision)
☑	☑	-3bzs7s1.local	946.6 GB	1.4 MB	Processing(3) + Review(3) + 3 Shared	Provisioned
□	□	QE-29.local	298.1 GB	0.0 KB	Processing(0) + Review(0) + 3 Shared	

To assign roles from Case Home, check the box next to one or more appliances you want to assign (for each case) the **Review** and/or **Processing** role. To return to previous settings, click the **Reset** button.

For more information, and to set up and configure your appliances to use a distributed architecture model, refer to the *Distributed Architecture Deployment Guide*.

Case-Level: Provisioning

To assign review and processing appliances to be used immediately without running another processing job, you can provision appliances manually using the **Provision** link in the *Review Status* column.



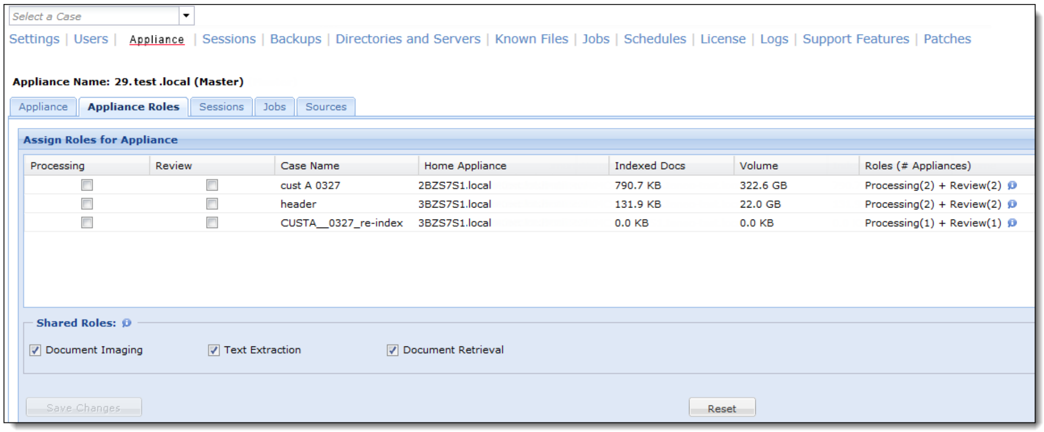
Name	Free Disk Space	Indexed Docs	Roles (# Cases)	Review Status
zs7s1.local	964.4 GB	790.7 KB	Processing(3) + Review(3) + 3 Shared	Provisioned (De-Provision)
zs7s1.local	946.6 GB	1.4 MB	Processing(3) + Review(3) + 3 Shared	Provisioned
29.local	298.1 GB	0.0 KB	Processing(0) + Review(0) + 3 Shared	Provision

Note: The “Provision” link is only displayed if the review appliance does not have the latest processed data. For example, if Case A does not yet have any data, the link does not appear because its review appliances will automatically be provisioned as soon as the first processing job completes. A “De-Provision” link provides the option of removing (unassigning) the Review Role from appliances that are already provisioned. The Case Home (Primary) appliance will not display a “de-provision” link.

For more information, and to set up and configure your appliances to use a distributed architecture model, refer to the *Distributed Architecture Deployment Guide*.

System-level: Shared Role Assignment

Accessed in **System > Appliances >** [*selected appliance*] **> Appliance Roles**, shared roles are distributed services for all cases in a cluster. Sharing roles allows you to leverage any existing capacity in a cluster to assist other appliances. These roles are dynamically managed, so no existing processes will be prematurely interrupted.


Select a Case
Settings | Users | Appliance | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | License | Logs | Support Features | Patches
Appliance
Appliance Roles
Sessions
Jobs
Sources
Save Changes
Reset

Appliance Name: 29. test .local (Master)

Assign Roles for Appliance

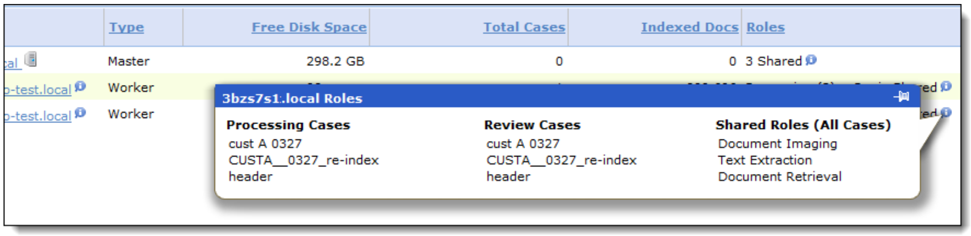
Processing	Review	Case Name	Home Appliance	Indexed Docs	Volume	Roles (# Appliances)
□	□	cust A 0327	2BZS7S1.local	790.7 KB	322.6 GB	Processing(2) + Review(2)
□	□	header	3BZS7S1.local	131.9 KB	22.0 GB	Processing(2) + Review(2)
□	□	CUSTA__0327_re-index	3BZS7S1.local	0.0 KB	0.0 KB	Processing(1) + Review(1)

Shared Roles:

☑ Document Imaging ☑ Text Extraction ☑ Document Retrieval

- **Document Imaging** assists these jobs: Cache (Native) and Export (Production)
- **Text Extraction** assists these jobs: Cache (HTML) and Export
- **Document Retrieval** assists these jobs: Cache, Export, and Review. Also controls if the crawler is enabled on the appliance.

Info bubbles for each appliance show case details for Processing, Review, and Shared Roles for cases that this node/appliance is provisioned for processing or review.



	Type	Free Disk Space	Total Cases	Indexed Docs	Roles
al	Master	298.2 GB	0	0	3 Shared
o-test.local	Worker				ed
o-test.local	Worker				ed

3bzs7s1.local Roles

Processing Cases	Review Cases	Shared Roles (All Cases)
cust A 0327	cust A 0327	Document Imaging
CUSTA__0327_re-index	CUSTA__0327_re-index	Text Extraction
header	header	Document Retrieval

For more information, and to set up and configure your appliances to use a distributed architecture model, refer to the *Distributed Architecture Deployment Guide.*

Logging In and Out as an Administrator

Your access privileges depend on the role associated with your account. The default admin account has unrestricted access to all cases and administrative functions.

To log in to an appliance as an administrator

1. Type the name or IP address (IPv4 or IPv6) of an appliance in your browser:

   ```
   http://<eDiscoveryPlatformServerName>
   ```

2. When logging in for the first time, type the Veritas-provided default user name and password and click **Login**.

   Note: Be sure to change the default account password. The password is the same on every appliance. Leaving the default password opens your system up to vulnerabilities.

3. If you have access to multiple cases you will be prompted to select a case immediately after logging in. Select a case.

4. If your preferences are set to save your session when you log out, when you log back in you might be prompted to resume your last session. You will not be prompted if you chose to always automatically resume the previous session.

To change the default password

- Click on the user name and click the **Reset Password** button to enter a new password, or see *"Defining User Accounts" on page 15*.

To log out of an appliance

- To log out, click **Logout** at the top of the screen.

  When you log out of the platform while viewing search results or reviewing documents in the Analysis & Review module, you have the option to save your place. The next time you log in, you have the option to return where you left off or to log in to the default screen.

Note: Inactive users are logged out automatically after a configurable amount of time (default is 30 minutes). If your session times out, you will be returned to your current state if you have previously logged out and (1) specified that you want your search state to be saved and (2) that you don't want to be prompted to save state again.

(Optional) Adding Appliances to a Cluster

See *"Adding New Appliances" on page 106*.

Defining System Settings

The system settings specify various options, such as the email address of a local administrator to be notified if a problem occurs, the maximum size of individual files that can be printed or exported, the minimum password length, and the idle timeout (automatic logoff).

Note: If you define a cluster of appliances, the system settings typically apply to all appliances in the cluster.

To change the system settings

1. From the **System** view, click **Settings**.
2. Click a tab to view or change the associated settings. The System Settings table describes the settings for each tab. An asterisk (*) indicates a required field.
3. Click **Save** on any screen to save all the settings under each tab.

System Settings

Field	Description
General	
Administrator email address*	The email address of an administrator to be notified when a problem occurs. This field updates the Feedback link in the eDiscovery Platform footer. **Note:** In rare cases, an error message may include a **Report Problem** link that users can click to notify the administrator.
SMTP server hostname/IP*	The name or IP address of the SMTP email server used to send summaries of document tagging operations, as well as to send problem notices to the administrator. **Note:** Earlier, eDiscovery Platform only supported IPv4 address format. Starting with 9.0.1, eDiscovery Platform supports IP addresses in IPv4 and IPv6 formats. If IPv6 format is used, then it must be enclosed in square brackets as shown in this example: [fd74:128f:f0b1:901f:1111:2222:3333:4444]. **Note:** This is also used to send legal hold notifications to custodians. (For more information, refer to *"Appendix A: Setup Requirements" Legal Hold User Guide*.
SMTP server authentication	The user name and password to be used when additional SMTP server authentication is required beyond the user name and password associated with your SMTP server.
Confirmation server hostname/IP*	The name or IP address of the Confirmation server to be used for legal hold notifications to custodians as well as to identify system administrators. **Note:** Earlier, eDiscovery Platform only supported IPv4 address format. Starting with 9.0.1, eDiscovery Platform supports IP addresses in IPv4 and IPv6 formats. If IPv6 format is used, then it must be enclosed in square brackets as shown in this example: [fd74:128f:f0b1:901f:1111:2222:3333:4444]. **Note:** This is required during set up of a licensed Legal Hold module. Follow the steps to configure your Confirmation server with the appropriate hostname/IP. For more information, refer to the Appendix in the *eDiscovery Platform Legal Hold Reference Guide*.

System Settings (Continued)

Field	Description
Auto-Recovery	**Enable appliance auto-recovery**. If an appliance fails or cannot access the primary appliance, the appliance attempts to recover automatically, up to a maximum number of retries (default is three). If this option is disabled, or each of the retries fails, the appliance is taken off-line and must be restarted manually (see *“Enabling, Disabling, and Restarting Appliances” on page 110*). Note that a primary appliance and standalone appliances always attempt to recover automatically.
Support Web Page URL	URL to be used as the Support link in the footer.
Windows authentication for appliance	The user name and password to be used for file browsing or accessing network resources from the appliance. This user name and password should match the logon account credentials used for the EsaApplicationService.
Additional account for mail conversion	(Optional) The platform will use the extra account to multi-thread MBOX (and other supported formats) conversion. Specify an administrative Windows account that is not used by any eDiscovery Platform Windows services and PrizmDoc services. This account must have access to the files to be indexed and be part of the local admin group on the appliance.
Locations	
Extracted Files	The location where the platform will store PST and NSF email files that are extracted from EnCase evidence files and other containers (such as ZIP and RAR files) during pre-processing. **Note:** This setting can be overridden at the case level. From **Case > Settings > Configure processing parameters and features**, you can specify a different location for each case. • Default directory—Use the default directory: `<appliance installation dir>\containedPstNsf\<case ID>\` • Custom directory—Specify the parent directory you would like the platform to use to store extracted PST and NSF files. Case-specific folders will be automatically added underneath the parent directory (\<*case ID*>\). **Note:** The system administrator is responsible for maintaining the integrity of the PST/NSF extraction directory, and Veritas recommends that you include it in the backup plan. However, if the contents of the directory are ever removed, the platform will automatically re-extract the necessary PST and NSF files from their container and replace them in the directory.

System Settings (Continued)

Field	Description
Converted Files	The location where the platform stores converted MBOX (and other supported types) files. Original files are kept intact at their original location. **Note:** This setting can be overridden at the case level. From **Case > Settings > Configure processing parameters and features**, you can specify a different location for each case. When setting locations, specify a File Share or disk drive location that: • Is consistently accessible to the appliances in the cluster • Has sufficient disk space to handle your expected volume of converted mail (MBOX and other supported file type) items. Specify the location by using a UNC path, `\\servername\directory` Put contained and converted files and known files on a separate network share from the local appliance drive. This is a requirement for distributed environments and is highly recommended for all configurations for optimum performance and processing. **Note:** The system administrator is responsible for maintaining the integrity of converted files directory, and Veritas recommends that you include it in the backup plan. However, unlike the extracted files, these files cannot be recreated by the system. For other system settings (including service account credentials) information, refer to the *QuickStart Guide*.
Known File Filtering	The storage directory for known file lists. Type the directory or click **Browse** to specify the storage directory. The directory must be accessible from all appliances in an eDiscovery Platform cluster, and it will not be backed up or managed by the platform. See *"Pre-Process Your Source Data" in the Case Administration Guide* for more information on known file filtering and how it is used.
Indexing	
Items to Include in Processing	Specifies which types of Exchange/PST items, notes, and archives should be included in processing (**Contacts**, **Calendar Items**, **Tasks**, **Journal entries**, and **Posts**). By default, all items are included. These system-level settings act as a template for new cases: any changes made to the case level settings for that particular case will override these system level settings. To modify the settings for a new case, go to [CaseName] > Processing > Settings > Configure processing parameters and features. **Note:** Different rules apply in a distributed architecture. Refer to the Distributed Architecture Deployment Guide for more information.
Security	
Session timeout*	The number of minutes (5 to 720) a user's session can be idle before the user is logged out (default is 30).

System Settings (Continued)

Field	Description
Minimum password length*	The minimum number of characters (8 to 40) required in an account password (default is 8). You can change the minimum and maximum values of the minimum password length by setting the following properties using **System** > **Support Features** > **Property Browser** feature: • *esa.min.value.mimimum.password.length* • *esa.max.value.mimimum.password.length* The value of *esa.max.value.mimimum.password.length* property must be lower or equal to the value set for the *esa.maximum.password.length* property. The *esa.maximum.password.length* property defines the maximum password length, which is 40 by default.
Password change interval*	The number of days (0 to 365) before a password expires (default is 0). A zero indicates that passwords never expire.
Failed logins allowed*	The number of consecutive failed login attempts allowed (0 to 100) before the user account is automatically disabled (default is 5). A zero indicates any number of failed attempts is allowed.
User Password Policy	The option to require users to change their passwords on initial login. If you select this option, the user is prompted to change the password. When an administrator sets the password for another user and this check box is selected, the user must reset the password upon next login.
Lockout message	The message displayed to the user (up to 255 characters) when the user account is locked out because the number of password retries was exceeded.
User Logon Help Message	There are options and delivery methods for a user message: • Enter the text (up to 255 characters) that is presented when the user clicks **Need help?** on the login screen. • Enter the email address and text. • Enter a URL link and text.
HTTPS	Forces redirection to HTTPS for all access attempts. Click the **Connect Securely** link to test whether you can access the web interface using HTTPS.
Errors and warnings	In the event of an error, this option will display more detailed information in the message window which will help the support team in diagnosing the issue. Errors with detailed information display next to the username with a yellow warning sign icon.

System Settings (Continued)

Field	Description
Browser Cache	The browser maintains 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. You can enable or disable browser cache. The default setting is enabled. 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. **Note:** 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.
Print	
	Enter the maximum size of individual files (in megabytes) that can be printed from the platform. A file that exceeds the maximum size is broken up into multiple files. Contact Technical Support if you are changing this value in a multi-appliance cluster: • Maximum CSV file size* (10 to 2000, default is 20) • Maximum PDF file size* (10 to 2000, default is 100)
Confidentiality footer used on printed reports	An alphanumeric string (up to 150 characters) used to print confidentiality information on printed reports. By default, this field is empty.
Time and Date **Note:** Note: The date, time, and time zone formats are used for display in all administrative and document contexts across all cases on the cluster, unless the values are overridden at the case level.	
Date Format	Choose the format from the drop-down list.
Time Format	Choose the format (12-hour or 24-hour clock) from the drop-down list.
Time Zone	Choose a time zone from the drop-down list, or use the current appliance time zone (default).

System Settings (Continued)

Field **Description**

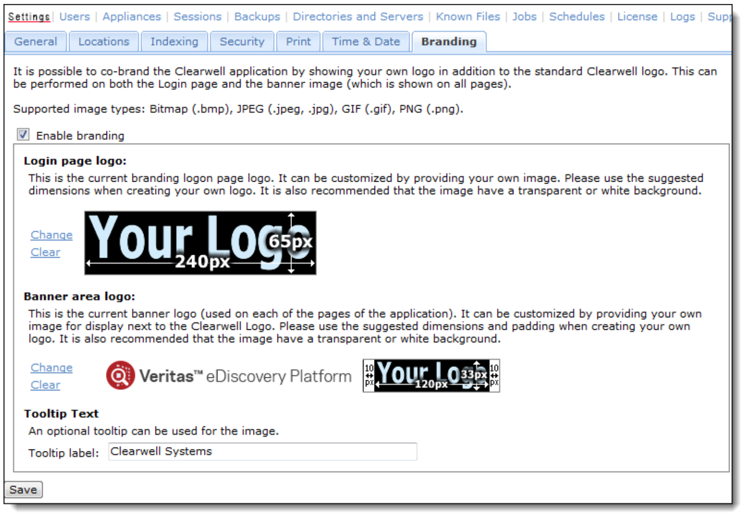
Branding

Enable Branding

Select the check box to enable co-branding of the application with your own logo in addition to the standard platform logo. The additional logo will be displayed on the login screen and in the banner image that is shown on all screens.

Supported image types include bitmap (.bmp), JPEG (.jpeg, .jpg), GIF (.gif), and PNG (.png).

When you select the **Enable Branding** check box, display options are presented.


Settings | Users | Appliances | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | License | Logs | Sup
General
Locations
Indexing
Security
Print
Time & Date
Branding
Change
Clear
Your Logo
65px
240px
Change
Clear
Veritas™ eDiscovery Platform
Your Logo
10 px
120px
33px
10 px
Save

It is possible to co-brand the Clearwell application by showing your own logo in addition to the standard Clearwell logo. This can be performed on both the Login page and the banner image (which is shown on all pages).

Supported image types: Bitmap (.bmp), JPEG (.jpeg, .jpg), GIF (.gif), PNG (.png).

☑ Enable branding

Login page logo:

This is the current branding logon page logo. It can be customized by providing your own image. Please use the suggested dimensions when creating your own logo. It is also recommended that the image have a transparent or white background.

Banner area logo:

This is the current banner logo (used on each of the pages of the application). It can be customized by providing your own image for display next to the Clearwell Logo. Please use the suggested dimensions and padding when creating your own logo. It is also recommended that the image have a transparent or white background.

Tooltip Text

An optional tooltip can be used for the image.

Tooltip label: Clearwell Systems

- Click the **Change** button in the **Login screen logo** or **Banner area logo** section to open the Upload branding image pop-up window.
- Click … and browse to select and upload the image. The image is automatically scaled to fit the available space.
- Click **Save**. The image is now included in the application banner and/or on the login screen.
- Type the tooltip label in the appropriate field.
- Click “Clear” to remove the customization.

Legal Hold Authentication

If using this feature, it needs to be enabled and set up. See the *Legal Hold User Guide “Legal Hold Authentication.”*

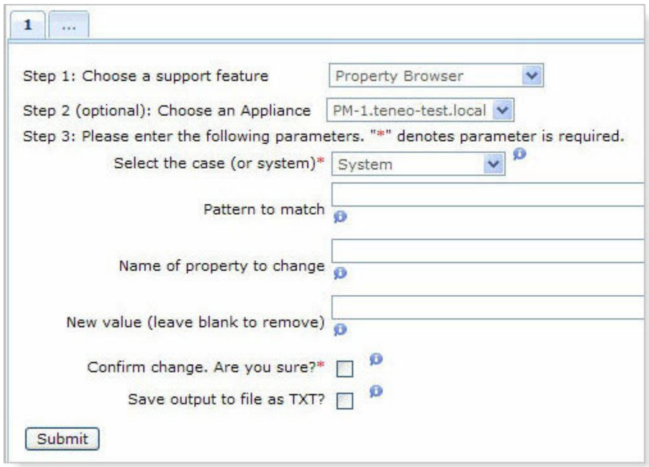
Configuring the Backup Location

By default, case and system backups are saved on the local appliance. Veritas recommends saving backups to a shared network location for disaster recovery in the event of an appliance failure. Saving backups to an external location also makes it easier to move cases between appliances in a cluster to optimize the use of available disk space. To perform case and system backups, see *"Backup and Restore" on page 127*.

To change the backup location

1. From the **System** view, click **Support Features**.

2. Select **Property Browser** from the feature menu, and click **Submit** to view the properties that you can change.



Step 1: Choose a support feature: Property Browser

Step 2 (optional): Choose an Appliance: PM-1.teneo-test.local

Step 3: Please enter the following parameters. "*" denotes parameter is required.

Select the case (or system)*: System

Pattern to match

Name of property to change

New value (leave blank to remove)

Confirm change. Are you sure?* □

Save output to file as TXT? □

3. Enter the following information. An asterisk (*) indicates a required field.

Directory Properties

Field	Description
Name of property to change	Enter the following property name: **`esa.case.backupDir`** You can change this value by editing the **`esa.case.backupDir`** property using the support feature. You must specify the **backupDir** for each appliance in the cluster by repeating the process for each appliance in the **Choose an appliance** drop-down list. You must also set the **`esa.case.sharedBackupDir`** property to **true** in order for the cluster to recognize the backupDir location as a shared location that is visible by all appliances in the cluster. It is not necessary to set this property for each appliance in the cluster.
Confirm change*	Select the check box to confirm the change.

4. Click **Submit** to apply the change.

Managing emails notifications for jobs completion

By default, users do not receive emails after the job completes. Users can enable the **Send emails after my jobs complete** settings on **Preferences** available at the top of the eDiscovery Platform user interface so that an email is sent after the job completes. The email notification includes information on the job status, job description, and case name.

Email notification is not sent for the status change jobs, such as, Stopped, Start, and so on. Emails are not sent for jobs that take less than 5 minutes. An administrator can configure this time limit by setting the **esa.jobmanager.notification.email.jobTimeTakenInSecs** property by using **System** > **Support Features** > **Property Browser**. The default value for this property is 300 seconds.

Configuring Privacy Info items for Bulk Redaction

Starting with release 10.0, eDiscovery Platform provides an option to redact privacy information, such as US phone number, email, US social security number, US postal code, and date in documents directly from the Bulk Redaction window.

By default, the above-mentioned five Privacy Info options are available. Administrators can add more options to the Privacy Info list by making additional entries in the ***<EDP_INSTALL_DIR>\config\configs\prizmdocViewerPredefinedSearch.json*** file and then restarting the eDiscovery Platform services.

Format for adding the Privacy Info options is mentioned below:

```
{
             "searchTermIsRegex": true,
             "searchTerm": "Privacy Info name",
             "description": "Privacy info Description",
             "userDefinedRegex": <User Defined Regex>,
             "selected": false,
        "options": {
            "matchCase": false,
            "endsWith": false,
            "beginsWith": false,
            "matchWholeWord": false,
            "exactPhrase": false
        }
  }
```

Here, administrators should update the *searchTerm*, *description*, *userDefinedRegex* fields and add the above text in the “terms” array of the **prizmdocViewerPredefinedSearch.json** file. Name of the **Privacy Info** field to be displayed in the user interface is picked up from the *description* field.

Note: When backslash (\) is used in the *userDefinedRegex* field, they must be escaped appropriately. For example, for searching words that begin with "Pa", the regular expression can be "Pa(\w+)". This regular expression should be appropriately escaped like: "Pa(\\w+)".

For a detailed breakdown of forming a Regular Expression pattern, see the *Regular Expressions Support* section in the *Veritas eDiscovery Platform™ User Guide.*

Virus Scanning Guidelines

The eDiscovery Platform does not come with bundled anti-virus software. Veritas recommends that users perform an anti-virus scan of the data that they wish to use the platform to analyze and provide anti-virus software on their end-user PCs since users do have the ability to download native files on their own.

Veritas recognizes the need for security compliance within an organization and the requirement for deploying anti-virus software. If you install anti-virus software on the appliance, consider the following guidelines for scanning directories and processes.

Refer to the following topics in this section:

- *"Directory Configuration" on page 98*
- *"Running Review Cache Job" on page 100*
- *"Disabling Your Anti-Virus Software" on page 100*
- *"Ensuring Operability" on page 100*

Directory Configuration

Follow the steps in this section to configure directories.

Excluded Directories

You should exclude the following directories from your antivirus scanning.

- `C:\jdk-8u291-windows-x32`
- `C:\jdk-8u291-windows-x64`
- `D:\CWShared`
- `D:\Clearwell Packages\Muhimbi Document Converter`

Note: If the mysql directory is scanned, the anti-virus software is likely to quarantine or delete the files. The first symptom of this scenario is that your backups start failing.

- `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, *To update the attachments directory (attCacheDir) location:*

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

- `C:\Program Files(86)\Nexidia`
- `C:\Program Files(86)\Nexidia\Language Packs`
- `C:\Program Files\Nexidia\Search Grid 2.0`
- `D:\Nexidia`

Note: The Nexidia directories only exist if you have the Audio Search module.

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

Note: This directory only exists if you use the Rights Management feature.

Scanned Directories

Before a document is displayed to the Reviewer in native view, the document is generated as a temporary file in its native format. Document rendering can be initiated in two different ways: (1) by downloading documents in real time through Review Mode's Native View or (2) as a batch process through Search Cache Job.

Note: Virus scanning documents will impact cache and review performance.

Downloading files in Real Time

When you review documents in their native format without running the Review Cache Job, the files are downloaded and converted in real time. By default, converted files are saved in the `d:\CW\<current_version>\scratch\temp\esadb\attCacheDir\ directory.`

The `attCacheDir` directory is a staging area for documents and attachments that need to be scanned for viruses prior to being displayed to the user. Because you can only exclude directories from a virus scan, move the attachments directory (`attCacheDir`) to a different location and then update the path.

To update the attachments directory (attCacheDir) location:

1. From the System view, click Support Features.
2. Select **Property Browser** from the feature menu.
3. Type **`esa.altAttachmentsDir`** in the **Name of Property to change field**.
4. Specify the new location of the attachments directory.

   Note: A UNC path is required in a Distributed Architecture environment.
5. Confirm the change.
6. Click **Submit**.

Summary: Configure your anti-virus software to scan the **`attCacheDir`** directory.

Running Review Cache Job

When you run the Review Cache Job, every document within the group is converted into its native format and then stored in an unspecified directory. To ensure these native-format files are scanned, you need to create a staging directory called `d:\CW\netitScan\` and then point your anti-virus software to that directory.

After creating the `netitScan` directory, files are converted to native format, copied to `d:\CW\netitScan`, scanned by your anti-virus software, and then copied to their final home.

How to create a fixed location to automatically scan temporary, native-format files

1. On the appliance, create the `d:\CW\netitScan\` directory if not already there.
2. Log on to the appliance and navigate to **System > Support Features**.
3. From the Choose a support feature drop-down list, select **Property Browser**.
4. In the Name of property to change field, type **`esa.netit.virus_scanner_dir.`**
5. In the New value (leave blank to remove) field, type `d:\CW\netitScan`.
6. Select the option: **Confirm change. Are you sure?**
7. Click **Submit** to save the configuration.

Disabling Your Anti-Virus Software

If you decide to discontinue the practice of scanning documents for viruses, ensure that you remove the **`esa.netit.virus_scanner_dir`** property through the **Support Features >**. Before upgrading or installing a new version of the product, Veritas strongly recommends disabling your anti-virus software first.

Note: For upgrade information, refer to the *Upgrade Overview*, and *Upgrade Guide*. For new installations, refer to the *Veritas Installation Guide*.

Ensuring Operability

Security Software and Windows Management Instrumentation (WMI)

The product depends on Windows Management Instrumentation (WMI) in order to gather hardware utilization statistics for adjusting processing speeds. In the event that the product is unable to obtain WMI statistics, the system will not be able to discover or process data successfully. Ensure that your security software configuration is not blocking or interfering with WMI and its ability to collect eDiscovery Platform management data.

Maintaining eDiscovery Appliances

For information about how to manage the appliances in a cluster, refer to the following topics:

- *"Managing Your License" in the next section*
- *"Clearwell Commander" on page 105*
- *"Adding New Appliances" on page 106*
- *"Changing Appliance Settings" on page 108*
- *"Enabling, Disabling, and Restarting Appliances" on page 110*
- *"Removing an appliance" on page 111*
- *"Upgrading Cases" on page 111*
- *"Moving Cache (On or Off) the Appliance" on page 113*

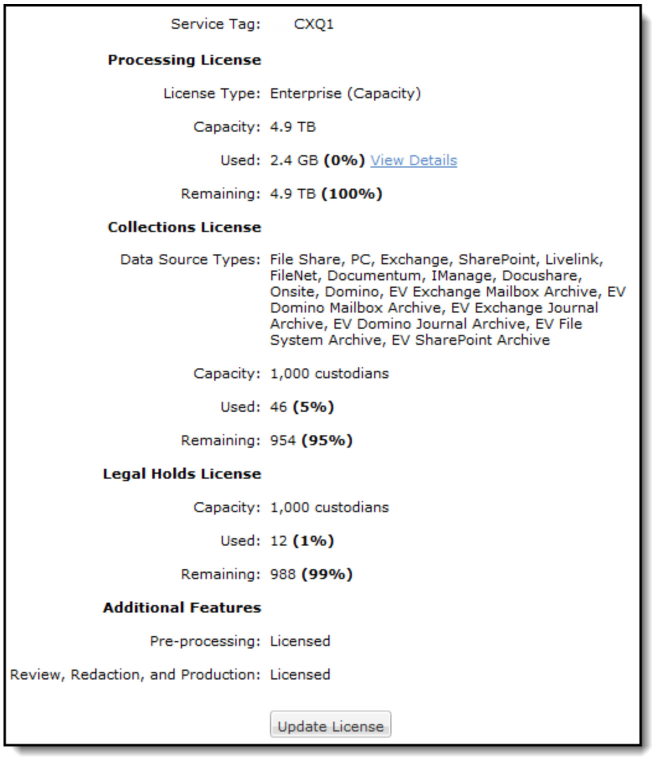
Managing Your License

Your license key is supplied by Technical Support based on the terms of your license agreement. For new appliances, the license key is usually already installed and activated. If you have upgraded your license to allow for expanded case and document processing, you may receive a new license file.

Use the System > License screen to view the license information and to update your license. On the associated Detail screen, you can view how much of your licensed capacity each case currently uses.

To view or update license information

1. From the **System** view, select **License**.



Service Tag:	CXQ1
Processing License	
License Type:	Enterprise (Capacity)
Capacity:	4.9 TB
Used:	2.4 GB **(0%)** View Details
Remaining:	4.9 TB **(100%)**
Collections License	
Data Source Types:	File Share, PC, Exchange, SharePoint, Livelink, FileNet, Documentum, IManage, Docushare, Onsite, Domino, EV Exchange Mailbox Archive, EV Domino Mailbox Archive, EV Exchange Journal Archive, EV Domino Journal Archive, EV File System Archive, EV SharePoint Archive
Capacity:	1,000 custodians
Used:	46 **(5%)**
Remaining:	954 **(95%)**
Legal Holds License	
Capacity:	1,000 custodians
Used:	12 **(1%)**
Remaining:	988 **(99%)**
Additional Features	
Pre-processing:	Licensed
Review, Redaction, and Production:	Licensed

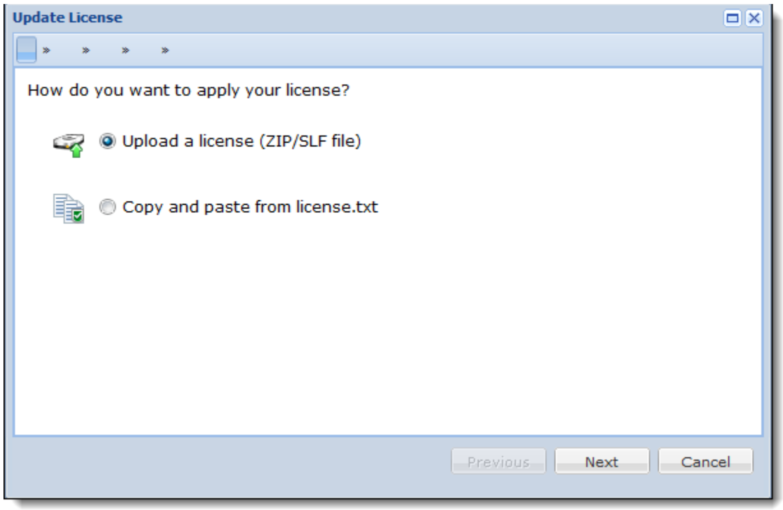
In this example, the current capacity is for 500 custodians. Periodically note this count, particularly each time a collection set or task is deleted, or a custodian is released from a legal hold from a case.

2. To view details for your cases, click **View Details**. The Details page shows each case with the capacity used for each.
   - Click **Done** to return to the License screen.
   - Click an underlined case link to open the Status screen for that case.

3. To update the license, click **Update License**.

   The Update License Wizard opens.

4. Select the method you want to use to update your license. (As shown in this example, you can choose to copy and paste the license information you received from an email message.)



Update License

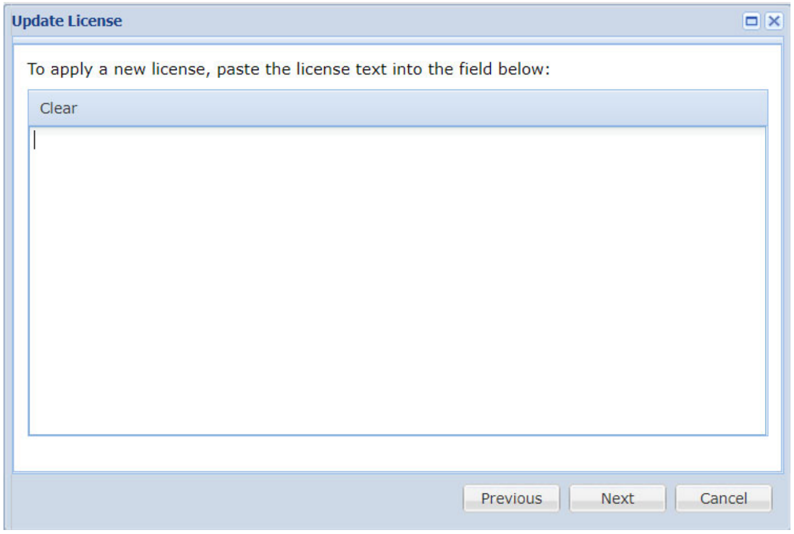
How do you want to apply your license?

● Upload a license (ZIP/SLF file)

○ Copy and paste from license.txt

Click **Next**.

5. Press Ctrl+V to place the copied text into the window. (Click **Clear** to delete.)

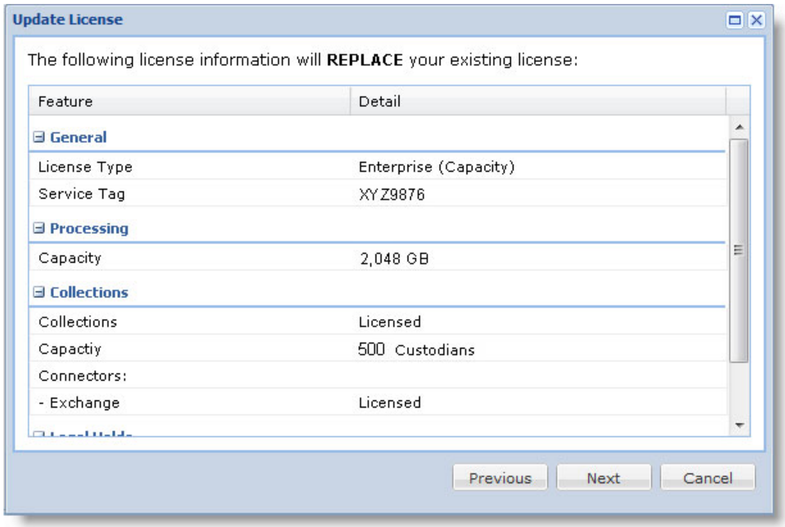


Update License

To apply a new license, paste the license text into the field below:

Click **Next**.

6. Review the license information to be applied (replacing your existing license).

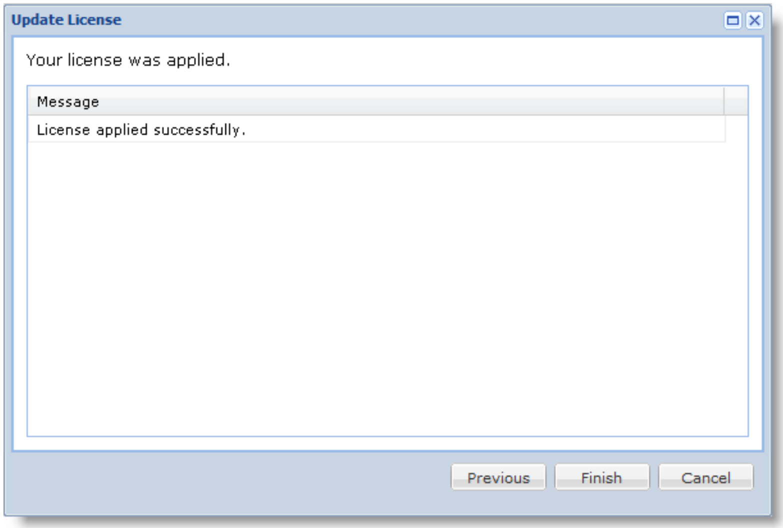


The following license information will **REPLACE** your existing license:

Feature	Detail
General	
License Type	Enterprise (Capacity)
Service Tag	XY Z9876
Processing	
Capacity	2,048 GB
Collections	
Collections	Licensed
Capactiy	500 Custodians
Connectors:	
- Exchange	Licensed

To confirm and continue, click **Next**. (Alternatively, click **Previous** to re-apply the license information.)

7. The final screen of the Wizard displays a message reflecting your license status. In this example, the license was applied successfully.



Your license was applied.

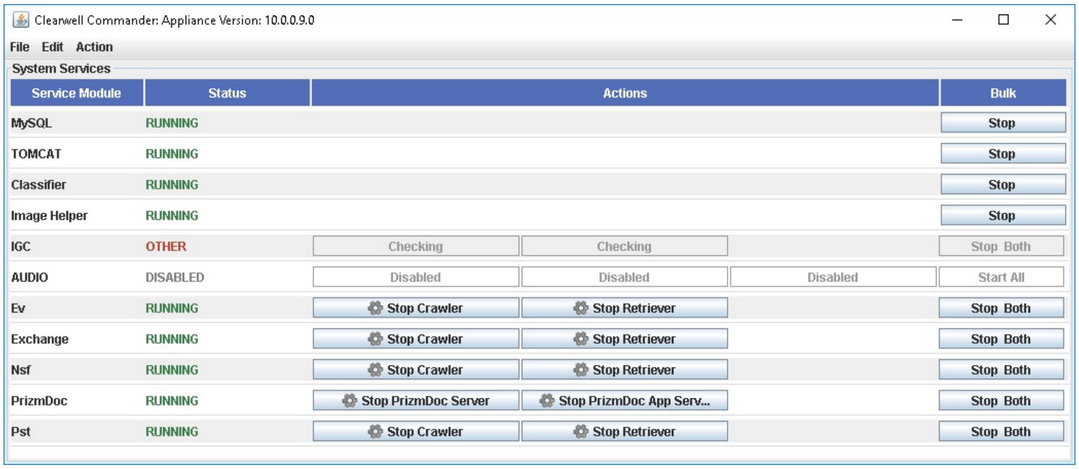
Message
License applied successfully.

Click **Finish**. (Alternatively, click **Previous** to re-apply the license information.)

Clearwell Commander

A user with System Manager rights can access **Clearwell Commander** from the icon on an appliance's Windows desktop.

Launching Commander will bring up a user interface where all the functions available through the Clearwell Utility will appear with improved control over some features. Version 8.2 adds the actions **Password Manager** and **Copy Tomcat Provided Certificate to Windows Trust Store**.



Service Module	Status	Actions			Bulk
MySQL	RUNNING				Stop
TOMCAT	RUNNING				Stop
Classifier	RUNNING				Stop
Image Helper	RUNNING				Stop
IGC	OTHER	Checking	Checking		Stop Both
AUDIO	DISABLED	Disabled	Disabled	Disabled	Start All
Ev	RUNNING	Stop Crawler	Stop Retriever		Stop Both
Exchange	RUNNING	Stop Crawler	Stop Retriever		Stop Both
Nsf	RUNNING	Stop Crawler	Stop Retriever		Stop Both
PrizmDoc	RUNNING	Stop PrizmDoc Server	Stop PrizmDoc App Serv...		Stop Both
Pst	RUNNING	Stop Crawler	Stop Retriever		Stop Both

On the **Main Dashboard**, users will see system services status. The controls displayed will allow users to start and stop services individually.

Under **Edit**, download preferences can be edited to specify whether there is a firewall to traverse and the password if authentication is required.

Under **Action:**

- **Password Manager** is where the System Administrator with the highest privileges can view, change, and update the MySQL root and common passwords.

  Important: This function is password protected. These passwords should only be managed with assistance from Support, or by someone in Support. Changing these passwords without understanding the effects can be disastrous, such as permanent loss of access to the data. This tech note contains the list of passwords managed by Clearwell Commander: 000114500 at *https://www.veritas.com/support*.

- Backup and restore appliance, stop and start appliance services, viewing and uploading logs, and build incremental configuration changes are all accessible here. This interface allows log preview and saving.

- **Generate Self-signed Certificate** allows the System Manager to replace the appliance SSL certificate. For details, see *"Clearwell Commander-Generated Certificate" on page 164*.

- **Copy Tomcat Provider Certificate to Windows Trust Store** allows the System Manager to propagate an installed provider generated certificate to all the areas where it is required in the system. For details, see *"Provider-Generated Certificate" on page 166*.

> **Note:** Once a certificate has been installed, the **Copy Tomcat Provider Certificate to Windows Trust Store** functionality can be used to propagate a certificate from any source. See *"Propagate the Valid Certificate for use by eDiscovery Processes" on page 170*.

Under **File**, the System Manager can exit the utility.

Adding New Appliances

You can manage a cluster of multiple appliances by defining a primary appliance. Simply log in to the appliance that you want to serve as the primary, and add the other appliances. After you add one or more appliances, you can use any appliance in the cluster to administer the other appliances and search any case on any appliance, provided the primary appliance is active and accessible from the appliance where you log in.

Global system changes are applied to all members of the cluster. There are some exceptions to this rule and these pertain to particular distributed architecture configurations. Refer to the Distributed Architecture Deployment Guide for more information. New cases are assigned to the appliance with the most free disk space, unless you manually select a specific appliance.

Note: An appliance must be idle (no users logged into any case, no jobs running) when it is added to a cluster. The primary appliance can have any number of cases. If you add an appliance that has its own cases to a cluster, the cases are in a "recoverable" mode after the appliance is added.

To define the appliances in a cluster

Before you begin: Ensure the following requirements are met.

- All cluster members must be running the same version (including fix packs).
- All appliances in a cluster must display the same date/time and be in the same time zone.

1. From the **System** view, click **Appliances**.

   The **Appliances** screen shows the appliance names, types, free disk space, the total number of cases, number of indexed documents, appliance roles and sharing, and active user sessions for each appliance in the cluster.

   The **Primary** is indicated in the **Type** column; the other appliances in the cluster are designated as **Secondarys**.

2. To add an appliance to the cluster:

Appliance Details

Field	Description
Appliance Name*	Enter an appliance name (up to 35 characters).
Host Name*	Enter the appliance host name (up to 255 characters).
Clearwell Application Port*	Enter the port used for inter-appliance communication. Do not change the default (2595) unless instructed by Technical Support.
Shared Roles:	Shared Roles are distributed services for all cases in this cluster. This allows you to leverage any existing capacity to assist other appliances. These roles are dynamically managed, so no existing processes will be prematurely interrupted.
Document Imaging	Document Imaging assists the following jobs: Cache (Native), Export (Production)
Text Extraction	Text Extraction assists the following jobs: Cache (HTML), Export, and Review
Document Retrieval	Document Retrieval assists the following jobs: Cache, Export, and Review

A. Verify that the appliances to be added are installed in your network and activated. (Asterisks indicate required entries). Specify the **Appliance Name**, **Host Name**, **Clearwell Application Port**, and click the **Verify** button. If the verification fails, you will be prompted for more information.

B. After verifying the appliances are installed in the network and activated, specify shared roles for the appliance.

Note: By default all roles are checked, so imaging, extraction, and retrieval can be distributed for better performance. If it is a utility node being added, then based on what was installed on the node, some shared roles may be de-selected. It is not recommended to make changes to these settings (such as de-selecting sharing) without consulting support first.

C. Click **Save** to submit the new appliance, or click **Cancel** to discard your changes.

3. To restart an appliance or perform other appliance management tasks, see *“Enabling, Disabling, and Restarting Appliances” on page 110*.

4. To remove an appliance from the cluster, see *“Removing an appliance” on page 111*.

Changing Appliance Settings

You can change an appliance name, monitor its current memory and disk space, view and terminate active user sessions, stop the job manager, stop or delete jobs, and enable or disable access to email server/archive document sources.

Note the following guidelines:

- Each appliance should be restarted once a month to maintain optimum performance (see *“Enabling, Disabling, and Restarting Appliances” on page 110*).
- As an appliance’s disk becomes full, you can:

  A. Back up one or more cases, and restore the cases to another appliance with more disk space (see *“Backup and Restore” on page 127*).

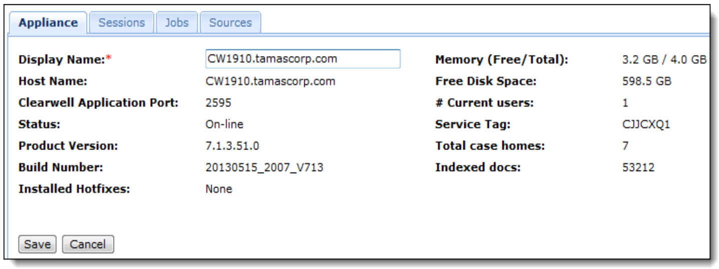
  B. Delete the backed-up cases from the original appliance (refer to *"Managing Cases" in the Case Administration Guide*).
- When you change user access privileges, you may want to terminate the active sessions. Some privilege changes do not take effect until the next time the user logs in.

To manage individual appliances

1. From the **System** view, click **Appliances**.
2. To view or change an appliance’s settings

   A. Click the appliance name.

   The Appliance details screen displays.



Display Name:*	CW1910.tamascorp.com	**Memory (Free/Total):**	3.2 GB / 4.0 GB
Host Name:	CW1910.tamascorp.com	**Free Disk Space:**	598.5 GB
Clearwell Application Port:	2595	**# Current users:**	1
Status:	On-line	**Service Tag:**	CJJCXQ1
Product Version:	7.1.3.51.0	**Total case homes:**	7
Build Number:	20130515_2007_V713	**Indexed docs:**	53212
Installed Hotfixes:	None		

B. Click a tab to view or change the associated settings. The following table describes the settings for each tab.

Appliance Settings

Tab	Description
Appliance	View the appliance details, such as the software version, free/total memory usage of the Clearwell Application Server (Java) process (CWJava.exe), and available disk space on the drive where the application is installed. **Note:** The free/total memory value does not indicate the physical memory (RAM) of the appliance. To change the appliance name, enter a new name (up to 35 characters), and click **Save**.
Sessions	View the current active sessions for the appliance. To terminate a session, click the trash icon placed in the user’s row. To view the active sessions for all appliances in the cluster, see Viewing System Sessions.
Jobs	View the recent jobs for the appliance, such as indexing, exporting, printing, and tagging. To view the jobs for all appliances in the cluster, see *“Viewing Jobs and Accessing Exported Files” on page 74*. You can do any of the following: • To limit the list of jobs displayed, select a user, case, or update time from the **User**, **Context**, and **Jobs updated** menus. Select **System Jobs** from the **Context** menu to view just the backup/restore and purge jobs. Note that discovery jobs for email server/archive sources are monitored on their respective screens (refer to *"Discovering Archive Sources" in the Case Administration Guide*). • To view the job log for a job, click ▣ in the status column. • To stop a running job, select the check box next to the job, and click **Stop Jobs**. To stop or pause the Job Manager, click **Stop** or **Pause**. Stopping the Job Manager cancels all running jobs. To restart or reactivate the Job Manager, click **Start** or **Resume**. To stop a paused Job Manager, click **Resume**, and then click **Stop**. • To delete a job, click 🗑 for the job, or select the check box next to the job, and click **Delete Jobs**. To delete all jobs older than 60, 30, or 14 days, select the time interval from the **jobs older than** menu, and click **Purge**. All files associated with a deleted job are also deleted, and will no longer be accessible from the Jobs window.
Sources	View the discovered email server/archive sources that can be accessed by the appliance. To enable or disable access to these sources, select the check box next to the appropriate sources, and click **Enable** or **Disable**. To view and enable or disable these sources for all appliances in the cluster, see *“Managing Schedules and Jobs” on page 71*.

Enabling, Disabling, and Restarting Appliances

We recommend that you restart all appliances, including the primary appliance, once a month to maintain optimum performance.

Note: Restarting the primary appliance restarts all Secondary appliances and terminates all user sessions

If an appliance other than the primary appliance malfunctions, you can disable it to ensure that it does not affect other appliances in the cluster. You can then re-enable it or remove it from the cluster.

The transition of a secondary appliance from disable to enable state may take some time (up to 30 minutes) depending on how quickly communication can be re-established with the primary appliance. To avoid this time delay, you can intervene and manually restart the services on the secondary appliance to enable the appliance and bring it online.

Note: You can check the secondary log file to verify that the appliance is in this state.

To enable, disable, or restart an appliance

1. From the **System** view, click **Appliances**.

   The appliance list shows the host name, appliance status, the free disk space on the drive where the platform is installed, and the number of cases, indexed documents, and active user sessions. Note the following appliance status values:

   – **Disabled**. The appliance is part of the cluster, but it cannot be accessed by users or other appliances.

   – **Off-line**. The appliance is part of the cluster, but is temporarily unavailable, such as during system backups or an auto-recovery (see the auto-recovery settings in *"Defining System Settings" on page 90*). You may have to restart the appliance to change its status to **On-line**.

2. To restart an appliance

   A. Select the check box next to the appliance you want to restart.

   B. Select **Restart** from the menu at the bottom of the screen, and click **Go**.

   C. If the **Off-line** status does not change, restart **EsaApplicationService** on the appliance.

      I. On the platform, right-click on **My Computer** and select **Manage**.

      II. Select **Services and Applications > Services**, right-click on EsaApplicationService, and select **Restart**.

3. To enable or disable appliances

   A. Select the check box next to the appropriate appliances.

   B. Select **Enable** or **Disable** from the menu at the bottom of the screen, and click **Go**.

Removing an appliance

Note: Some cluster implementations may be set up with primary and secondary nodes sharing a single database.

- When appliances are in a Distributed Architecture configuration (sharing a single remote database), a node must be prepared before it is removed. See “Prepare Nodes for Backup, Restore, or Removal” of the Distributed Architecture Deployment Guide.
- When appliances have been set up in a cluster with primary and secondary nodes that each have their own database, proceed to the step below.

1. To remove an appliance from the cluster, click 🗑 for the appliance.
   Note the following:
   - You can delete an on-line appliance that has cases, provided that the appliance is idle. To delete cases from an appliance, go to the **All Cases** view and click the trash icon for the case. To first move a case to another appliance, see *“Migrating Cases” on page 153*. When you delete an appliance with cases, the cases are also removed from the cluster, but the case data remains intact and recoverable on the deleted appliance.
   - There is no need to make a distinction between the online/offline/disabled state of the appliance - appliances can now be deleted in any state.
   - A disabled appliance can be deleted without first deleting its cases.
   - When you delete an appliance from a cluster, it becomes accessible as a single-appliance cluster and the cases on the appliance have the status “Recoverable.”

Upgrading Cases

When you upgrade the platform, the system is unavailable until all services and internal data have been upgraded. After the upgrade completes and services come online, users are able access the user interface.

When a newly-upgraded appliance comes online, the appliance automatically begins creating and running upgrade jobs for existing, upgradeable cases. When the appliance upgrades cases automatically, the most recently-created cases are upgraded first.

If you have cases that need to be upgraded first, you can control the order in which the cases are upgraded.

Note: You cannot delete a case while it is being upgraded.

Case Upgrade Phases

1. **Upgradeable**

   The initial state of a case after a software upgrade.

   A case can also be labeled “Upgradeable” if the upgrade job for the case is manually stopped or if it fails to upgrade for a non-critical reason. Upgrading the cases again at a later point causes the upgrade to pick up where it left off when the job was stopped.

2. **Upgrading**

   The case is currently being upgraded. The last step in an upgrade job is to start a post-processing job for the case, if it's needed.

   You can view the status of upgrading cases from the status log of each upgrade job.

3. **Processing**

   The case has finished upgrading and is running through post-processing.

4. **Online**

   The case upgraded and ready to be accessed.

To view the status of upgrading cases

You can view the status of upgrading cases from the Jobs window found above the navigation bar. When you click the file icon associated with the Upgrade job, the case log displays.

After the upgrade completes, the upgrade job is removed from the Jobs window.

To view the details of a completed upgrade job

You can view the logs of a completed upgrade job from **System > Jobs**. Click the file icon associated with the upgraded case, and the log file displays.

To specify the order in which to upgrade cases

1. From the Jobs window, stop the existing upgrade jobs.
2. From **All Processing > Cases**, select the case that you want to upgrade first.
3. Click **Recover/Upgrade** to upgrade the case.

   You can view the progress of the case upgrade from the case log file that can be accessed from the Jobs window.

4. In the order that you want to upgrade the cases, select and upgrade each high-priority case.

   Note: By default, up to five cases can be upgraded at a time. If more than five cases are submitted for upgrade, the cases are upgraded in the order they are submitted.

5. After each high-priority case is upgraded, you can select the remaining cases and click **Recover/Upgrade**.

Moving Cache (On or Off) the Appliance

To improve processing efficiency, system administrators can configure the platform to store cached data in another location either on or off the appliance. This storage solution provides the flexibility and capacity for larger document caches. Thus, you can relocate cache as a method for reducing interruptions that can occur between cases when appliance storage caching is in progress. (This feature applies to the appliance as a whole. The platform does not support moving cached data at the case level.)

Before you begin: Be sure to back up your appliance before moving cached data off the appliance. (See *"Creating Appliance Backups" on page 142*.)

Best practice: After backing up your appliance, create a directory on an external file system.

To relocate cache

1. From the **System** view, click **Support Features**.
2. From the **Choose a support feature** drop-down list, select **Property Browser**.
3. Choose an appliance where you want to move cached data.
4. For selecting the case (or system), select **System**. (Moving cached data applies to the appliance only.)
5. For name of property to change, type: esa.cluster.externalBaseDir
6. To return to default settings for cached data on the appliance, leave the New value field blank. (This removes the property in order to revert to the default location on the local appliance.)
7. To move cached data off the appliance, for the New value field, type the UNC path: **`\\[`*`sharename`*`]\extdata`**

   This value will not be used by the appliance until services are restarted.

   Note: If you are moving the cache off the appliance, be sure to use a shared folder rather than a mapped drive.
8. Select the **Confirm change. Are you sure?** option.
9. Click **Submit**.
10. Stop services on the appliance.

11. Move the existing local extdata and exttemp directories to the new external path, as described in the following table:

Moving Cached Data

`esa.cluster.externalBaseDir` **value *not* set**	**`esa.cluster.externalBaseDir`** **value set**

`{esa.home}/extdata/`
`{esa.common.db.dbname}`
	`{externalBaseDir}/extdata/`
	`{esa.common.db.dbname}`

`{esa.home}/scratch/exttemp/`
`{esa.common.db.dbname}`
	`{externalBaseDir}/scratch/exttemp/`
	`{esa.common.db.dbname}`

Note: For a typical environment, there will only be one "esadb" directory for `{esa.common.db.dbname}`. It is generally safe to move the entire "extdata" directory to the external location. The target location is expected to be empty when performing the cache relocation.

12. Restart services on the appliance, then log on to the appliance.

In a cluster, the above steps should be performed for each appliance in the cluster. Each appliance must use a distinct value for the external directory. If the appliances are going to share the same device, they should each be configured to write into a different subdirectory on the device.

Managing FIPS mode for classification

Veritas eDiscovery Platform integrates with Veritas Information Classifier (VIC) to analyze and classify eDiscovery data. VIC uses both pre-defined and user-defined policies to assign classification tags to your eDiscovery data during the processing phase. Once these tags have been applied, users can view pre-selected classification filters (system tags) in the Analysis and Review mode to quickly identify documents that match the VIC tags.

Starting with release 2.4.0, VIC is Federal Information Processing Standards (FIPS) 140-2 standards compliant and meets the security requirements for cryptographic modules. When integrated with eDiscovery Platform, VIC operates in the Approved mode by default. eDiscovery Platform recommends using the default FIPS mode even though it has a slight performance degradation in the classification stage of processing.

The system administrator can change the FIPS mode by setting the system property **esa.classifier.portal.fips_arg** from **Support Features** > **Property Browser**.

The default value for this property is set to **-Dvic.fips.enable.approvedmode=true**, which keeps the FIPS mode as Approved by default.

To change the FIPS mode to the non-Approved mode, change the value of the **esa.classifier.portal.fips_arg** property to **-Dvic.fips.enable.approvedmode=false**.

After the property is changed, you must restart the **EsaClassifierService** service. Make sure that no processing job is running while you restart the service.

Note: You must perform this step on all Case Home nodes.

Summary of Additional Administrative Tasks

The following table summarizes additional tasks that administrators can perform.

Summary of Additional System Tasks

Task	Description
Defining User Accounts	A user's account and its associated user role determine the system administration tasks the user can perform, and the cases the user can search and/or administer. In addition, an access profile can override the case privileges in a user's role, and limit document visibility within a case to specific folders and/or a specific date range.
Discovering Email Server/ Archive Document Sources	To collect and process email content from Microsoft Exchange servers, Hewlett-Packard Integrated Archive Platform (IAP) archives, and/or Veritas Enterprise Vaults, you must configure the platform to discover these sources (see *"Discovering Archive Sources" in the Case Administration Guide*). You can skip this task if you plan to index content exclusively from PST or NSF files and/or other "loose" files.
Case Preparation	(Optional) Enable searches for punctuation.
Defining and Monitoring Cases	At least one case is required to specify the sources of the documents that you want to index and analyze. For example, a case might include all Exchange servers and archives in an enterprise, or a combination of Exchange mailboxes, archives, selected PST files, and one or more directories of loose files. You can also: • Monitor the indexing progress for each source and the statistics on indexed email messages and loose files (refer to *"Monitoring Source Processing Status" in the Case Administration Guide*). • Define folder names and tag categories that platform users can assign to documents in the case to expedite the review process (refer to *"Processing (or Resubmitting) Documents for OCR" in the Case Administration Guide*). • Define customized groups of internal email users to easily monitor the email activity of any arbitrary group of users (refer to *"Viewing Groups" in the Case Administration Guide*). • Define new topics used to classify email, and/or edit the topics that are discovered automatically (refer to *"Viewing Groups" in the Case Administration Guide*). If you plan to create multiple cases, consider creating templates for the most common case settings. For example, if you often use the same folder names or tag categories, define them in a template and use the template to create new cases (refer to *"Defining Case Templates" in the Case Administration Guide*).
Monitoring Appliances	Available disk space and memory can be monitored on each appliance, along with the tasks, user sessions, and the email server/ archive document sources that each appliance is allowed to access (see *"Maintaining eDiscovery Appliances" on page 101*).

Summary of Additional System Tasks (Continued)

Task	Description
Managing Schedules and Jobs	Discovery of email server/archive document sources and the processing of case document sources can be scheduled to occur automatically (see *“Managing Schedules” on page 71*). Tasks can be stopped and started as needed (see *“Viewing Jobs and Accessing Exported Files” on page 74*).
Backing Up and Restoring Cases	Cases should be backed up periodically to minimize data loss in the event of a system failure (see *“Creating Case Backups” on page 135*).
Backing Up the System Files	The system files on the primary appliance must also be backed up periodically (see *“Creating Appliance Backups” on page 142*).
Managing Licenses	You can view and update the system license (see *“Managing Your License” on page 101*).
Troubleshooting	System logs can be uploaded to Technical Support for analysis (see *“Troubleshooting” on page 156*).

Using the Support Features

Advanced support features are available to administrators who have support access granted: those users are able to access **System > Support Features** menu options. This availability applies to all the features described in this section. For more information about User Role details, see *“Defining User Roles” on page 20*.

To access the support features:

1. From the **System** view, click **Support Features**.
2. Select an item from the **Choose a support feature** drop-down list.
3. Optionally choose an appliance to which the feature will apply.
4. Specify the information in the following table, according to the selected feature. To configure an additional features, click the support … tab. An asterisk (*) Indicates a required field.

For information about Pre-Processing Reports, refer to *"Generating Processing Reports" in the Case Administration Guide*.

Support Feature Settings

Field	Description
Case Status Report	
Choose an Appliance (optional)	Select the appliance.
Checksum Comparator	
Choose an Appliance (optional)	Select the appliance.
Select the case	Case of the documents to be compared with a checksum of their content.
Document ID 1	Document ID in dotted notation or long value.
Document ID 2	Document ID in dotted notation or long value.
Clear Native View Rendering Errors	
Enter the following parameters for case*	Select a specific case to view rendering errors, or select ALL (by default).
Save output to file as TXT?	Redirects the output to a unique TXT file.
Configure SubNodes	
Choose an Appliance (optional)	Select the appliance.
Choose an Action	Select whether to Export/Import Cluster Topology.
Choose to write configuration to file	Write current cluster configuration to file. Applies when selected action is EXPORT.

Support Feature Settings (Continued)

Field	Description
Either Paste New Cluster State XML OR Enter Fully Qualified Path of XML File	Apply New Cluster State from XML String OR Cluster State will be imported from XML File. Both apply when selected action is IMPORT.
Overwrite Current Cluster State	Overwrite applies when selected action is IMPORT.
Save output file as TXT	Redirects the output to a unique .TXT file.
Confirmation Server Management	
(For Legal Hold licensed users only)	Refer to the Appendix in the *Legal Hold User Guide* for more information on how to configure your confirmation server for the Legal Hold module.
Crawler Manager	
Select the case (or system)*	Select a source for the properties.
Pattern to match	Find properties that match the specified pattern.
Name of property to change	Specify the full-qualified property name.
New value	Specify the property value, or leave blank to remove the property.
Confirm change*	Select to require confirmation of the change to the property value.
Crawler Command*	Specify the command crawler command: • **Configure**—Displays the list of settings that you can change. For an example of how to change a setting, see *"Configuring the Backup Location" on page 96*. • **Help**—Displays a description of the menu options. • **Status**—Indicates which services are enabled. • **StartCrawlers**—Enables all the Clearwell services. • **StopCrawlers**—Disables all the Clearwell services.
File Based Search	
Case	Select the case that you want to search.
Query file path	The file containing the search query terms.
Folder to restrict search	Specify which folders you want to search.
Folder for results	Specify the new folder's name. Search results will be tagged and placed in this folder. The folder is created under the Root folder. If the folder already exists, results are copied to the existing folder.
Save output file as TXT?	Redirects the output to a unique TXT file.

Support Feature Settings (Continued)

Field	Description
Firewall Browser	
Firewall Command*	The Windows firewall is enabled by default, and Clearwell applications are registered by path name as trusted applications. A system administrator can view the firewall status and settings through the Clearwell web interface. In general, changes to the firewall should be made through Windows, but several Clearwell commands are provided to configure the firewall from the appliance command line. In most cases, no changes should be necessary. Firewall command options: • **Help**—Displays a description of the menu options. • **Status**—Indicates whether the Windows firewall is enabled and displays the list of registered Clearwell applications and all registered port numbers. • **Windows**—Displays all the Windows firewall settings. • **Config**—Displays the list of Clearwell applications that are registered by name with the Windows firewall. Port number 3389 is also registered to support the Remote Desktop application. Use this option to view the Clearwell applications that must be registered with the new firewall. The following commands can be entered on the command line of the Clearwell appliance. These commands apply only to the Windows firewall. • **firewall enable**—Enables the Windows firewall (if disabled) and registers the Clearwell applications by path name. Port number 3389 is also registered for the Remote Desktop application. • **firewall disable**—Disables the Windows firewall and deregisters the Clearwell applications and ports. • **firewall status**—Displays the status of the Windows firewall and lists the registered Clearwell applications and registered ports. • **firewall reset**—Resets the Windows firewall to its original Windows server default settings. This deregisters both Clearwell and non-Clearwell applications and ports.
Save output to file as TXT	Redirects the output to a unique TXT file.
Generate new collection encryption keys	
Save output to file as TXT	Saves output to TXT file.
Get Service Tag **Note:** The service tag is required to license a server.	
Save output to file as TXT	Saves output to TXT file. This information is used when updating license information.
Image Cache Conversion	
Choose an Appliance (optional)	Select the appliance.
Within Case	Select a case.

Support Feature Settings (Continued)

Field	Description
Options	RUN_CONVERSION: Run upgrade for the selected case. BUILD_REPORT: Build Report for the selected case. ENABLE_IMAGE_CACHE_OPERATIONS: Enable Cache Operations. **Do not** use while job is running. CHECK_CASE_STATE: Checks whether the Image Cache Operations are Enabled or Disabled.
Imaging Tools Management	
(For Utility Nodes)	For details, see *Utility Node Guide*
Imports tagging Errors	
Select the case	Select the case containing import tagging errors.
Row Limit	Specify the maximum number of import tagging errors to report.
Save output to file as TXT	Saves output to TXT file.
LDAP Configuration Tester	
User Name and password	Domain user account and password used to connect to LDAP
Save output to file as TXT	Saves output to TXT file.
LDAP Utility	
Enter clear-text password*	Type a clear-text password in the field. See *“To set up authentication via LDAP” on page 46*
Algorithm	For security, you can select a password encryption algorithm.
Save output to file as TXT	Check to save the output to a .TXT file. When you click **Submit**, links to the file are displayed. If you do not select this option, the converted password is displayed on the screen under the **Submit** button.
List Frequent Terms	
criteria for list	Generates a list of terms frequently indexed within a case. Output can be saved to a TXT file.
Netit Validate and Export	
Choose an Appliance (optional)	Select the appliance.
Select the case	Choose from the cases on the system. Analyze Exported Messages Analyze Locked Production Folder Analyze All Perm Cache Analyze All Temp Cache Clear Temp Cache
Timezone Difference in minutes	Difference in (+ or -)in minutes between utility nodes and app server.

Support Feature Settings (Continued)

Field	Description
Save output to file as TXT>	Redirects the output to a unique .TXT file.
PKI Certificate Installer	
PKI Certificate information	Provide the location of the PKI certificates along with the appropriate authentication information to install the certificates on the Clearwell server.
UserName	The name of the dedicated user account
Password	Password for the user account
Save output to file as TXT	Saves output to TXT file.
Property Browser	
Select the case (or system)*	Select the case for which you want to specify properties.
Pattern to match	Find properties that match the specified pattern.
Name of property to change	Specify the fully qualified name of the property to change. To see a list of properties, click **Submit**.
New value	Specify the property value, or leave blank to remove the property.
Confirm change*	Select to require confirmation of the change to the property value.
Save output to file as TXT	Saves the output at a TXT file.
Repair Index	
Within case*	First, determine whether there is case data needing repair. Select each case that appears here. **Only cases having data that is eligible for repair will be listed.** Whether a case has data needing repair can be determined after upgrade to a version that includes this support feature. The *Upgrade Guide* for versions with this feature recommends that the **System Administrator** check for data needing Index Repair as a part of the Upgrade process. If cases appear here after upgrade, contact the **Case Administrator**, who can assess whether running Index Repair is necessary for affected cases. Only a **System Manager** or **Group Admin** can access the page with this feature.
Saved search path*	A saved search is required to run the third **Repair** step and optional **Report,** but not for **Prepare.** Saved searches are under **Analysis and Review** for the case under the **Searches** pane. Select **Actions > Edit Saved Search Folders**, then the **Saved Searches** tab. **`<Search Type>/<Folder Name>`**(if applicable)**`/<Search Name>`** in the **Folder** column is the saved search path.

Support Feature Settings (Continued)

Field	Description
Prepare case*	Second, after determining which cases need to be repaired, prepare each case. This step will analyze all the items in the case to determine which will need repair. It is required to run before **Report** and **Repair**. **Note:** Because this step requires time to complete, it is not recommended to run **Prepare** unless the **Case Administrator** determines the data should be repaired. The job will appear in the case pick-up window, and a log with the number of items needing repair will appear when completed.
Generate report	This is not required, but will generate a report that lists items requiring repair. You can also rerun the report after a **Repair** job, to see if the repair has succeeded.
Repair Index	Third, after **Prepare** case, you will be able to run the repair. It is not necessary to do it immediately. Select the case from **Within Case**, then use the **Saved Search Path** described above used to generate the report. Select **Repair Index** from the dropdown and click **Submit**. As with **Prepare** case, job progress can be viewed in the case area under **Processing Status**. When complete, the job log will appear in the case area. The log will report the number of repaired items. You can run **Generate Report** for the same **Saved Search Path** to see the number of repaired items and if there are any remaining to repair. If there are failures, try rerunning **Repair** and **Generate Report** again. If rerunning **Repair** does not fix them, look for specific information for the flagged files that failed repair on the **Processing > Exceptions** page, **File Notices** tab for the case. Give the specific failure information for the files to the case administrator, who should determine the value of taking further steps to repair them.
Source Locator Modifier	
Within case	Updates source location values for selected case (for documents whose source locations are to be modified). **Note:** This is intended for archiving source data only; do not use for moving 'Collection' sources.
OPERATION	Select whether to: • **execute**—archive source data • **verify**—verify the row counts from tables that will be affected
SOURCE	Enter the source path to be identified and replaced.
DESTINATION	Enter the destination path that would replace the source.
Save output to file as TXT	Saves output to TXT file.
System Stats	
	System statistics provide the total number of bytes processed for messages and loose files across all cases, and for each individual case. Be aware that if a case is transferred from one system to another (for example, by restoring a case backup from a different system) the system statistics for that case are not transferred and incorporated into the System Stats. To view more detailed statistics for a specific case, refer to *"Monitoring Source Processing Status" in the Case Administration Guide*.

Support Feature Settings (Continued)

Field	Description
Unmount all UNC paths mounted by Clearwell appliance	
	Click **Submit** to unmount all UNC paths mounted during identification and collection.
Unprocessed Documents	
Choose an Appliance (optional)	Select the appliance.
Select the case	Select the case for which the dropped messages need to be retrieved.
Reason Code	All reasons is the default, or select one from the dropdown.
File Format	CSV is the only option.
Unprocessed Mailboxes	
Choose an Appliance (optional)	Select the appliance.
Select the case	Case for which the dropped mailbox needs to be retrieved
Update Checksum for Emails	
Select the case*	When case data may have been partially indexed in different versions of the eDiscovery Platform with upgraded versions of Microsoft Office and Lotus notes, this may result in the same items having different checksums. The purpose of this feature is to deduplicate data where upgraded versions of Microsoft Office and Lotus client that use updated checksum calculation methods prevent complete deduplication. **Note:** Users with data indexed in a version previous to 8.1, and have indexed data with upgraded versions of these clients, should consult this feature to see if there are cases that are affected. First, determine whether there is case data affected by this on the system. Select each case that appears here. **Only cases having data that needs to be scanned will be listed.** Whether a case has data needing repair can be determined after upgrade to a version that includes this support feature. The *Upgrade Guide* for versions with this feature recommends that the **System Administrator** check for data needing the checksum update as a part of the Upgrade process. If there is, the **System Administrator** should consult the **Case Administrator** to determine if running this scan on the case is necessary, and to coordinate timing. Only a **System Manager** or **Group Manager** can access the page with this feature.

Support Feature Settings (Continued)

Field	Description
Submit	Second, once you have selected the case, click **Submit** to start the job. The scan will run on PST, MSG, and NSF files. Attachments are not affected by the hash mismatch. Observe job progress in the **Job Log**. When the job is complete, the log will state **Job Finished**, whether the update completed successfully, and where the csv file is available. Third, check the summary and CSV report: A **Log Summary** will generate, giving the last three lines of the job log: numbers of each file type to be deduplicated, the number of successfully deduplicated items, and a statement that the job is complete. **CSV "Finalresult"** is a detailed list of updated items identified by DocID, with the original and updated crawler checksum IDs. **Note:** If items fail to update successfully, the **Case** or **Group Administrator** should investigate the job log and CSV "Finalresult" for details. Some items may be corrupted, missing from the original location, or were opened by another process when the update job was running. Once any issues have been addressed, the case should be scanned by running the feature again, as in steps one through three. The case will no longer appear in the pulldown after the data checksums have been updated completely.
Upload to Support	
Name	Enter a name to identify the log file package to send. A timestamp is automatically appended to the name.
Current Appliance Only	Select the check box to restrict the logging only the appliance that was selected. If this check box is not selected, log content from all appliances for which the selected appliance is the primary is sent.
Date Range	Includes logs for all dates, or limit the logs to today or from a specified date to the current time. Click 📅 to specify the starting date.
How to Send	Select whether to send the information to Clearwell by HTTPS or to generate a ZIP file.
Include Extra System Information	Select the check box to include additional information, such as windows system and application event logs and case information. Because this option requires system communication and processing resources, considering deselecting this check box if you are concerned about system load.

Support Feature Settings (Continued)

Field	Description
Utility Node Resource Management	
Mode	Each mode performs a different management task. • **Add Utility Node**—adds a node. Specify the **Utility Type - Retriever** and use the **Utility Nodes to Add/Remove** field to specify the node name. • **Remove Utility Node**—removes a node. Specify the **Utility Type - Retriever** and use the **Utility Nodes to Add/Remove** field to specify the node name. • **Resource List**—generates a list of resources. Select the node by using the **Utility Node** menu. Select the type of Resource with the **Resource Type** menu. • **Statistics**—provides the following statistics for the node: Job Count, Error Count, Capacity, and Conversions currently taking place. Specify the **Utility Type - RETRIEVER**. Select the node by using the **Utility Node** menu. (Optional) You can select the number of hours to be used in the **Hour-range to be used for Statistics Mode** menu. • **Configure Resource Manager**—enables you to define a new resource manager. Specify the new resource manager by using the Resource Manager Host Name field. • **View Retriever Source Mappings**—provides the mappings of PST/NSF source files to the PST/NSF retrievers running on various nodes. No other fields are required to perform this task.
Utility Node	Name of the node.
Resource Type	Type of resource. The list of resource types includes ALL, PST, or NSF.
Utility Type - RETRIEVER	Check this box to configure nodes for Retrievals. Actions that will use this are ADD_UTILITY_NODE and REMOVE_UTILILTY_NODE.
Hour-range to be used for Statistics Mode	Select the number of hours to be used to generate statistics.
Utility Nodes to Add/ Remove	When adding or removing utility nodes, specify the node name.
Resource Manager Host Name	When configuring the resource manager, provide the new resource manager name in this field.
Save output to file as TXT	Check to redirect output to a unique TXT file.

Backup and Restore

This section describes basic administrative tasks involving backup and restore.

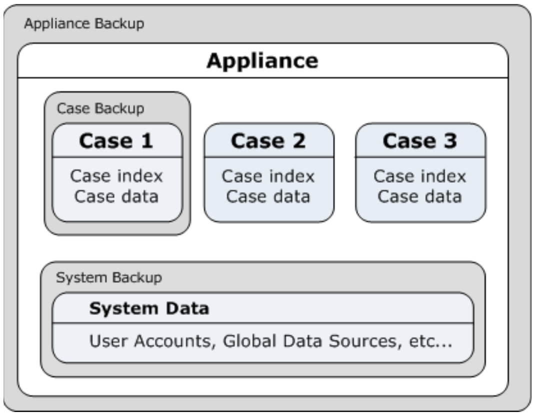
- *"About Backups" on page 127*
- *"Common Backup Practices" on page 130*
- *"Creating Collections Backups" on page 132*
- *"Creating Case Backups" on page 135*
- *"Creating Appliance Backups" on page 142*
- *"Creating System Backups" on page 149*
- *"Backing up a Cluster" on page 150*
- *"About Archiving" on page 150*
- *"Managing Backups and Archives" on page 151*
- *"About Restore" on page 152*
- *"Migrating Cases" on page 153*
- *"About Backing up Case Source Data" on page 154*

About Backups

Creating a backup routine is a critical aspect of system administration. You can back up your eDiscovery Platform data by case, appliance, and system. Cluster backups are performed through a combination of backup types.

Note: The product does not back up source case files (such as PST, NSF, Loose Files, and converted files) in either a case or appliance backup. You need to back your source files up using a separate data backup product.

The following diagram illustrates the difference between case, appliance, and system backups.



Collections Backups

Creating a backup for your collections is a critical aspect of collections administration. You can backup your eDiscovery Platform data by running an on-demand, or scheduled backup. You may also want to change the default backup destination.

For information about regular collections administrative tasks, refer to the section *"Collection Administration and Maintenance" in the Identification and Collection Guide*.

Note: Only the eDiscovery Platform's catalog of collections, tasks, data map sources, custodians, and locations are backed up, not the data preserved at your storage destinations. Data map and collection areas cannot be viewed or modified while the backup job is running.

Case Backups

Case backups contain all the index and database information related to the selected case, including user-generated tags and notes. Case backups are used to checkpoint a case, that is, restore a case to a previous state. Case backups can also be used as a tool to transfer cases to different appliances. See *"Creating Case Backups" on page 135*.

Note: For more information about case backups in a distributed environment, refer to the *Distributed Architecture Deployment Guide*.

Appliance Backups

Appliance (or node) backups include all index and database information for all cases on the appliance. Node/appliance backups enable you to restore an appliance and are the backup option to guard against appliance failure. See *"Creating Appliance Backups" on page 142*.

Note: When you restore from an appliance backup you restore the entire appliance. You cannot restore specific cases from an appliance backup.

System Backups

System backups include the system files on the primary appliance required to restore a cluster on a new primary appliance. System backups *do not* include all system data.

The following data is not included in a system backup. You can only obtain this data from an appliance backup:

- System statistics and logs
- List of data sources enabled for each cluster appliance
- Schedules or history of system-level jobs (such as backup/restore)
- Backups or exported results stored on the primary appliance

System occur as part of a node backup and can be included when performing a case backup, See *"Creating System Backups" on page 149*.

Cluster Backups

Cluster backups are a combination of backups that enable you to restore the cluster. There are two backup combinations that can result in a successful cluster backup.

- Appliance backups for each appliance (which include a system backup)
- Case backups for all cases AND a system backup

For more information in this guide, see *“Backing up a Cluster” on page 150*

Note: For more information about node backups in a distributed environment, refer to the *Distributed Architecture Deployment Guide*.

Common Backup Practices

The following tips represent common backup practices in use by customers.

Backup Frequency

- **On-demand Case Backups**
  - After initial case processing has completed and before end-user work begins.
  - Before processing additional batches.
    Because the node backup does not allow you to back out or delete processed batches, strategically-used case backups provide a way to back out problematic batches.
- **Scheduled Case Backups**

  Based on checkpoint requirements, case-level backups are often scheduled to run nightly with a rolling 7-day case backup history.
- **Scheduled, Appliance Backups**

  Based on recovery sensitivity, an appliance-level backup is often scheduled to run weekly during an off-hour weekend backup window.

For more information on creating your backup schedule, see *“Developing your Backup Routine” on page 131*.

Backup Location

Your case and system files should be backed up periodically on an external device for disaster recovery in the event of an appliance failure.

- The backup destination for case- and appliance-level backups should be changed to a network-based directory off of the appliance.
- If the backup destinations are not changed, it is suggested to schedule a script to copy any local backups off of the appliance to a network-based directory (This script is not provided by Veritas).

Note: A high bandwidth, low latency network connection between the appliance and the destination backup network directory is strongly recommended.

Cautionary Practices

- **Using Third-party backup software packages**

  Third-party backup software is often unable to back up the MySQL database and other locked files while the eDiscovery Platform services are running.

  Note: Do not attempt to back up cases manually by copying the case data store folders on the appliance. Case information is stored in multiple locations.

Developing your Backup Routine

You can implement a range of different backup strategies based on your end-user requirements for check-pointing and your sensitivity to recover in the event of a failure.

The following scenarios describes how the (intensity of use) impacts your backup routine. These examples are on opposite ends of the spectrum. Your environment will most likely fall between these cases.

Scenario: Your eDiscovery server is in constant use.

- Case administrators and reviewers work late into the night
- You have several large cases
- Processing jobs run most weekends while users are offline

Recommendation: Schedule case backups nightly and appliance backups for every weekend.

Reason: If your cases are being used during off-peak business hours or your cases are very large, your nightly case backups are likely to fail.

Case backups automatically fail if a user is logged into the case: if users work on case files after business hours, the case backup will not run.

If cases are large, the nightly backup might not complete by the time users are ready to start reviewing again. In this situation, the backup is likely to be canceled so the work can continue. Repeated cancellations of your case backups can put your work product at risk by not having an up-to-date backup.

To address this, you can ensure that you get a weekly backup by running an appliance backup over each weekend. Appliance backups ensure your work product and appliance are backed up. The downside is that appliance backups shut down the system and can interfere with other tasks that are likely to be scheduled for non-working hours.

Summary: If case backups fail every night, use an appliance backup every weekend. Schedule a maintenance window to ensure processing jobs do not interfere with the appliance backup.

Scenario: Your eDiscovery server has no off-hour traffic and your cases are not too large.

Recommendation: Schedule case backups every day and appliance backups monthly or as needed.

Reason: If your cases and system backup regularly, you can restore your cases without the need of an appliance backup. Appliance backups provide more system data than a system backup, however, you can perform appliance backups on a less rigorous schedule.

The Benefit: Weekend processing time (when users are not online and accessing cases) can be used to process, create productions, and perform other tasks which require users to be offline.

Creating Collections Backups

This section describes setting the location for your collection backups and how to run a backup on your data map and collections.

- *"Configuring the Collections Backup Location" on page 132*
- *"Running an On-Demand Collections Backup" on page 133*
- *"Scheduled Collections Backups" on page 134*

Configuring the Collections Backup Location

By default, system backups are saved on the local appliance. Veritas recommends saving backups on Identifications and Collection to a shared network location for disaster recovery in the event of an appliance failure. Saving backups to an external location also makes it easier to move cases between appliances in a cluster to optimize the use of available disk space. To perform Collections backups, refer to *"Running an On-Demand Collections Backup" on page 133*.

To change the backup location

1. From the **System** view, click **Support Features**.
2. Select **Property Browser** from the feature menu, and click **Submit** to view the properties that you can change.
3. Enter the following information. An asterisk (*) indicates a required field.

Directory Properties

Field	Description
Name of property to change	Enter the following property name: `esa.case.backupDir` You can change this value by editing the `esa.case.backupDir` property using the **Property Browser** support feature. You must specify the **backupDir** for each appliance in the cluster by repeating the process for each appliance in the **Choose an appliance** drop-down list. You must also set the `esa.case.sharedBackupDir` property to **true** in order for the cluster to recognize the backupDir location as a shared location that is visible by all appliances in the cluster. It is not necessary to set this property for each appliance in the cluster.
New value (leave blank to remove)	Enter the full path of the backup location in Uniform Naming Convention (UNC) format (up to 256 characters). For example: `\\pine\backup_folder`
Confirm change*	Select the check box to confirm the change.

4. Click **Submit** to apply the change.

Running an On-Demand Collections Backup

On-demand backups are a convenient way to save collected data should your data become unusable or source data unavailable. Running a collections backup will also backup any legal holds.

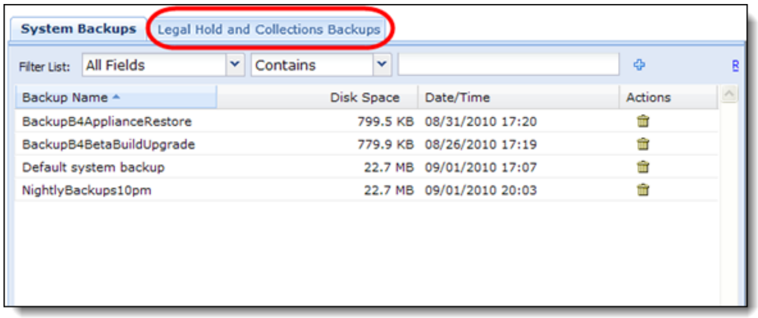
It is typical to perform an on-demand collections backup after collected new data and before the case management workflow begins.

To backup a collection on demand

Before you begin: Verify that no one is currently accessing the collection.

To backup a collection, you must have the Collections Admin role with collection management permissions.

1. From the **System** view, click **Backups.**



Backup Name	Disk Space	Date/Time	Actions
BackupB4ApplianceRestore	799.5 KB	08/31/2010 17:20	🗑
BackupB4BetaBuildUpgrade	779.9 KB	08/26/2010 17:19	🗑
Default system backup	22.7 MB	09/01/2010 17:07	🗑
NightlyBackups10pm	22.7 MB	09/01/2010 20:03	🗑

2. Click the **Legal Hold and Collections Backups** tab.

   The Backups page displays showing any backups previously performed.

3. Click **Start New Backup...**

4. Provide a backup name.
   Best Practice: Only use alphanumeric characters in backup names.

5. Select the option to perform a system backup on completion.

   The system will not be available during a system backup. The platform delays user-performed operations that impact the system until the system backup completes. System backups typically run between 1-5 minutes.

6. Click **Start Backup**.

   The backup begins.
   The duration of a collections backup depends on the size of the collection and the backup location.

Next Steps:

- To stop the backup, click **Pickup** at the top of the page, and click **Stop**.
- To verify that the backup was successful, go to **System** > **Jobs**. Successful jobs are automatically pruned from the jobs list. If you do not see the backup in the Jobs pane and it has completed running, it was successful.

Scheduled Collections Backups

Scheduled collections backups help you maintain a set of up-to-date backups on all collected data.

Each scheduled collection backup overwrites the most recent backup with the same backup name. If you need to preserve multiple copies of a collection backup, schedule a weekly backup to occur on each day of the week.

For example, you can create seven weekly-backup schedules with one backup for each day of the week. This would result in a scheduled Sunday backup, Monday backup, Tuesday backup, Wednesday backup, Thursday backup, Friday backup, and Saturday backup.

Note: If you schedule several weekly backups and plan to have a full, appliance backup over the weekend, consider skipping a case backup on Saturday and Sundays since they may be redundant to other backup types.

To schedule a collection backup

Before you begin: To backup a collection, you must have the Collection Admin role with collection management permissions.

1. From the **System** view, click **Schedules**. The Schedule pane displays with a list of current schedules.
2. At the bottom of the Schedule pane, click **Add.** The Add Schedule page displays.
3. From the Task Type menu, select **Backup**.
4. Set the Initial Run Date, Start Time.
5. Choose whether the backup should be run daily or weekly.

   Remember that scheduled collection backups overwrite the most recent backup with the same backup name.
6. Select **Enabled** to run the scheduled backup at the next scheduled time.
7. If there are existing cases you want to back up at the time of the collection data backup, choose either all, or selected cases that you want to backup.

   Note: If the collection backup name is changed after setting up a backup schedule, the new name is automatically added to the schedule, and the collection continues to be backed up. Backups made with the old name are not deleted.
8. If you also want to back up the system at the same time, select **System backup**.
9. Select **Collections, Data Map backup**.

10. Provide a name for the collection backup.

    Best Practice: Only use alphanumeric characters in backup names.

    Note: The eDiscovery system will not be available during a system backup. The platform delays user-performed operations that impact the system until the backup completes, if the collections backup includes a system backup. System backups typically run between 1-5 minutes.

11. Click **Save**.

    The new collection backup displays in the Schedule pane.

Next Steps:

- To view when the backup ran, go to **System** > **Schedules**. The Last Run column lists the most recent time that the backup ran.
- To verify that the backup was successful, go to **System** > **Jobs**. Successful jobs are automatically pruned from the jobs list. If you do not see the backup in the Jobs pane and it has completed running, it was successful.

To view the collection backup schedule

- You can view all scheduled tasks, including backups, from **System** > **Schedules**.

The Schedule pane describes when the task is scheduled to run, when it was last run, and whether the task is enabled.

For more information about other collection administration tasks, refer to the section *"Collection Administration and Maintenance" in the Identification and Collection Guide*.

Creating Case Backups

Case-level backups are often used to checkpoint end-user work in order to provide a point-in-time backup of tags, exports, etc. for the case. Case backups are recommended before indexing new data, large tagging operations, or other substantial changes.

Additionally, you can use case backups to move cases from one appliance to another. As a case becomes larger and requires more disk space, you can move the case to another appliance by backing up the case and then restoring it to another appliance in the cluster.

Note: eDiscovery Platform supports cases created in 7.x and later releases.

Case backups can be performed on-demand or scheduled to run on a daily or weekly basis.

Note: For more information about case backups in a distributed environment, refer to the *Distributed Architecture Deployment Guide.*

Case Backup Characteristics

- All index and database information related to the selected case is backed up.

- Source case files (PST, NSF, Loose Files, converted files, etc.) are never backed up in either a case, appliance, or system backups.
- **Best Practice:** Only use alphanumeric characters in backup names.
- For a case backup to start, all users must be logged out of the case and no jobs related to the case can be running (for example, processing or export jobs).
- Once started, users cannot access the case until the case backup completes.
- By default, case backups are saved locally to the appliance at
  `D:\CW\<current_product_version>\caseBackups\cases`

On-Demand Case Backups

On-demand backups are a convenient way to mark milestones in a case workflow. You can create checkpoints to establish fallback positions should your data become unusable.

It is typical to perform an on-demand, case-level backup after indexing any new data and before end-user work begins.

To backup a case on demand

Before you begin: Verify that no one is currently using the case.

To backup a case, you must have System Management permissions.

1. From the **All Processing** view, click the **Cases** tab.
2. Select the check box of the case you want to backup.
3. Click **Backup.**

   The Backup Case screen displays.
4. Provide a backup name.
   Best Practice: Only use alphanumeric characters in backup names.
5. Verify that you want to perform a system backup on completion.

   The system will not be available during a system backup. The platform delays user-performed operations that impact the system until the system backup completes. System backups typically run between 1-5 minutes.
6. Click **Start Backup**.

   The backup begins.
   The duration of a case backup depends on the size of the case and the backup location.

Next Steps:

- To stop the backup, click **Jobs** at the top of the screen, and click **Stop**.
- To verify that the backup was successful, go to **System > Jobs**. Successful jobs are automatically pruned from the jobs list. If you do not see the backup in the Jobs pane and it has completed running, it was successful.

Scheduled Case Backups

Scheduled cases help you maintain a set of up-to-date backups.

Each scheduled case backup overwrites the most recent backup with the same backup name. If you need to preserve multiple copies of a case backup, schedule a weekly backup to occur on each day of the week.

For example, you can create seven weekly-backup schedules with one backup for each day of the week. This would result in a scheduled Sunday backup, Monday backup, Tuesday backup, Wednesday backup, Thursday backup, Friday backup, and Saturday backup

Note: If you schedule several weekly backups and plan to have a full, appliance backup over the weekend, consider skipping a case backup on Saturday and Sundays since they are redundant to the appliance backup.

To schedule a case backup

Before you begin: To schedule a case backup, you must have System Management permissions.

1. From the **System** view, click **Schedules**.

   The Schedule pane displays with a list of current schedules.

2. At the bottom of the Schedule pane, click **Add.**

   The Add Schedule screen displays.

3. From the Task Type menu, select **Backup**.

4. Set the Initial Run Date, Start Time.

5. Choose whether the backup should be run daily or weekly.

   Remember that scheduled case backups overwrite the most recent backup with the same backup name.

6. Select **Enabled** to run the scheduled backup at the next scheduled time.

7. Select the case or cases that you want to backup.

   Note: If the case name is changed after setting up a backup schedule, the new case name is automatically added to the schedule, and the case continues to be backed up. Backups made with the old case name are not deleted.

8. Provide a backup name.

   You identify specific case backups from the combination of Case name and Backup name.

   For example, you can identify your Tuesday backup of your case named, Patent Lawsuit by naming your backup “Tuesday”. From the **All Processing > Backups** screen, each case name displays with the backup name.

   Best Practice: Only use alphanumeric characters in backup names.

9. Verify that you want to perform a system backup on completion.

   The system will not be available during a system backup. The platform delays user-performed operations that impact the system until the system backup completes. System backups typically run between 1-5 minutes.

10. Click **Save**.

    The new case backup displays in the Schedule pane.

Next Steps:

- To view when the backup ran, go to **System > Schedules**. The Last Run column lists the most recent time that the backup ran.
- To verify that the backup was successful, go to **System > Jobs**. Successful jobs are automatically pruned from the jobs list. If you do not see the backup in the Jobs pane and it has completed running, it was successful.

To view the case backup schedule

- You can view all scheduled tasks, including backups, from **System > Schedules**.

  The Schedule pane describes when the task is scheduled to run, when it was last run, and whether the task is enabled.

Managing the Case Backup Destination

By default, case backups are saved locally to the appliance at **`D:\CW\<current_product_version>\caseBackups`**\cases.

For a higher level of redundancy and to simplify management of clustered deployments, direct case backups to a shared network location.

Tip: Veritas strongly recommends a high-bandwidth, low-latency network connection between the appliance and the destination network share.

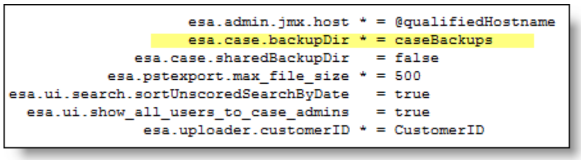
To view the case backup destination

1. From the **System** view, click **Support Features**.
2. Select **Property Browser** from the drop-down menu.
3. Select the appliance that hosts the case.

4. Click **Submit**.

   The backup directory displays as the **`esa.case.backupDir`**.

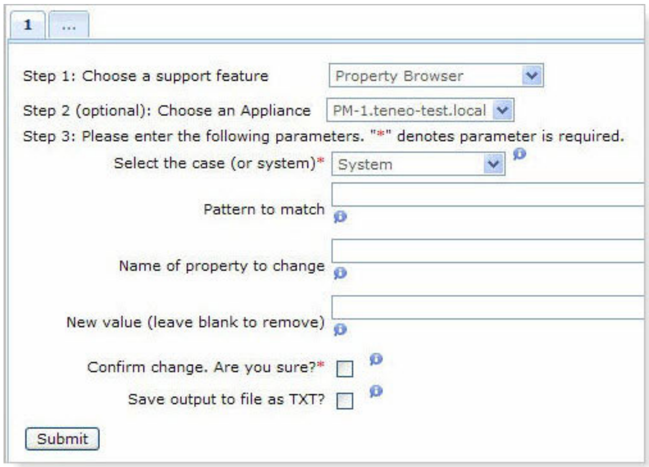
   In the following example, the default **`caseBackups`** directory is being used.



```
                    esa.admin.jmx.host * = @qualifiedHostname
                    esa.case.backupDir * = caseBackups
              esa.case.sharedBackupDir   = false
           esa.pstexport.max_file_size * = 500
esa.ui.search.sortUnscoredSearchByDate   = true
  esa.ui.show_all_users_to_case_admins   = true
               esa.uploader.customerID * = CustomerID
```

To change the backup location

1. From the **System** view, click **Support Features**.
2. Select **Property Browser** from the feature menu, and click **Submit** to view the properties that you can change.



Step 1: Choose a support feature: Property Browser

Step 2 (optional): Choose an Appliance: PM-1.teneo-test.local

Step 3: Please enter the following parameters. "*" denotes parameter is required.

Select the case (or system)*: System

Pattern to match

Name of property to change

New value (leave blank to remove)

Confirm change. Are you sure?* □

Save output to file as TXT? □

3. Enter the following information. An asterisk (*) indicates a required field.

Directory Properties

Field	Description
Name of property to change	Enter the following property name: **`esa.case.backupDir`** You can change this value by editing the **`esa.case.backupDir`** property using the **Property Browser** support feature. You must specify the **backupDir** for each appliance in the cluster by repeating the process for each appliance in the **Choose an appliance** drop-down list. You must also set the **`esa.case.sharedBackupDir`** property to **true** in order for the cluster to recognize the backupDir location as a shared location that is visible by all appliances in the cluster. It is not necessary to set this property for each appliance in the cluster.
New value (leave blank to remove)	Enter the full path of the backup location in Uniform Naming Convention (UNC) format (up to 256 characters). For example: *\\pine\backup_folder*
Confirm change*	Select the check box to confirm the change.

4. Click **Submit** to apply the change.

Troubleshooting Case Backups

A case backup (either on-demand or scheduled) will fail if:

- A user is logged into the case being backed up.
  By default, users are automatically logged out after 30 minutes of inactivity.
- The case name includes special characters such as ampersand ("&").
- Another job (processing, tagging, export, etc.) is running for the case being backed up.
- Your virus scanning software is setup incorrectly.
  Verify that the **`mysqltemp`** directory is excluded from your virus scans. If the **mysqltemp** directory is scanned, the virus scanner is likely to quarantine or delete the files. These files are necessary for backups to complete successfully.

Note: If the backup for a case fails, scheduled backups for other cases are still attempted.

Case Backup Maintenance

To ensure that backups run smoothly, perform the following tasks periodically.

Check Disk Space and Date/Time of backups

From the **All Processing** view, click **Backups**. On the Backups screen, you can check the Disk Space and Date/Time of the case backups.

- Disk Space - Case backups contain the case's entire job output, including any export jobs for the case. Cases with large export jobs can result in larger-than-expected backup sizes.

  Note: The available disk space at the backup destination should be frequently monitored to ensure there is adequate disk space for the backups.
- Date/Time - Verify that backups complete during the desired backup windows. If you find that backups are running over their allotted time, you can reduce the number of cases being backed up in an evening or move inactive cases to archive status.

View Failed Backup Jobs

From the **System** view, click **Jobs** and check for any failed case backup jobs.

Unneeded case export jobs can be deleted from here to reduce the size of a case's backup.

Delete Backups

You might want to delete unwanted backups if you are running low on disk space.

To delete a case backup

- From the **All Processing > Backups** screen, find the unwanted case backup and click the delete icon.

Creating Appliance Backups

Appliance (or node) backups are often used to guard against the rare event of an appliance failure. Appliance backups include index and database information for all cases on the appliance into a single appliance backup package.

Appliance backups are performed through the desktop Clearwell Utility or through a command line script. Appliance backups can be scheduled to run on a daily or weekly basis or performed on-demand. See *"Common Backup Practices" on page 130* for more information on determining the frequency of your backups.

Appliance Backup Considerations

- An appliance backup stops all eDiscovery services for the entire duration of the backup. This will render the user interface unusable during the appliance backup.
- Old appliance backups are not purged through the scheduled appliance backup process.

  Consideration should be given to periodically clean up the old appliance backups from the destination appliance backups directory.
- If the appliance backup destination is modified to point to a network share, the Windows account you are logged in as when running an on-demand appliance backup needs to have read/write permissions to the network share.
- Appliance backups do not include case backups unless the users chooses to do so. If case backups are running regularly enough to prevent loss of data, it is not required to include them in the appliance backup.

WARNING: Do not schedule appliance backups and case backups to run at the same time. Appliance backups include case backups. If a case backup starts and is interrupted by an appliance backup, the case backup will restart after the appliance backup completes. This is not harmful, but can result in extra time being committed unnecessarily to the backup process.

On-Demand Appliance Backups

On-demand appliance backups are performed on the appliance through the Clearwell Utility.

To backup an appliance on demand

1. On the appliance, double-click the Clearwell Utility icon (shortcut icon on the desktop).

   A shortcut link to the Clearwell Utility is also on the appliance desktop.
2. Type `1` to perform an appliance backup.

   All eDiscovery services will be stopped and the appliance backup will prompt the user for the following information:

   A. Type the appliance backup name.
   Best Practice: Only use alphanumeric characters in backup names.

   B. Would you like to backup log files?
   Type **`yes`**. Backup log files are not necessary to restore an appliance, however, they help with debugging issues.

C. Would you like to backup case backups?
Type `no`.

Each case is backed up into the appliance backup package. This option determines whether or not to also backup any existing case-level backups into the appliance backup package.

Note: This prompt should not be presented if the case backup destination has been changed to a remote location. If the option displays, type `no`.

Scheduled Appliance Backups

The platform provides a backup script to use for scheduling appliance backups. Using this script in conjunction with the Windows Scheduled Task Wizard is the recommended way to schedule appliance backups.

The scheduled backup script will copy the appliance backup to the configured backup appliance destination using a folder named with the backup date and time in the form YYYYMMDD_HHMM. For more information on changing the backup appliance destination, see *"Managing Appliance Backup Destination" on page 146*.

When using the backup script, log files are backed up and case backups are not backed up.

Note: Scheduled appliance backups are less common than on-demand appliance backups. Because large processing and production tasks tend to occur during optimal backup windows, it is likely that a backup cannot be scheduled at a predictable interval.

To schedule an appliance backup
For clustered deployments, the backup script on each appliance in the cluster should be configured to run at the same time.

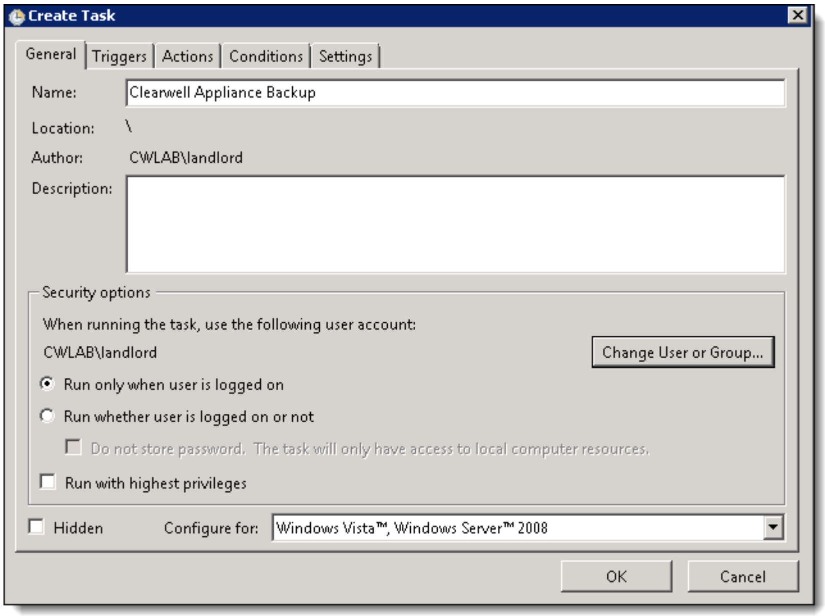
Before you begin: This procedure must be completed on each appliance in the cluster.

1. On the appliance, access Scheduled Tasks from the Control Panel.

   Click **Start** > **Administrative Tools> Task Scheduler>**

2. When the Task Scheduler opens, click on **Create Task...** under **Task Scheduler (Local)**.

3. On the **General** tab:



Name: Clearwell Appliance Backup

Location: \

Author: CWLAB\landlord

Description:

Security options

When running the task, use the following user account:

CWLAB\landlord

● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

A. Type in a name for the task (such as “eDiscovery Appliance Backup”).

B. It may be necessary to have the task run as a user that is different from the user currently logged in. If so, the same user that is running the EsaApplicationService is a recommended alternative user. To change the user, click the **Change User or Group...** box.

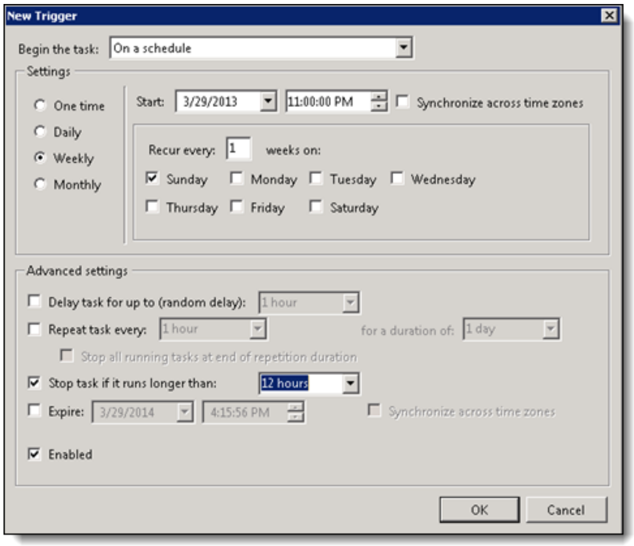
Note: If the appliance backup is writing to a remote location, it should have permissions to write to the destination.

C. Check **Run whether user is logged in or not**.

D. Check **Run with highest privileges**.

E. Click the **OK** button.

4. Click the **Triggers** tab and click **New**.



Begin the task: On a schedule

Settings

○ One time
○ Daily
● Weekly
○ Monthly

Start: 3/29/2013 11:00:00 PM □ Synchronize across time zones

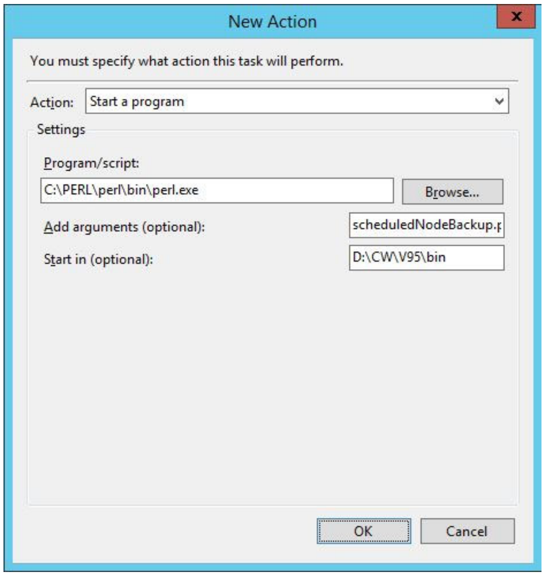
Recur every: 1 weeks on:

☑ Sunday □ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday □ Saturday

Advanced settings

□ Delay task for up to (random delay): 1 hour
□ Repeat task every: 1 hour for a duration of: 1 day
□ Stop all running tasks at end of repetition duration
☑ Stop task if it runs longer than: 12 hours
□ Expire: 3/29/2014 4:15:56 PM □ Synchronize across time zones
☑ Enabled

5. Click the **Actions** tab and then click **New**.



You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: C:\PERL\perl\bin\perl.exe

Add arguments (optional): scheduledNodeBackup.p

Start in (optional): D:\CW\V95\bin

A. Click **Browse** and then navigate to ***C:\PERL\perl\bin\perl.exe***.

B. In the **Add arguments (optional)** field, enter **scheduledNodeBackup.pl**.

C. In the **Start in (optional)** field, enter the starting directory. For example, *D:\CW\V10\bin*.

D. Click **OK** when done.

Note: The Task Scheduler command paths must be modified after each major upgrade of the eDiscovery Platform.

6. The default settings for **Conditions and Settings** must not be edited.
7. Click **OK** to save the task.
8. Enter in the account password for the **esaApplicationService** account, and then click **OK**.
9. Validate that the newly created task runs correctly:

- Backups will stop all eDiscovery services, so the time chosen for backups should be when no users will be accessing the appliance, or in the case of a distributed architecture deployment, any of the appliances in the cluster.
- The backup node location should also be checked to verify that it can be created. The default location is:
  `D:\CW\<current_product_version>\backups\`
- The `scheduledNodeBackup.pl` script generates a log to the D:\CW <version number> directory, which should be examined for errors.

Managing Appliance Backup Destination

By default, appliance backups are saved locally to the appliance under

`D:\CW\<current_product_version>\backups\`

For a higher level of redundancy and to simplify management in clustered deployments, it is possible to direct the appliance backup destination to a network share.

Veritas strongly recommends a high bandwidth, low latency network connection between the appliance and the destination network share.

If the appliance backup destination is modified to point to a network share, the Windows account you are logged in as when running an on-demand appliance backup needs to have read/write permissions to modify the network share.

To verify that the user account has modification permissions

1. Log in to the appliance with the user account being used for the backup.
2. Create a temporary directory.
   - If it succeeds, the user account is configured correctly.
   - If you cannot create a temporary directory with the user account, modify the user account permissions or update the service to run under a user account with the correct permissions.

To view the appliance backup destination

- The default location of an appliance backup is:
  `D:\CW\<current_product_version>\backups\`

To determine if the location has been changed from the default

1. From the appliance, view the **`config.properties`** file.

   ```
   D:\CW\<current_product_version>\config\configs /
   \esauser\config.properties
   ```

2. Search the file for the auto.backup.dir property.
   This property configures the appliance backup directory.

   Note: If it is not listed, the default location is being used.

To change the appliance backup destination

Create a network directory to store the backups which is accessible via UNC from the appliance. For a clustered deployment, it is recommended to write each appliance backup to a directory of the same name such as:

```
\\FileShareServer\Directory\applianceBackups\Appliance1
\\FileShareServer\Directory\applianceBackups\Appliance2
\\FileShareServer\Directory\applianceBackups\Appliance3
```

1. Open the **`config.properties`** file under

   ```
   D:\CW\<current_product_version>\config\configs /
   \esauser\config.properties
   ```

2. At the end of the file, insert the following lines where the UNC path is that of the respective appliance directory created in Step 1.

   Note: For this configuration property, forward slashes / must be used in the directory path syntax.

   ```
   #Configure Remote Appliance Backup directory
   auto.backup.dir=//FileShareServer/Directory/appliance-
   Backups/Appliance1
   ```

3. Save and close the file.

4. On the appliance desktop, double-click the Clearwell Commander.

5. From Action, select Stop Appliance Services. Allow services shutdown to complete.

6. Select **Build Incremental Configuration Changes**.

7. For a clustered deployment, repeat this procedure on each appliance in the cluster.

Troubleshooting Appliance Backups

Appliance backups fail in these situations.

- The appliance backup is directed to a non-existent location.
- The backup name is incorrect or misspelled.
- The appliance backup is stopped before it completes. See *"Appliance Backup Maintenance" on page 148* for information on partial appliance backups.

Appliance Backup Maintenance

Clean up partial appliance backups.

WARNING: If an appliance backup does not complete successfully, you must manually delete the backup folder. Otherwise, you might attempt an appliance restore with a partial backup, leading to the loss of your case data.

1. Navigate to the appliance backup directory.
   The backup directory destination is configured in the config.properties file. For more information, see *"To change the appliance backup destination" on page 147*.
2. Delete the directory containing the incomplete backup.
3. Rerun your appliance backup.

Check Disk Space

Verify that you have sufficient disk space for additional appliance backups.

Creating System Backups

If the primary appliance fails, a current backup of the system files is required to restore the cluster on a new primary appliance.

System backups rarely need to be performed on their own. By default, all case backups include a system backup.

You might want to create a system backup after performing the following tasks.

- Creating user accounts
- Updating or creating user roles
- Creating or editing global data sources
- Creating load file import/export templates
- Creating case templates

To backup system files

1. From the **System** view, click **Backup**.
2. Provide a name for the system backup, and click **Start Backup**.

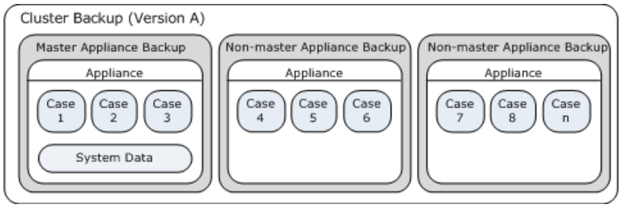
Managing System Backup Destination

The system backup destination is the same as the case backup destination. For more information, see *“Managing the Case Backup Destination” on page 138*.

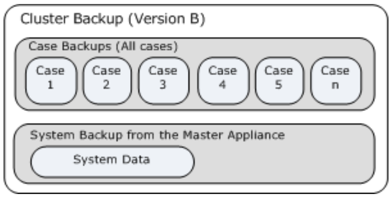
Backing up a Cluster

A combination of backups that enable you to restore the cluster:

- Appliance backups for each appliance (which include a system backup)



- Case backups for all cases **and** a system backup



About Archiving

When the platform archives a case, it creates a new backup of the case and then deletes the case from the list of active cases.

To archive a case

1. From the **All Processing** view, click the **Cases** tab.
2. Select the case you want to archive, and click **Archive**.

- You can view the archived case by clicking the **Archives** tab.

Managing Backups and Archives

A backup is a copy of a case that you make while the case is on-line and accessible. You can use backups to provide case checkpoints, or make a copy for disaster recovery purposes. A backup is portable to other eDiscovery Platform clusters provided that the cluster has a different cluster ID than the original cluster.

An archive is a final backup of a case. The system performs a backup and then removes the active version of the case from the system. The license quota is returned (the space becomes available) if you have a capacity-based license. You can restore archives, only if sufficient quota space is available to bring the base back online. Contact Veritas for licensing information.

Use the **Backups** and **Archives** tab under the **Manage Cases** screen to manage case backups and archives.

Note: Only users with the predefined System Manager role can see and restore case archives from the **Archives** tab.

To manage backups and archives

1. From the **All Processing** view, click the **Backup** or **Archives** tab.
2. Use the controls at the top of the screen to filter the list:
   A. Choose the backups you want to view from the **Show** drop-down list.

   B. Specify a date range by entering the date (mm/dd/yyyy format) or clicking the calendar icons and selecting dates.

   C. Click **Filter** to display the filters results.
3. To export a table of information from the Cases screen (in CSV format), select the backup and click **Export**.
4. To restore a backup, select the backup and click **Restore**. Verify the information, and click **Start Restore**.
   The progress of the restore is shown on the Backup screen.

About Restore

The process of restoring a backup and restoring an archived case is the same.

- Restoring a backup overwrites your current, live case data.
  To prevent data loss, verify that your backup of the live case is current before performing a backup restore.
- Restoring an archive creates a new copy of the case.
  Before restoring an archive, verify that the case will not cause the system to exceed your license quota.

To restore a backed up or archived case

1. From the **All Processing** module, click the **Backups** or **Archives** tab.
2. Find the backup or archive that you want to restore.
   - To view case backups or system backups, select All Case Backups or All System Backups from the Show menu.

   Note: System backups are view-only. To restore a system backup, contact Technical Support.

   - To view all case archives or all system archives, select All Case Archives or All System Archives.

   Note: If you are restoring either an archive or a backup that contains more data than the current live version of the case, you will need a sufficient archive restoration license quota.
3. To limit the backups for a specific date range, click 📅 to specify the from and/or to dates, and click **Filter**.
4. Select the backup or archive to restore, and click **Restore**.
5. Verify the case name, select an appliance, and click **Start Restore**.

   Note: If the backups are stored in a shared network location, you can restore a backup to any appliance. If backups are stored on the appliance, each backup can be restored only on the local appliance unless you manually copy the backup directory.

To restore an appliance or cluster

An appliance- or cluster-level restoration restores all cases in the appliance backup package. Specific cases cannot be restored from an appliance backup package.

Contact Veritas eDiscovery Platform Customer Support for assistance regarding a full appliance or cluster restoration.

Note: The platform relies on the integrity of a case backup when restoring a case, which may optionally contain empty folders. When copying a case backup from one location to another, Veritas strongly recommends the use of an application which creates a true replica of the source folder, such as Robocopy, which ships with Windows® Server 2008 and Windows Server 2012. The use of /E and /DCOPY:T are highly recommended options for backup copying.

Migrating Cases

Case migration is the process of restoring a case backup on a different appliance. You can migrate cases between appliances or clusters.

You might want to migrate a case in the following scenarios.

- To share case data with a geographically-dispersed team
- To maximize the disk space on your appliances.
  Large cases require more disk space. Distributing large cases between different appliances can improve performance.

Case Migration Considerations

You can move a case between appliances or between clusters.

When a case is moved to a new cluster, the system data associated with the appliance moves with it. This means that users with access to one cluster will have access to the new cluster when the case is moved.

The platform resolves user accounts if the information matches. If the user account information does not match, new user accounts are created on the system.

To ensure users accounts are properly defined, verify the user accounts and user roles continue to be set correctly after the case migration completes.

To migrate a case

Before you begin: In clustered environments, verify the configuration property, **`sharedBackupDir`**, is set to **`true`**.

1. Backup the case that you want to migrate.

2. Restore the case.

   – To migrate the case to a new appliance within the same cluster using a shared network location, click the Restore button and select the new appliance when prompted.

   – To migrate the case to a new cluster or to an appliance using an unshared backup location:

     A. Navigate to the case backup destination.

        The backup directory uses this structure.
        `caseBackups\cases\<case_ID>_<case_Name>\<backup_Name>`
        For example, **`caseBackups\cases\0.6.1.28_SECvsTamas\Monday-Weekly`**

        For instructions on locating the case backup destination, see *"Managing the Case Backup Destination" on page 138*.

     B. Copy the backup directory.

        In the example above, the entire **`0.6.1.28_SECvsTamas`** directory is copied.

     C. Paste the backup directory on the new appliance under the **`caseBackups\cases`** directory.

        From the platform web interface, the backup displays in the list of archived cases.

     D. From the **All Processing** module, click the **Archives** tab.

     E. Select the archived case and click **Restore**.

        The case is restored on the new appliance and displays on the Cases screen.

3. If you migrated the case to a new cluster, verify the user accounts and user roles continue to be set correctly after the case migration completes.

   Migration status displays from the **All Processing** > **Processing** > **Backups** tab. A status message displays while case migration is in progress. A message also displays if the case migration does not complete successfully.

About Backing up Case Source Data

Backing up case source data

Case source data is never backed up by the platform. Your backup routine needs to include a plan for handling case data.

Note: Archive operations do not back up content extracted from source files, such as PST and NSF files contained within container files (e.g. ZIP, RAR, and LEF files). While this does not have an impact on the outcome of your case, users may experience delays upon accessing this content for the first time upon restore. These files should be backed up separately.

To see where files are stored:

- If the backup location is defined at the system level, click **System > Settings > Locations**. The directory containing the extracted files displays.
- If a backup location was defined at the case level, select the case, choose **Processing** in the ribbon, then expand **Configure Processing Parameters and Features** to see the location specified for that case.

Backing up converted data

OST and MBOX files are converted to PSTs for processing. These converted source files are not backed up by the node backup and need to be added to your source file backup routine.

To see where converted files are stored:

- If the location is defined at the system level, click **System > Settings > Locations**. The directory containing the converted files displays.
- If a location was defined at the case level, select the case, choose Processing in the ribbon, then expand **Configure Processing Parameters and Features** to see the location specified for that case.

Troubleshooting

This section describes how to report problems to the local administrator and Technical Support. Refer to the following topics:

- *"Reporting Problems" in the next section*
- *"Managing Logs" on this page*

Reporting Problems

To report problems to the administrator, users can:

- Email your organization's Technical Support by clicking **Feedback** at the bottom of any screen. (This is configured in **System > Settings**.)
- Contact Technical Support by clicking **Support** at the bottom of any screen. This opens the website where you can access Veritas's Support Portal.
- Report an error message by clicking **Report Problem** on a displayed error message

  When the user enters a problem description and clicks **Send**, an email is sent to the address defined on the Resources screen (see *"Defining System Settings" on page 90*). The email includes a link to a zip file that contains a copy of the server and crawler logs made at the time the problem report is sent.

Managing Logs

System administrators can view all appliance and case logs, send logs to Technical Support, delete outdated logs, and change or add log settings (when instructed by Technical Support). Case administrators can send or view only the logs for their cases.

To manage the logs:

1. To manage all the logs, from the **System** view, click **Logs**.
2. To send or view the logs for one case, select a case from the **All Cases** view, and click **Logs**.
3. To send the logs to Technical Support, specify the following information, and click **Submit**. An asterisk (*) indicates a required field.

   Note: You can also upload logs by choosing **System > Support Features** and then choosing **Upload to Support** from the drop-down list.

Upload Parameters

Field	Description
Choose an Appliance	Select an appliance. If you select the primary appliance, you can upload logs for all the appliances in the cluster.
Name*	Enter a name for the uploaded logs (up to 255 characters). **Note:** When associated with a Support case, the name should be the case number.
Current Appliance Only	If you select the primary appliance, the logs are uploaded for the entire cluster by default. Select the check box to upload only the logs for the selected appliance (required if the selected appliance is not the primary).
Date Range	To limit the uploaded logs, select one of the following: • **Today**. Uploads only the logs modified today. • **Since Specified Date**.Uploads only the logs modified on or after the date specified in the **Since Date** field.
Since Date	Specify the date of the oldest log you want to be uploaded: • Click 📅 and select a month and day**.** or • Enter the date directly as: MM/DD/YYYY.
How to Send	Select one of the following options: • **HTTPS directly to Clearwell**. Posts a ZIP file directly to the technical support site. Use the HTTPS web uploader site to upload logs: https://support.clearwellsystems.com/uploads/upload.html • **Generate ZIP file to send manually**.Stores a ZIP file on the appliance. To view the file location, click **Jobs** at the top of the screen, and click 📁 in the status column when the task is complete.
Include Extra System Information	Include additional case-related system information, windows system and application event logs. Veritas recommends that you deselect this check box if your system is heavily loaded or responding slowly.

4. To view or purge the logs, click the **View Logs** tab. To change the log settings, click the **Settings** tab. These options should be used only with guidance from Technical Support.

Appendix A: Web Services Access Options

This appendix describes how to configure your system to optimize access to the Web user interface.

Refer to the following topics in this section:

Web Interface Access Ports

In the eDiscovery Platform, there are *Default Ports* each of which enables either HTTP or HTTPS; however administrators have the option of *Redirecting all HTTP Requests to HTTPS*.

Default Ports

By default, both HTTP and HTTPS are enabled for accessing the eDiscovery Platform web interface. HTTP is enabled on port 80 and HTTPS is enabled on port 443. Each of these ports may be changed from their default ports. Please contact Customer Support for additional detail.

Redirecting all HTTP Requests to HTTPS

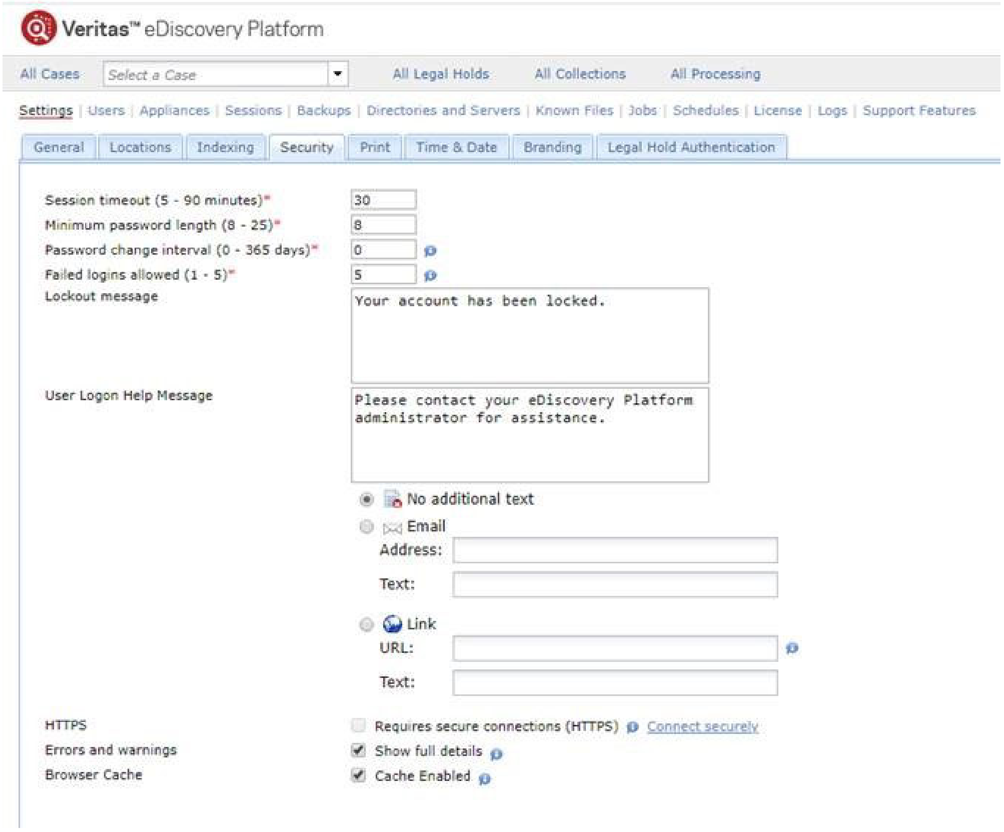
The product provides a feature to re-direct all HTTP requests to the HTTPS port. It is strongly suggested to enable this feature for Internet accessible deployments or deployments that require stringent security.

To redirect HTTP requests to HTTPS

1. Under **System > Settings** select the **Security** tab.

2. Select the option **Requires secure connections (HTTPS)**.

   Note: This option may only be enabled while connected via HTTPS. View the info bubble for additional detail.


Veritas™ eDiscovery Platform
All Cases
Select a Case
All Legal Holds
All Collections
All Processing
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: □ Requires secure connections (HTTPS) Connect securely

Errors and warnings: ☑ Show full details

Browser Cache: ☑ Cache Enabled

Cluster Considerations

All appliances in a cluster should be configured with the same **Requires secure connections** setting.

Consult your IT department’s security specialists to determine secure settings for your browser. For more information about SSL/TLS communication, refer to:

“Configuring User Authentication for LDAP” on page 45

“Secure LDAP SSL/TLS Support” on page 57

“SSL Configuration Details” on page 161

Certificates

Refer to the *Certificate Options Summary* for a reference of the certificate options, and error messages. Refer also to the following topics:

- *"SSL Configuration Details" on this page*
- *"Certificate Options Summary" on this page*
- *"Default Certificate" on page 163*
- *"Clearwell Commander-Generated Certificate" on page 164*
- *"Provider-Generated Certificate" on page 166*

Note: Starting with release 10.0, the keystores and truststores of BCFKS type are used. When using a keytool command to manage these stores, you need to add the storetype and providerclass arguments in addition to your other arguments.
Usually, the store type is passed using -storetype, but it may vary based on the keytool option being used.
The value for the store type should be *BCFKS*, and that for providerclass should be *com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider*.

For example, if the keytool command used in pre-10.0 release is *keytool -list -keystore tomcat\conf\server.keystore -storepass <password>*, it should be changed as below in release 10.0:

keytool -list -keystore tomcat\conf\server.keystore -storetype BCFKS -providerclass com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -storepass <password>

SSL Configuration Details

By default, the SSL configuration in the eDiscovery Platform is set to accept 128-bit or greater ciphers and requires the use of the TLSv1.2 protocol or better.

SSLv1, SSLv1.1, SSLv2, v3.0 are all disabled. The set of supported ciphers and protocols can be modified if needed.

Consult your IT department's security specialists to determine secure settings for your browser.

See also *"Secure LDAP SSL/TLS Support" on page 57*. For details on how to work with SSL backward compatibility, see Tech Note 226376: *https://www.veritas.com/support/en_US/article.TECH226376*.

Legal Hold Module and Browser Variations

For installations with the Legal Hold Module where users will be using Chrome or Firefox to access the Legal Hold Confirmation page, a DSA system certificate will not work. Those browsers are only compatible with an RSA 2048-bit keysize. If you need to request a provider certificate or generate your own, 2048-bit RSA encryption is required.

Certificate Options Summary

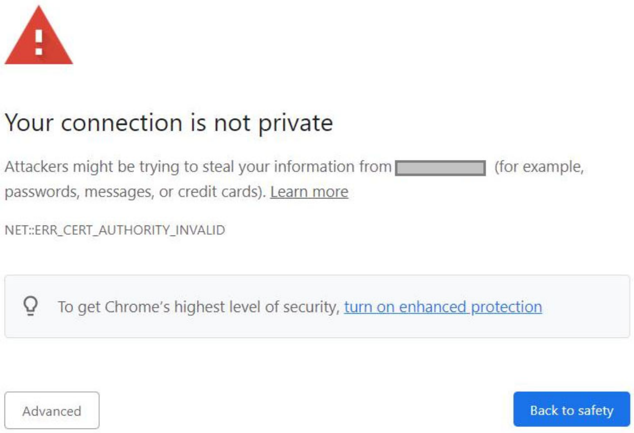
Certificate Options

Certificate Option	Error Message? (Yes/No)
Clearwell Default Certificate	Yes, even if user installs certificate
Clearwell Utility/Clearwell Commander Generated Certificate	Yes, until certificate is installed
Provider generated certificate	No

Default Certificate

Veritas ships the appliance with a default signed (self-signed) certificate that does not have a valid trust chain.

As a result, users attempting access the eDiscovery Platform’s interface over HTTPS will receive the “Your connection is not private” warning every time they access the login screen. Users can still proceed to access the interface by clicking **Proceed to**.

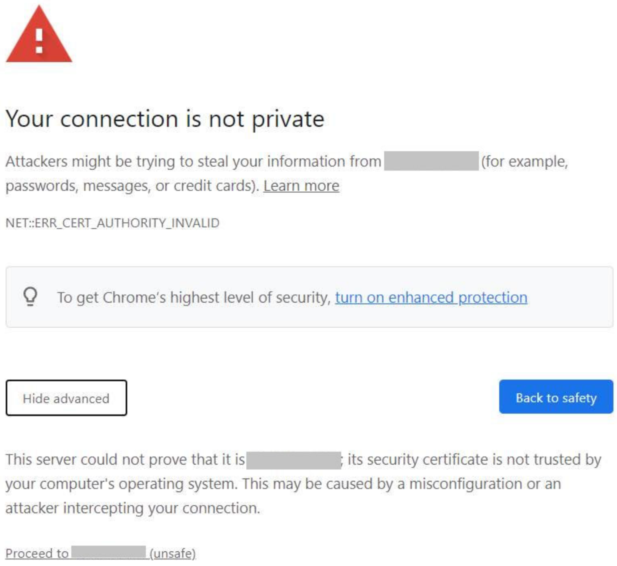


Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome’s highest level of security, turn on enhanced protection



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome’s highest level of security, turn on enhanced protection

This server could not prove that it is [redacted]; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to [redacted] (unsafe)

Going through the steps to install this certificate will not suppress certificate error warnings.

Clearwell Commander-Generated Certificate

Veritas provides a feature through Clearwell Commander to generate and install a self-signed certificate with the DNS name of the appliance. Note that the certificate generated through this feature will ***not*** be known by your browser's trust chains.

If using a Commander-generated certificate users will receive the messages: **Your connection is not private** warning when they access the login screen.

Generating the self-signed certificate using Clearwell Commander

1. From Clearwell Commander (found on the appliance's Windows Desktop), use the **Action** pulldown to select **Stop Appliance Services**. Wait for the application shutdown box to display **Finished**.
2. Use the **Action** pulldown to select **Generate Self-signed Certificate**.
3. The appliance’s DNS name will appear in the **Server Name** field.
4. Choose the number of years from the duration pulldown.
5. Click OK button to generate and propagate the certificate to the locations where it needs to be.
6. Once the sequence is complete, restart the eDiscovery Platform services.

   Note: For a self-signed certificate generated using the appliance's Clearwell Commander, you must set the following property to secure source account credentials, ensure success of AD discovery, and to complete collections from Office 365 and Domino sources:

   esa.common.security.custom.cert.thumbprint
   The value for this property is the thumbprint of the certificate.

   For details, refer to the *Securing source account credentials* section in the *Identification and Collection Guide.*

Cluster Considerations

Since the platform’s web interface for all appliances in a cluster is exposed to end users, a certificate is needed for each appliance in the cluster.

Provider-Generated Certificate

Overview

Deployments that require more stringent security than that afforded by the self-signed certificate options included with the eDiscovery Platform, such as implementing the TLS 1.2 protocol, should obtain and install a certificate from a certificate authority provider. Provider-signed certificates have the added benefit of eliminating client browser warnings.

Securing eDiscovery Platform with Provider-Signed Certificates

For new certificates or to change certificate providers, follow the instructions below to create a new Java keystore, generate a Certificate Signing Request, install the provider-signed certificate into the new Java keystore, and direct the platform to leverage this certificate.

To renew an existing provider-signed certificate, see *"Renewing an Expired Provider-Generated SSL Certificate" on page 170.*

To install a PFX Wildcard SSL Certificate in the Veritas eDiscovery Platform, please see knowledge management article 000017509 at *https://www.veritas.com/support*.

Since the eDiscovery Platform web interfaces for all appliances in a cluster are exposed to endusers, a certificate is needed for each appliance in the cluster. When it is necessary to update certificates, it must be done for all appliances in the cluster.

Creating a New Java Keystore

The actions below require a remote connection to the eDiscovery Platform server via Remote Desktop or VM Console.

1. Create a folder on the eDiscovery Platform appliance to contain the new Java keystore and related files, hereinafter referred to as the SSL Folder.

2. Open an administrative command prompt in the SSL Folder.

3. Create a new Java keystore using the basic keytool command below.

   ```
   keytool -genkeypair -alias clearwellkey -keyalg RSA -keystore new-server.keystore
   ```

4. Answer each question when prompted.

   `Enter keystore password:123456` (This password is required)
   `What is your first and last name? [Unknown]:`your_appliance_FQDN, DNS **`alias or IP address`**: (IP address is not recommended as it is subject to change.)
   `What is the name of your organizational unit? [Unknown]:` your_org_unit
   `What is the name of your organization? [Unknown]:` your_org
   `What is the name of your City or Locality? [Unknown]:` your_city
   `What is the name of your State or Province? [Unknown]:` your_state
   `What is the two-letter country code for this unit? [Unknown]:` your_country_code
   `Is CN=your_appliance_name, OU=your_org_unit, O=your_org, L=your_city, ST=your_state, C=your_country_code correct? [no]:` (If this is correct, enter: y or yes)
   `Enter key password for <clearwellkey>`
   `(RETURN if same as keystore password):` (Return required)

5. This will create a Java keystore named new-server.keystore in the SSL Folder.

   Note:

   › Use caution if using copy/paste with these examples as some PDF clients do not copy/paste the "-" character properly into a command prompt.

   › The `-alias` must be `clearwellkey` to be compatible with the eDiscovery Platform.

   › The keystore password must be `123456` to be compatible with the eDiscovery Platform.

   › Use the `-keysize` option to specify the certificate encryption strength. The RSA algorithm supports keysizes up to 4096 and the DSA algorithm supports keysizes up to 2048.

Creating a Certificate Signing Request

1. Open an administrative command prompt in the SSL Folder.

2. Create a Certificate Signing Request (CSR) using the basic keytool command:

```
keytool -certreq -keyalg RSA -alias clearwellkey -file my.csr
-keystore new-server.keystore
```

3. Transmit this CSR to your certificate authority provider for creation of your certificate.

   Note:

   › Use the `-keysize` option to specify the certificate encryption strength. The RSA algorithm supports keysizes up to 4096 and the DSA algorithm supports keysizes up to 2048.

   › You must acquire or convert your certificate in a form that can be imported in to Java via keytool.exe. Java's SSL keytool can import X.509 v1, v2, and v3 certificates, and PKCS#7 formatted certificate chains consisting of certificates of that type. The data to be imported must be provided either in binary encoding format, or in printable encoding format (also known as Base64 encoding) as defined by the Internet RFC 1421 standard. In the latter case, the encoding must be bounded at the beginning by a string that starts with "-----BEGIN", and bounded at the end by a string that starts with "-----END".

   › The web server that the product ships with is Tomcat. This is important to know, since most certificates are generated based on the type of web server being secured. If Tomcat is not an option with your provider, use Apache instead. If you generate a certificate based on a different web server type (like Microsoft IIS), the certificate will not work with the eDiscovery Platform.

Installing a New Certificate

Below are the basic steps to install your provider-signed certificates into the previously create Java keystore, new-server.keystore. These steps will depend to some extent on your certificate provider. You should receive and follow the instructions from your certificate provider for installing the certificate into Tomcat. Examples for major certificate providers are outlined later in this section.

1. Copy the provider-signed certificate(s) into the SSL Folder.

2. Make a backup copy of the new-server.keystore file before proceeding.

3. Open an administrative command prompt in the SSL Folder.

4. Import the certificates into the new-server.keystore using the following commands, in order, to ensure a proper certificate chain. The root certificate must be imported first, followed by any intermediate certificates ending with the import of the server public-key certificate. The keystore password `123456` is required to complete these commands.

```
keytool -import -trustcacerts -alias root -file root.cer -keystore new-server.keystore
keytool -import -trustcacerts -alias intermediate -file intermediate.cer -keystore new-server.keystore
keytool -import -trustcacerts -alias clearwellkey -file server.cer -keystore new-server.keystore
```

   Note:

   - The `-alias` options for root and intermediate certificates can be modified to better identify the certificate(s) involved. The `-alias` for the server certificate must be `clearwellkey` to match the existing private key entry already in the new-server.keystore.
   - The -file option names must be changed to match their respective certificate names.

5. Use the following command to verify the imported certificate information in the new-server.keystore:

```
Keytool -list -keystore new-server.keystore
```

   Note:

   - For more detailed output, use the verbose option `-v` after the `-list` command.
   - To dump the output to a text file, add `> keystore_output.txt` at the end of the command.
   - The root and intermediate certificates should have the EntryType of trustedCertEntry.
   - The server certificate must have an EntryType of PrivateKeyEntry.

6. Run the following keytool command to convert the keystore to BCFKS type.

```
keytool -importkeystore -srckeystore new-server.keystore -srcstoretype JKS -srcstorepass 123456 -destkeystore new-server.keystore -deststorepass 123456 -deststoretype BCFKS -providerclass com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
```

   Note: The value for the `deststorepass` and `destkeystore` are the same as `srcstorepass` and `srckeystore`. You may get a warning similar to the one below. This may be safely ignored in the current context.

```
Migrated "new-server.keystore" to Non JKS/JCEKS. The JKS keystore is backed up as "new-server.keystore.old".
```

Major Certificate Authority Provider Installation Examples

Comodo Example

The following is an example of how to import certificates from Comodo:

```
keytool -import -trustcacerts -alias root -file
AddTrustExternalCARoot.crt -keystore new-server.keystore
keytool -import -trustcacerts -alias INTER -file
ComodoUTNServerCA.crt -keystore new-server.keystore
keytool -import -trustcacerts -alias clearwellkey -file
EssentialSSLCA.crt -keystore new-server.keystore
```

Symantec (Verisign) Example

The following is an example of how to import certificates from Symantec (VeriSign):

```
keytool -import -trustcacerts -alias primaryIntermediate -file
primary_inter.cer -keystore new-server.keystore
keytool -import -trustcacerts -alias secondaryIntermediate -file
secondary_inter.cer -keystore new-server.keystore
keytool -import -trustcacerts -alias clearwellkey -file
<SSL-cert- name>.cer -keystore new-server.keystore
```

GoDaddy Example

The following is an example of how to import certificates from GoDaddy:

```
keytool -import -trustcacerts -alias root -file
valicert_class2_root.crt -keystore new-server.keystore
keytool -import -trustcacerts -alias cross -file
gd_cross_intermediate.crt -keystore new-server.keystore
keytool -import -trustcacerts -alias intermed -file
gd_intermediate.crt -keystore new-server.keystore
keytool -import -trustcacerts -alias clearwellkey -file
<SSL-cert-name>.crt -keystore new-server.keystore
```

Deploying the New Java Keystore

1. In Windows Explorer, navigate to the Tomcat template directory, D:\CW\v<90>\config\templates\tomcat and rename the existing server.keystore file to create a backup, e.g., server.keystore.YYYYMMDD.

2. Copy the new-server.keystore file from the SSL Folder to the Tomcat template directory and rename it to server.keystore.

3. The new keystore containing the provider-signed certificates is now ready for deployment. Deployment requires running an Incremental Configuration Rebuild, which requires stopping the appliance services and should be coordinated to occur when no users are active in the application and no jobs are running. This can be done in one of two ways:

   A. Using the **Clearwell Utility** on the eDiscovery Platform appliance desktop, run Option #7 “Build Incremental Configuration Changes”. This will stop services, deploy incremental changes and restart services.

B. Using **Clearwell Commander** on the eDiscovery Platform appliance desktop, you will need to run these three separate steps under **Actions**:

- **Stop Appliance Services**
- **Build Incremental Configuration Changes**
- **Start Appliance Services**.

Note: If you are deploying the new keystore on the Cluster Primary in a Distributed Architecture environment, you must first stop the services on all secondary nodes to ensure proper reconnection on restart of the Cluster Primary.

4. Use your browser to test the deployment of the new certificate by browsing to the fully-qualified domain name (FQDN) of the server or the DNS alias, whichever was used during the generation of the Certificate Signing Request (CSR).

5. Verify server name, expiry date, and provider information is correct by double-clicking on the lock in the address bar and click on the **View Certificate** link. This information will be under the **Details** tab of the certificate.

Renewing an Expired Provider-Generated SSL Certificate

For certificate renewal from the same certificate provider, follow the instruction below to install the updated provider-signed certificate into the existing Java keystore.

1. In Windows Explorer, navigate to the Tomcat template directory, D:\CW\v90\config\templates\tomcat and make a backup copy of the existing server.keystore file, e.g., server.keystore.YYYYMMDD.

2. Open an administrative command prompt in the D:\CW\v90\config\templates\tomcat folder.

3. Import the server certificate into the server.keystore using the following command:

```
keytool -import -trustcacerts -alias clearwellkey -file server.cer -
keystore server.keystore -storetype BCFKS -storepass 123456 -
providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
```

   Note:

   - If you have changed the server.keystore password, use the changed password instead of 123456 for storepass.

4. Deploy the renewed keystore using the steps described in *"Deploying the New Java Keystore" on page 169*.

Propagate the Valid Certificate for use by eDiscovery Processes

Introduced in version 8.2, communication channels for some internal processes are now secured using SSL encrypted communications. This includes Active Directory/Employee synchronization and collections from Office 365 Exchange and Domino sources. For these processes to function, the new, renewed, or Clearwell Commander generated certificate must be propagated to other system locations where it is required.

1. Log into the eDiscovery Platform appliance as a local administrator and launch Clearwell Commander from the desktop.
2. From the **Action** pulldown, select **Stop Appliance Services**. Wait for all services to stop.

   Note: If this is a Distributed Architecture environment, you must first stop the services on all secondary nodes to ensure proper reconnection on restart of the Cluster Primary.
3. Go to **Action** and select **Copy Tomcat Provider Certificate to Windows Trust Store**. The propagation of the certificate will proceed.
4. When copying is complete, select **Start Appliance Services**. Then quit Clearwell Commander from the **File** pulldown.
5. For all certificate types (with the exception of the default self-signed certificate), the certificate thumbprint must be updated to secure account credentials.
6. To locate a certificate's thumbprint, refer to the “Securing source account credentials” section in the *Identification and Collection Guide*.
7. Log into the eDiscovery Platform UI as a System Manager and navigate to **System > Support Features**.

   A. From the **Support Features** pulldown, **Select Property Browser**.

   B. (optional) If the appliance does not appear in the **Choose an Appliance** window, use the pulldown to select the eDiscovery Platform appliance associated with the thumbprint.

   C. For the **Select the case (or system)** pulldown, make sure **System** is chosen.

   D. In **Name of property to change**, enter:
   `esa.common.security.custom.cert.thumbprint`

   E. In **New value (leave blank to remove)**, enter the thumbprint value with no spaces between bytes.

For further details regarding SSL certificates, refer to Oracle's Java security documentation:
http://docs.oracle.com/javase/8/docs/technotes/guides/security/

And in particular, the chapter on Public Key Cryptography Standards (PKCS):
http://docs.oracle.com/javase/8/docs/technotes/guides/security/p11guide.html

Appendix B: Web Services APIs for Case Creation

This appendix provides the details and steps to write a web service client to invoke some features not otherwise accessible through the user interface. These specific APIs can be used to import information from other case management systems into the platform.

This document contains the APIs which correspond to their respective feature capabilities:

- Authenticate Credentials (required to obtain proper authentication for all APIs)
- Case Creation
- Case Update

Refer to the following topics in this section:

- *"Framework" on this page*
- *"Authentication" on this page*
- *"Exception" on this page*
- *"APIs: Retrieving Case Related Information" on page 175*
- *"Authenticate Credentials" on page 175*
  - *"Case Creation" on page 176*
  - *"Case Update" on page 177*
  - *"Validating User Input: ClearwellCaseImport.xsd" on page 178*
  - *"Validating Against Server Error Responses" on page 179*

Framework

The authentication API uses JSON as the format for data exchange. The case creation and case update APIs use XML as the format for data exchange.

Authentication

The client has to invoke the authentication API first. This will return a session cookie and a fraud-prevention token. These items need to be used for any subsequent (API) request - the token has to be part of the URI parameter. The session is initiated by this invocation and is maintained across all subsequent API invocations. The session time out is based on the application configurations.

Exception

Any exception is indicated by the appropriate HTTP response header. In addition to the header, the return response will contain the following:

1. URI – the URI of the requested resource
2. Description – A brief description of the error
3. Details – detail information of the error e.g. it may include the server stack trace

APIs: Retrieving Case Related Information

The following APIs are used for retrieving case related information.

Authenticate Credentials

This is the authentication API.

Description	Provide the user name and password to initiate the session and obtain a session ID and a fraud-prevention token. **All subsequent APIs must use these.** The token must be a part of the URI of any subsequent API invocation.
Operation	POST
URI	http://host:port/esa/services/auth

Request	Body:
	cwu=userid
	cwp=password

Response	Headers: Code: 200 OK Set-Cookie: sessionid=124ee456 Body: `"cwfpToken":6685499956365532308`

Case Creation

This API can be used to import case information from other case management systems to create a new case in the platform.

Description	Create a case and an associated legal hold. **Input:** XML document containing the full metadata for the case. This XML document must validate against the ClearwellCaseImport.xsd file shown later. **Output:** Code 200 if successful. Otherwise an appropriate HTTP error response with a corresponding XML document, which will validate against the ClearwellCaseImportError.xsd file below.
Operation	POST
URI	http://host:port/esa/services/case/create
Response	Code: 200 OK Error example:- Header Code 403: Body: `<?xml version="1.0" encoding="UTF-8" standalone="yes"?><error><errorDescription>[#60015] Unauthorized Access</errorDescription><requestResource>http://localhost/esa/services/case/create</requestResource></error>`

Case Update

This API can be used to update an eDiscovery Platform case with metadata from other case management systems.

Description	Update the metadata for an existing case. **Input:** XML document containing the full metadata for the case. This XML document must validate against the ClearwellCaseImport.xsd file shown later. Note: Missing fields will be treated as deletes to the fields. **Output:** Code 200 if successful. Otherwise an appropriate HTTP error response with a corresponding XML document, which will validate against the ClearwellCaseImportError.xsd file below.
Operation	POST
URI	http://host:port//esa/services/case/update
Response	Code: 200 OK Error example: Header Code 403: Body: `<?xml version="1.0" encoding="UTF-8" standalone="yes"?><error><errorDescription>[#60015] Unauthorized Access</errorDescription><requestResource>http://localhost/esa/services/case/create</requestResource></error>`

Validating User Input: ClearwellCaseImport.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:complexType name="customAttribute">
<xsd:sequence>
<!-- add type attribute for value, must be string for now -->
<xsd:element name="name" type="xsd:string" minOccurs="1" maxOccurs="1" />
<xsd:element name="value" type="xsd:string" minOccurs="1" maxOccurs="1" /
>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="teamMember">
<xsd:attribute name="name" type="xsd:string" use="required"></
xsd:attribute>
</xsd:complexType>
<xsd:element name="case">
<xsd:complexType>
<xsd:sequence>
<xsd:element name="name" type="xsd:string" minOccurs="1" maxOccurs="1" />
<xsd:element name="description" type="xsd:string" minOccurs="0"
maxOccurs="1" />
<xsd:element name="type" type="xsd:string" minOccurs="0" maxOccurs="1" />
<xsd:element name="status" type="xsd:string" minOccurs="0" maxOccurs="1"
/>
<xsd:element name="number" type="xsd:string" minOccurs="0" maxOccurs="1"
/>
<xsd:element name="businessUnit" type="xsd:string" minOccurs="0"
maxOccurs="1" />
<xsd:element name="court" type="xsd:string" minOccurs="0" maxOccurs="1" /
>
<xsd:element name="docketNumber" type="xsd:string" minOccurs="0"
maxOccurs="1" />
<xsd:element name="filed" type="xsd:date" minOccurs="0" maxOccurs="1" />
<xsd:element name="served" type="xsd:date" minOccurs="0" maxOccurs="1" />
<xsd:element name="courtDate" type="xsd:date" minOccurs="0" maxOccurs="1"
/>
<xsd:element name="closeDate" type="xsd:date" minOccurs="0" maxOccurs="1"
/>
<xsd:element name="in-houseCounsel" type="teamMember" minOccurs="0"
maxOccurs="1" />
<xsd:element name="outsideCounsel" type="teamMember" minOccurs="0"
maxOccurs="1" />
<xsd:element name="leadAttorney" type="teamMember" minOccurs="0"
maxOccurs="1" />
<xsd:element name="leadParalegal" type="teamMember" minOccurs="0"
maxOccurs="1" />
<xsd:element name="teamMember" type="teamMember" minOccurs="0"
maxOccurs="unbounded" />
<xsd:element name="notes" type="xsd:string" minOccurs="0" maxOccurs="1" /
>
```

```
<xsd:element name="caseCaption" type="xsd:string" minOccurs="0"
maxOccurs="1" />
<!-- Custom fields will need custom type -->
<xsd:element name="otherAttribute" type="customAttribute" minOccurs="0"
maxOccurs="unbounded"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:schema>
```

Validating Against Server Error Responses

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="error">
<xsd:complexType>
<xsd:sequence>
<xsd:element name="errorDescription" type="xsd:string" minOccurs="1"
maxOccurs="1" />
<xsd:element name="requestResource" type="xsd:string" minOccurs="1"
maxOccurs="1" />
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:schema>
```

Appendix C: Product Documentation

This table lists the administrator and 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 the software application
Utility Node Guide	For customers using utility nodes, describes how to install and configure appliances as utility nodes for use with an existing software 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, 8.x compared to 7.x and 7.x compared to 6.x
Administrator's QuickStart Guide	Describes basic appliance and case configuration
Reviewer's QuickStart Guide	A reviewer's reference to using the Analysis & Review module
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 appliance for Legal Holds, and use the Legal Hold module as an administrator
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
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 10.0, workflows affected when the cases are upgraded or not upgraded, and frequently asked questions (FAQs).

Veritas eDiscovery Platform Documentation

Document	**Comments**
User Guide	Describes how to perform searches, analysis, and review, including detailed information and syntax examples for performing advanced searches
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
Audio Search Guide	Describes how to use the Audio Search feature to process, analyze, search and export search media content
Reference and Support	
Audio Processing	A quick reference card for processing multimedia sources
Audio Search	A quick reference card for performing multimedia search tasks
Legal Hold	A quick reference card of how to create and manage holds and notifications
Collection	A quick reference card of how to collect data
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
Online Help	
Includes all the above documentation (excluding Installation and Configuration) to enable search across all topics. To access this information from within the user interface, click **Help**.	
Release	
Release Notes	Provides latest updated information specific to the current product release