Veritas eDiscovery Platform™

Legal Hold User Guide

10.1

Veritas eDiscovery Platform™: Legal Hold User 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: 2021-11-20.

Legal Notice

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

Contents

Legal Hold User Guide

Welcome to the *Veritas eDiscovery Platform Legal Hold User Guide*. This feature guide provides a source of reference for legal administrators and end users of the Veritas eDiscovery Platform Legal Hold module with the tools and information for notifying system administrators and custodians of holds, and tracking legal hold responses.

Note: Refer to the Appendix for the necessary steps to set up and configure the appliance for use with the Legal Hold module.

The Legal Hold module provides administrators with the ability to ensure critical information is held in response to a legal request. With Legal Hold, administrators control the legal hold notification process, from creation of the legal hold, through confirmation and release.

This section contains the following sections:

About This Guide

CAUTION: *System administrators must ensure that appliances are properly configured with at least one server used as a Legal Hold Confirmation server. See* *"Appendix A: Setup Requirements" on page 97* *prior to using the Legal Hold module in Veritas eDiscovery Platform.*

This guide provides an overview of the Legal Hold module, a separately licensed add-on feature to Veritas eDiscovery Platform. The sections in this guide provide an overview of Veritas eDiscovery Platform's legal hold process and how to perform administrative legal hold and notification related tasks.

This guide is intended for legal hold administrators tasked with sending notifications in response to a legal hold. However, system and IT administrators, as well as your organization's decision makers may also be interested in understanding how Veritas eDiscovery Platform manages legal hold notifications using the Legal Hold module.

Related Documents

For a quick reference of Legal Hold tasks, refer to the *Legal Hold Quick Reference Card*.

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
December 2021	• Updated version for release 10.1
March 2021	• Added information about SAML 2.0-based authentication • Minor edits
October 2018	• Minor edits
March 2018	• Added information related to Header-based Authentication. See *"Single Sign-On for Legal Hold using IWA or Header-based authentication" on page 19*. • Added information related to IPv6 support
December 2017	• Added information on Integrated Windows Authentication Single Sign-On • Added information on clearing Confirmation Server • Minor edits
June 2017	• Added information on resending last notice • Added information on the Legal Hold Report by Custodian report • Minor edits
June 2016	• Added information on Legal Hold Authentication • Updated the Setup Checklist • Updated information on Legal Hold Admin user role • Updated information on viewing and responding to Legal Hold Notices • Branding and minor edits
August 2015	• Minor updates throughout • Removed Rights Management Guide from the Product Documentation section • Removed Prompt for reason code field from the Document Access Rights section
March 2015	• Branding and minor edits
October 2014	• Added information on the formatting toolbar • Added information on characters limitations for a survey question • Added information on Access Groups Permissions • Added information on editing the sender's name and email address in the Legal Hold notices
December 2013	• Updated the Product Documentation section

Revision Date	New Information
June 2013	• Added information on Cc recipients in the Creating a Legal Hold Notice section • Added a note about editing notices in the Sending/Scheduling Notices section • Updated information on Legal Hold Defensibility report and Employee Report • Updated the Apply Templates to a Notice • Added information on using an external IP address for the confirmation link • Added information on setting up SMTP server for Legal Hold • Updated information on synchronizing Active Directory with Employee List • Minor updates throughout
September 2012	• Incorporated Legal Hold setup requirements into guide, as the Appendix (formerly "Legal Hold Setup Guide") • Documented new features: – New Legal Hold Admin role: Separated from Collections Admin – Enhanced administrative functionality on Legal Holds (and notices), including enabling repeating status reminders and setting recurrence
May 2012	• Behavior of legal hold restore from backup: Restore not honored if holds were released prior to restore
March 2012	• New features: Legal Hold activity reports and report export, and ability to archive/restore legal holds
February 2012	• Obtaining a license update; formatting changes throughout
November 2011	• New feature: "Add Attachment" to hold notices • Updated procedures and graphics for new navigation
May 2011	• Minor updates throughout
February 2011	• All - New guide created to document new Legal Hold feature

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 Veritas 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/

Getting Started

To help you get started, use this section to guide you through verifying your setup, and what to do after logging on to the Veritas eDiscovery Platform.

In this section:

About Legal Hold

The Legal Hold module allows administrators to select potential custodians and system administrators to send customized notifications for legal hold, and track their responses.

The Legal Hold module allows you to:

- integrate with your organization's Active Directory to identify and select from a populated list of existing custodians and system administrators. See *"Discovering Custodian Data" on page 13*.
- create and customize (by administrators) legal holds and create/add notifications according to recipient types. See *"Creating Legal Holds and Notices" on page 17*.
- customize and send notifications to system administrators and custodians depending on role and responsibility, and creating/applying hold notice templates. See *"Customizing and Sending Notices" on page 39*.
- track hold notice status, view report notification recipient activity, including viewing survey results, statistics and responses, and generate and/or export and download legal hold and defensibility data. See *"Tracking and Reporting" on page 59*.
- archive/restore old or previously inactive legal holds, update your custodian count, and perform other administrative tasks. See *"Administration and Maintenance" on page 69*.

Legal Holds Module User Interface

There are two views of the Legal Holds module: All Legal Holds, or the legal hold associated with a particular case.

To view legal holds across all cases on the appliance, click **All Cases** on the top navigation bar, and then click **All Legal Holds**:

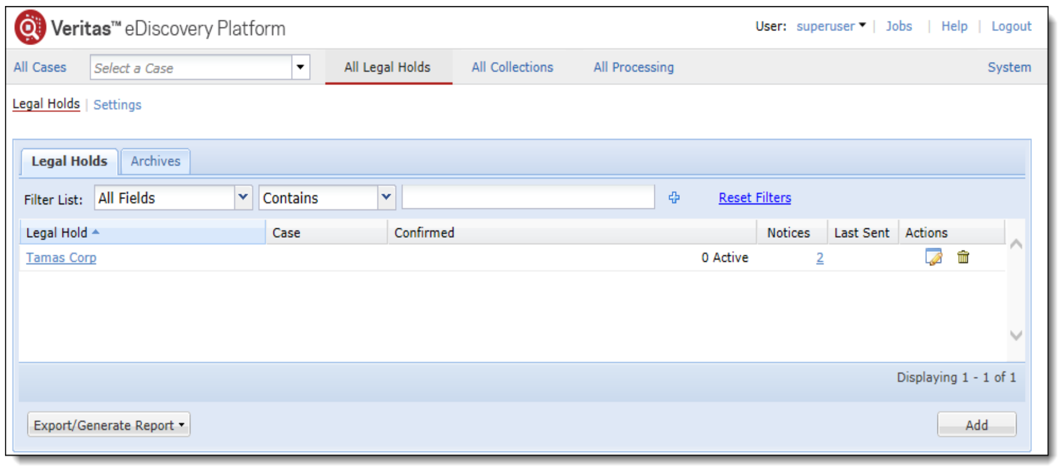


Figure: Legal Holds Module: All Legal Holds View

From the All Legal Holds view, an administrator can manage all Hold activities in one dashboard view across all cases on the appliance.

To view holds and notices in a specific case, click the drop-down to select the case (or select **Create a new case**), and then click **Legal Holds**.

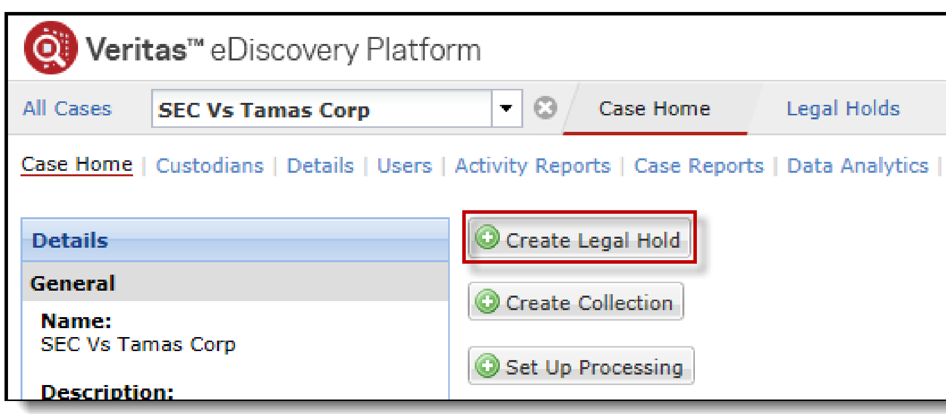


Figure: Legal Holds Module: Within a Selected Case

When a legal hold is selected, the administrator can view all legal holds specific to the selected case. Click **Create Legal Hold** to start a new hold and add notices. See *"Creating Legal Holds and Notices" on page 17*.

Checklist: Before You Begin...

Verify your setup and check that your appliance and the Confirmation Server is properly installed and configured before you begin working with the Legal Hold module:

- Appliance is properly installed.
  Refer to the "*Veritas eDiscovery Platform Installation Guide*" to verify your basic installation.
- Confirmation server is installed and configured for the setup.
  See *"Appendix A: Setup Requirements" on page 97* to install and set up the Legal Hold server, or "Confirmation Server" for use with Legal Holds.
- Legal Holds License is installed.
  See *"Managing Your Legal Holds License" on page 91* to check for license information.
- Change/update account, Help, and Support link information.
  See *"Logging On" in the next section*.

Logging On

The first time you log on, be sure to:

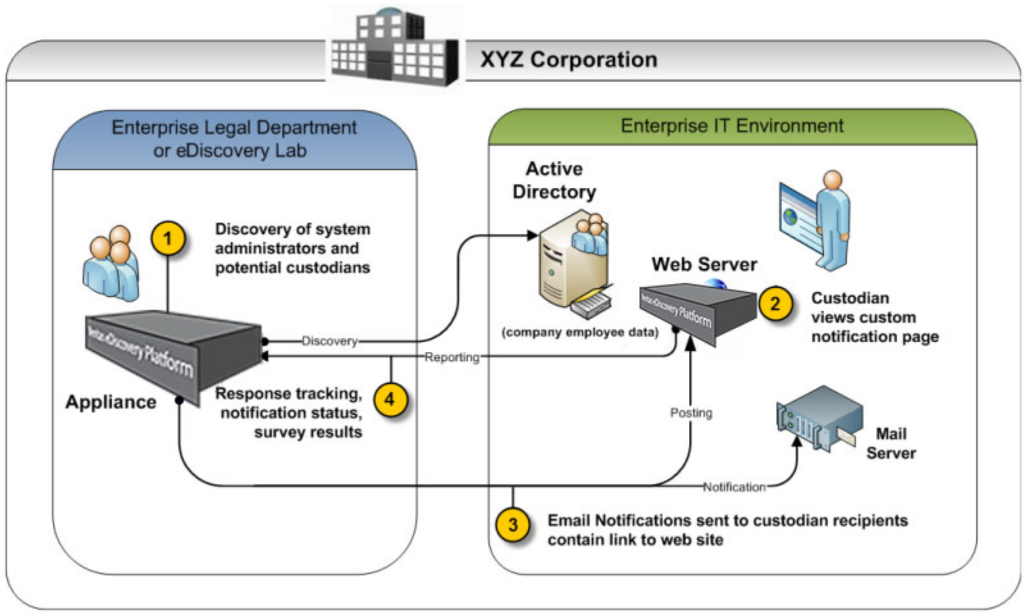
1. Change the account password.

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

2. Update the Need Help? link on the Login page.
3. Update the Support link.

Veritas eDiscovery Platform Legal Holds Workflow

The following diagram illustrates the basic steps in the Legal Holds process, which correspond to the sections in this guide to help you prepare your notifications for applying legal holds.



After initial setup and configuration (see *"Appendix A: Setup Requirements" on page 97*), continue with the next steps in the Legal Hold process:

1. **Populating the Employee List**. Populate the Employee List with a list of potential custodians and their contact information. See *"Discovering Custodian Data" on page 13*.

2. **Legal Holds & Notices**. Create, customize and send notifications to selected custodians and system administrators. See *"Creating Legal Holds and Notices" on page 17* and *"Customizing and Sending Notices" on page 39*.

3. **Custodian View/Response.** Recipients view customized web page displaying holds (Active/Pending, and Released) and respond accordingly. See *"Receiving Notification" on page 51*.

4. **Reporting**. Track responses and monitor status of all notices; view survey results. See *"Tracking and Reporting" on page 59*.

Occasionally, you may also want to set Legal Hold user permissions, check Legal Holds licensing information, and perform other legal hold administrative tasks. See *"Administration and Maintenance" on page 69*.

Discovering Custodian Data

This section describes Active Directory discovery, the first step in the Legal Holds process, to populate Veritas eDiscovery Platform's Custodian table in preparation for Legal Holds.

- *"About Populating the Employee List" in the next section*
  - *"Add (or Import) Custodians to Your Employee List" on page 14*

About Populating the Employee List

The Veritas eDiscovery Platform Legal Hold module can automatically populate its Custodian table (list of potential custodians and system administrators) by importing data directly from Active Directory (or other archive source). The Employee List contains potential custodians or recipients of custodian and system administrator hold notices.

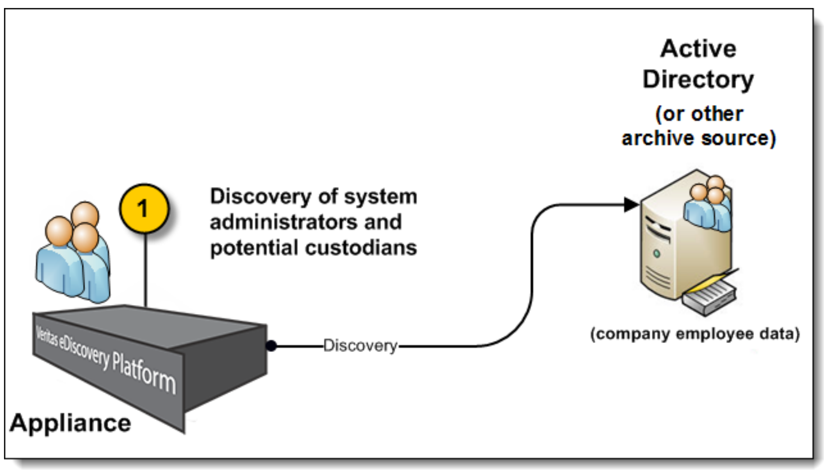


Figure: Legal Hold Process—Step 1: Discovering Custodian Data

Your system administrator may have already performed data discovery, such as Active Discovery or Lotus Domino (for Lotus Notes sources) on the email servers for your collections environment. For more details about performing discovery, refer to the *Identification and Collection Guide*. To perform an initial Active Directory discovery on your employee source data (before custodian import), see *"Populating the Employee List" on page 74*.

As employee data changes, you may want to perform automatic updates on Active Directory to be sure you are accessing the latest updated custodian information. For information on setting up periodic Active Directory Discovery tasks, see *"Schedule Discovery" on page 87*.

To ensure that custodian information is periodically saved and preserved, you can schedule system backups to recur. See *"Performing Backups" on page 82*.

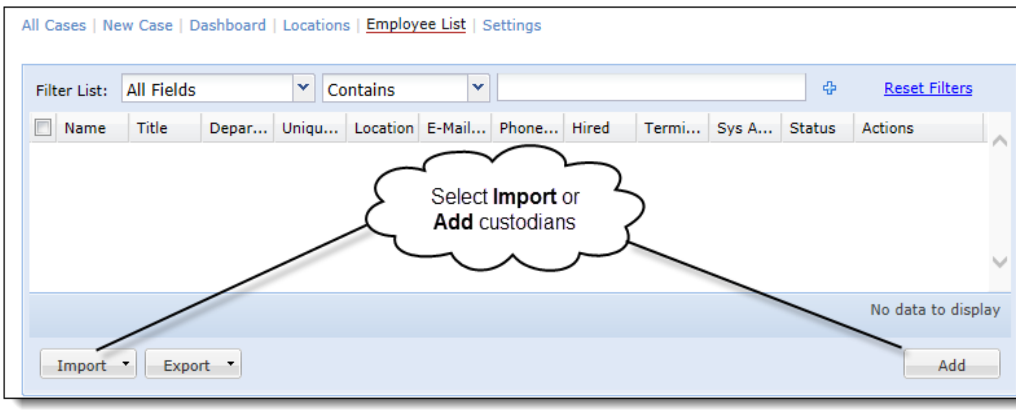
Add (or Import) Custodians to Your Employee List

After performing Active Directory discovery, you can import all employees at once, or add employees individually. Follow the set of steps that best suits your needs.

Note: Later, after your selected custodians have been added to a case, you can use the “Custodian Merge” feature to resolve any same-name, or similarly-named custodians (that represent the same source or individual). For more information, refer to *"Merging Custodians" in the Case Administration Guide*.

To add custodians

1. From the **All Cases** view, click **Employee List**.



2. From the Employee List, determine if you want to:

   A. Import all custodians at once.

   B. Add custodians individually.

To add custodians by import (option A)

1. From the **Custodians** window, click **Import** and select one of the following options:

   A. Active Directory:

   - **Synchronize Now with Active Directory** (synchronize the entire Active Directory with the Employee List)

   B. From File:

   - **From CSV** (enter CSV file name and path, or browse to location)
   - **From Script** (enter Script file name and path or browse to location)

   If you are importing custodians from a file, a job runs to add all their names to your Employee List. To view the status of your CSV or Script file import, click the **Jobs** link at the top of the screen. If an error occurs during import, a warning icon appears next to the link. Click the book icon in the Status column to view details in the job status log.

2. If your import was successful, all the people records that you imported appear in the list of custodians.

To add a custodian individually (option B)

1. From the All Cases view, click **Employee List**.
2. Click **Add**.

   Note: Several options are visible only if your enterprise has a Legal Holds module license installed and you have the appropriate permissions.

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

Adding a Custodian

Field	Description
Name*	Enter the name of the custodian (up to 35 characters). The name is not case sensitive.
Title	Enter the custodian's title (if applicable).
Department	Enter the custodian's division or department (if applicable).
Unique ID	Enter an identification number or code unique to this custodian.
Location	Enter a location.
E-Mail: Address	Enter the custodian's email account. (Example: jsmith@acmemail.com). By default, the icon is selected to indicate that this is the primary address. Click the icon to add additional addresses for this custodian.
Phone Number	Enter a phone number for the custodian. Click the icon to add additional phone numbers for this custodian.
Escalation Manager (Legal Hold users only)	Enter or browse for the name of this custodian's manager to whom legal hold notifications should be escalated.
Hired / Terminated	Enter the date of hire and termination, or click the calendar icon to select a date.
Owner Info. (Domain, Owner Name, SID)	Enter the Domain name, owner name, and the Security Identifier. **Note:** The owner name will only be collected (when filtering for collection) if the Windows user for the collection is running as the source account (or *EsaApplicationService* user if there is no account on the source), and it is in the domain where the owner name is kept.
System Admin for Legal Hold (Legal Hold users only)	Select this check box if this custodian's role is a System Administrator, for use in customizing Legal Hold notifications. The System Administrator custodian will appear by default for any System Admin Notices which are created.

4. Click **Save** to associate the new custodian to the selected source, or click **Cancel** to discard your changes.

Creating Legal Holds and Notices

This section describes how to create legal holds and notices in preparation for sending to potential custodians using Veritas eDiscovery Platform's Legal Hold module.

- *"About Legal Holds and Notices" in the next section*
  - *"Who are "Custodians" and "System Administrators"?" on page 18*
  - *"Create a Legal Hold" on page 25*
  - *"Creating a Legal Hold Notice" on page 28*

About Legal Holds and Notices

Through the Legal Hold module on the Veritas eDiscovery Platform, administrators can create *Legal Holds*—a container for tracking all required legal hold notices related to a particular matter. The court typically orders legal hold notices when a legal matter arises, in an effort to preserve critical data.

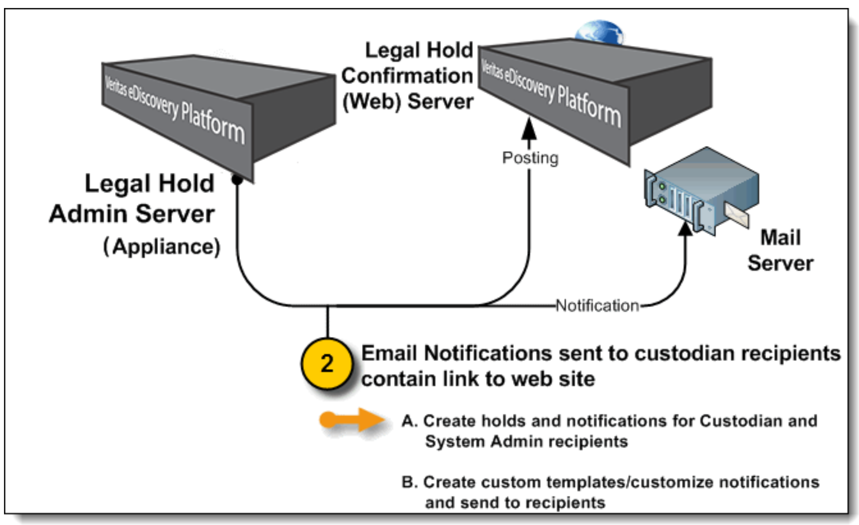
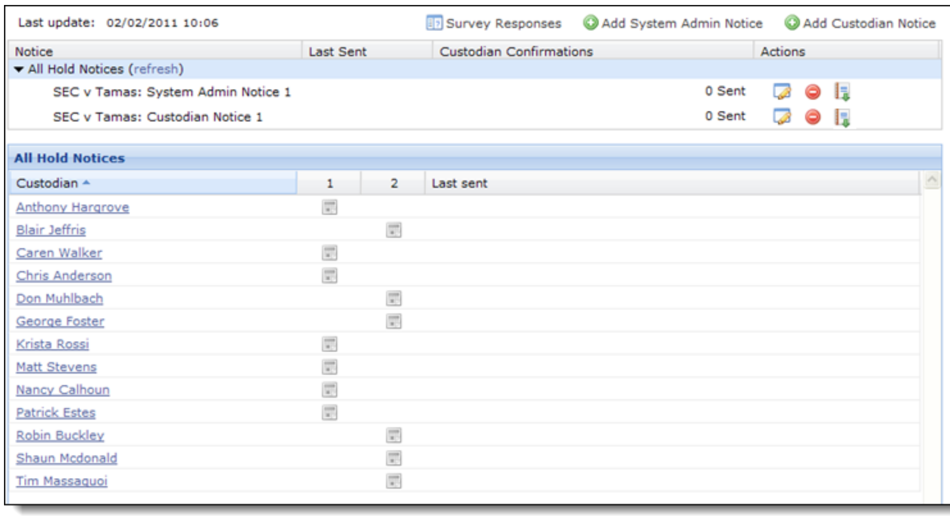


Figure: Legal Hold Process—Step 2 (A): Creating Legal Holds and Notices

Who are “Custodians” and “System Administrators”?

Custodians receiving legal hold notifications are those identified as holders of information related to, or having some involvement in a legal matter. Similarly, system administrators are also “custodians of data”, and often receive notification requests to put systems or archived custodian data on Legal Hold. In the Legal Hold module, you can differentiate each custodian by their role. From the Custodian table, you can specify (by selecting from the list) which custodians are system administrators, then customize your hold notices accordingly.



Later, refer back to the Custodian table to display a summary of legal hold information for each custodian, including details about the holds and escalation managers associated with a particular custodian. (See *“Sending Reminders or Escalations” on page 46*.)

Customize Notices Using Templates

If you plan to send multiple notices to both custodians and system administrators, you can create a template when adding a new System Admin Notice and Custodian Notice to a Legal Hold. For information about how to create templates, see *“Creating/Saving Notices as Templates” on page 41*.

Legal Hold Authentication

Release 8.2 and later offers an authentication mechanism where system administrators can limit access of the legal hold confirmation page only to the intended custodians. The system administrators can choose to enable legal hold authentication so that only the intended recipients of the notice with valid LDAP accounts would be able to view and respond to the legal hold notice.

The system administrator must ensure that the required custodians exist in Active Directory before enabling LDAP authentication for legal holds. When custodians are imported or added manually, the Active Directory sync must be performed to be able to use LDAP authentication. Refer to the *Identification and Collection Guide* for details on adding or importing custodians.

To maintain proper load balancing and a secure legal hold environment, it is recommended to install the Confirmation server on a separate server other than your main administrative appliance. In this case, the system administrator should make sure that the Confirmation Server is up and running.

When legal hold authentication is enabled, only the intended custodians with valid LDAP account can respond to the notice as the system displays the legal hold confirmation page only after successful authentication and authorization. The system shows a warning message for unintended custodians that they are not the intended recipient of the legal hold notice link that they clicked, and they can view only those legal hold notices that they are authorized to view.

When a custodian having both types of notices, i.e. notices that require authentication and the notices that do not require authentication, opens the link for a notice that does not require authentication, then custodian cannot see the notices which require authentication. The system asks such custodians to log in using their enterprise user name and password to view and respond to the legal hold notices that require authentication.

For the notices that were sent before enabling the LDAP authentication, the system does not ask for LDAP authentication to respond to such notices. If you have created legal holds with LDAP authentication enabled and then at later stage you disable LDAP authentication, then the system does not ask for LDAP authentication for any pending legal holds. It is not a recommended practice to disable LDAP authentication once it is enabled.

Note: It is recommended to validate the LDAP properties after a node backup is restored. If the Legal Hold Authentication properties are overwritten, you should manually set the properties from the **System** > **Settings** > **Legal Hold Authentication** tab.

Legal Hold supports the following methods for SSO:

- *"Single Sign-On for Legal Hold using IWA or Header-based authentication" in the next section*
- *"Single Sign-On for Legal Hold using SAML" on page 24*

Single Sign-On for Legal Hold using IWA or Header-based authentication

Veritas eDiscovery Platform supports integrated Windows authentication (IWA) and header-based authentication to configure Single Sign-On (SSO) for Legal Hold authentication. You can use any of these authentication methods. By default, IWA is used.

To use the SSO option, LDAP must be configured and enabled against the Active Directory domain from which Windows users will be authenticating. The custodians must be present in the Active Directory.

Note: Once the SSO login is enabled, custodians do not get an option to log in by providing their credentials explicitly.

Integrated Windows Authentication

When integrated Windows authentication is enabled, the logged-in Windows credentials of the custodian are used for authentication, and the custodian is subsequently directed to the Legal Hold Confirmation page without the need to enter login credentials.

For IWA, Kerberos authentication is preferred over NTLM authentication and is selected by default. Users also have an option to use Kerberos first and then if it fails, use NTLM for authentication.

NTLM and Kerberos are Integrated Windows Authentication protocols. Microsoft implements Kerberos as the default authentication protocol for the Windows OS. Kerberos is considered a better authentication option than NTLM as it provides advantages over NTLM such as faster and mutual authentication, delegation support, improved performance, and interoperability.

Header-based authentication

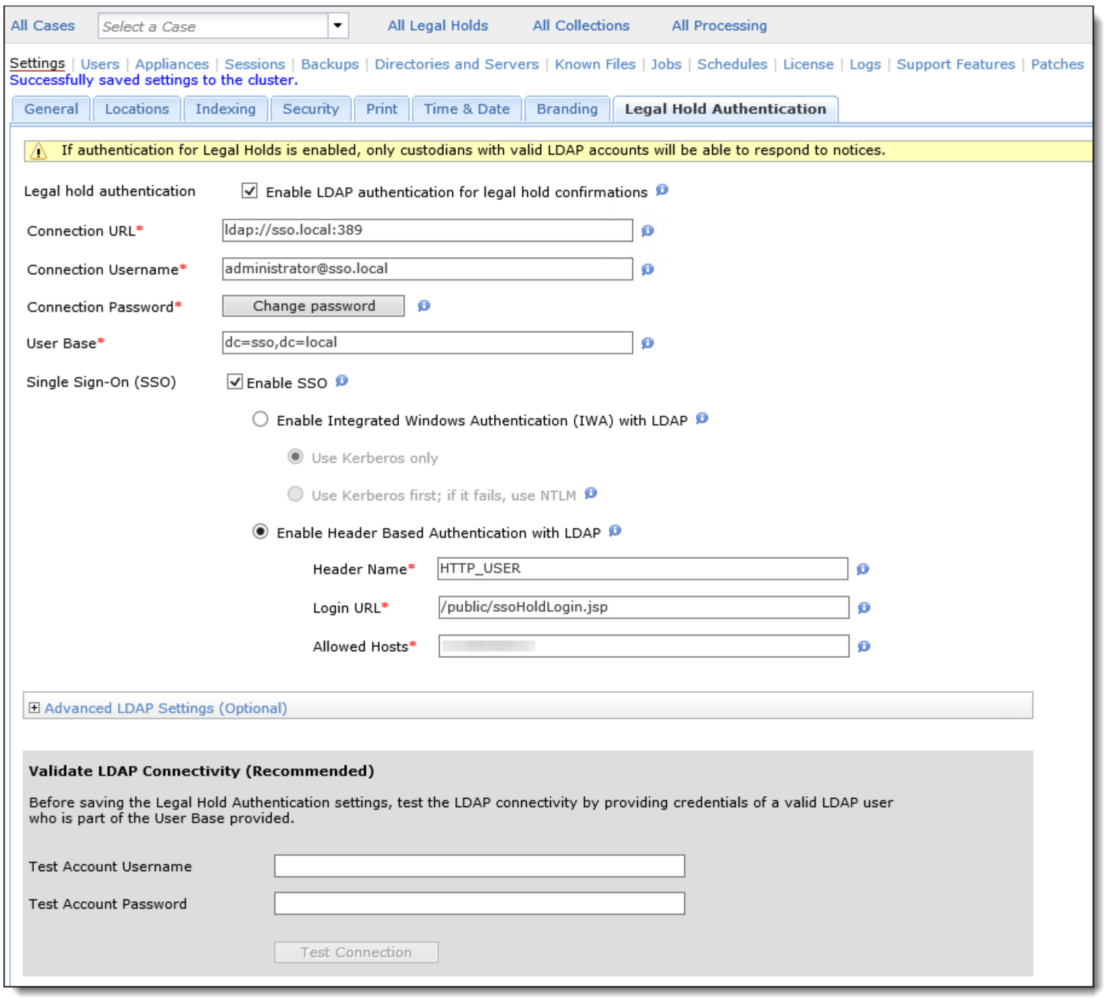
Starting with 9.0.1, Veritas eDiscovery Platform also supports header-based authentication Single Sign-On (SSO) for Legal Hold authentication. If header-based authentication is enabled, the custom HTTP header with the username provided by the configured Identity Service Provider (ISP) is used for login through a reverse proxy. The custodian is directed to the Legal Hold notice without the need to enter login credentials.

To enable LDAP authentication for legal hold notices:

The LDAP authentication for legal hold is disabled by default. You should perform these steps if you want to enable LDAP authentication for legal hold notices.

Note: Clear your browser cache before performing these steps.

1. From the **System** view, click **Settings**, and then click the **Legal Hold Authentication** tab.



2. Select the **Enable LDAP authentication for legal hold confirmation** check box. If authentication for legal hold is enabled, then the custodians will be prompted for LDAP credentials for accessing the legal hold confirmation page.

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

   Note: If LDAP settings are already configured, then the system asks whether to copy those settings. If you choose to copy the preconfigured LDAP settings, the values are populated in these fields except for the Connection Password field.

Field	Description
Connection URL*	An LDAP URL to connect. Contact the network administrator of your organization to get the LDAP URL. Example: *ldaps://foo.com* *ldap://foo.com* **Note:** When “ldaps” is used in the connection URL, the authentication details are transmitted over HTTPS.
Connection Username*	The domain user account to use to connect to LDAP. The network administrator assigns the user account. Example: *user@foo.com*
Connection Password*	Credentials for connection user name. The passwords are transmitted from user to confirmation server over SSL by default, which is a recommended practice. The network administrators should configure “ldaps” for securing passwords sent to Active Directory server.
User Base*	Base DN used to search for a custodian while authenticating against LDAP. The network administrator provides the user base DN. **Note:** Restrict the user base to the minimally required branch of the tree or forest. For example, *ou=Clearwell,dc=foo,dc=com* Also, see Partitions Container.

4. To enable Single Sign-On, select the **Enable SSO** check box. You can use either integrated Windows authentication or header-based authentication. By default, IWA is selected.

   A. For IWA, Select the **Enable Integrated Windows Authentication (IWA) with LDAP** option, and then select the authentication preference:

      › **Use Kerberos only**: When selected, only the Kerberos authentication is used.

      › **Use Kerberos first; if it fails, use NTLM**: When selected, the default Kerberos authentication is used first, and if it fails, NTLM is used for authentication.

   B. For header-based authentication, select the **Enable Header Based Authentication with LDAP** option, and then enter the required details for the following mandatory fields:

      › **Header Name**: Name of the HTTP header, which specifies the username to authenticate. Default value is "*HTTP_USER*".

      › **Login URL**: URL of the webpage that the user should be sent to upon logging out. Default value is "*/public/ssoHoldLogin.jsp*".

      › **Allowed Hosts**: Comma-separated list of hostnames or IP addresses to be accepted. This is a list of Identity Service Providers (ISP)/Gateway Servers through which request is rerouted to the Legal Hold Confirmation Server. Any host not on the list is denied access. At least one allowed hostname or IP address must be specified.

5. Expand **Advanced LDAP Settings (Optional)** and specify the following information.

Note: If you have opted to copy the preconfigured LDAP settings, then the values are populated in some of these fields.

Field	Description
User Subtree	Defines whether to enable or disable searching users in subtrees of the base DN. Defined values are true (default and recommended) or false.
Referrals	Specifies how LDAP provider should follow referrals. Defined values are: • follow (default and recommended for Active Directory): to automatically follow any referrals • throw: to throw a *ReferralException* for each referral • ignore: to ignore referrals.
User Search	Defines a pattern used to determine logon name format for users. Default and recommended value for Active Directory is: *(&(objectClass=user)(|(sAMAccountName={0})(userPrincipalName={0})))*
Protocol	Recommended to keep the security protocol unset for Active Directory. For using SSL for Active Directory, use LDAP Connection URL starting with ldaps (e.g. *ldaps://foo.com*).
Partitions Container	Specifies a configuration container in an Active Directory Partition. Do not set the value if the User Base specified is the forest root. Set the value if the User Base specified is different than the forest root. A typical value is *CN=Partitions,CN=Configuration,DC=foo,DC=com*
Authentication	Specifies the authentication mechanisms for the LDAP provider to use depending on policy requirements. Defined values are: none, simple, or a space-separated list of one or more SASL mechanism names. Recommended to keep it unset.
Deref Aliases	Specifies how LDAP provider should dereference aliases. Recommended to keep it unset. Defined values are: always, never, finding, or searching. • always: to always dereference aliases • never: to never dereference aliases • finding: to dereference aliases only while locating the target entry • searching: to dereference aliases after locating the target entry
Deref Link	Specifies whether enable or disable link dereferencing during the search for user. Defined values are: true or false. Recommended to keep it unset.

6. Before saving the Legal Hold Authentication settings, test the LDAP connectivity. Enter credentials of a valid LDAP user who is part of the User Base provided and then click **Test Connection**.

   Note: Connection gets tested on the confirmation server. If any issue related to LDAP connectivity occurs, then it must be fixed on the confirmation server.
   If LDAP authentication fails, ensure that you have entered correct data such as login credentials and connection URL. You can see the server logs for additional information. If the issue persists even after entering correct data, please contact your network administrator.

7. Click **Save**.

If integrated Windows authentication Single Sign-On is enabled, then perform the following step:

For Active Directory configurations: set the **Service Principal Name (SPN)** for the Legal Hold confirmation server. A domain administrator should run the following **setspn** command for the Legal Hold confirmation server from any system in the domain.

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

where,

cw.LHConfirmationserver.fqdn is the fully-qualified domain name (FQDN) for the confirmation server

customer-domain is the fully-qualified domain name. Example, corp.local

user-running-esa is the user account running the application service on the Legal Hold confirmation server. Example: esaAdmin

Note: Recipients of the legal hold notices must configure their browsers for IWA Single Sign-On. For detailed steps on how to do so, end-users can click **Need Help!** on the Legal Hold Confirmation Portal screen.

Single Sign-On for Legal Hold using SAML

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 Provider (IdP).

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.

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.

For more details and configuration steps, refer to the “Configuring SAML 2.0 based authentication with trusted Identity Provider” in the *System Administration Guide*.

Creating a Legal Hold

Before you can create and send a notice of legal hold, you must create the Legal Hold container. Typically, the Legal Hold is named for the legal matter for which you want to hold information.

Customize Administrator Settings

As the Legal Hold Admin, from the **All Legal Holds > Settings** screen, you can customize the default subject and body text for initial email reminders, escalations, status reminders, and release messages that will be sent out for all notices associated with a single hold. You can also format the body text using the formatting toolbar. The legal hold notice body text does not support image and image hyperlinks.

If you create a hold first, these settings also appear for you to customize on the *Hold* level at the time you create a new hold. If you choose to customize your settings on the Hold level, you will override the default text in **All Legal Holds** > **Settings** with your updated text. If you do not modify the text on the Hold level, the text specified on the *System* level in **All Legal Holds** > **Settings**, will be the default text.

If you choose to customize your settings prior to creating a new hold, your updated text will appear in the new hold as the default. These settings will also be reflected in the text for legal hold notices, (and can only be modified by an administrator, by changing from the Settings screen).

Create a Legal Hold

Each case can contain one Legal Hold, within which you can create multiple legal hold notices. You must have administrator privileges to view multiple holds (from the All Cases Dashboard view.)

Users can view only those legal holds that are added in their associated access groups and the legal holds that are open. Legal holds are considered as open when they are not associated with any access group. By default, when a new legal hold is created, it becomes part of all access groups to which the user has access. When the user is not associated with any access group, then the newly created legal hold becomes an open entity. In this case, the access group permissions should be enforced explicitly.

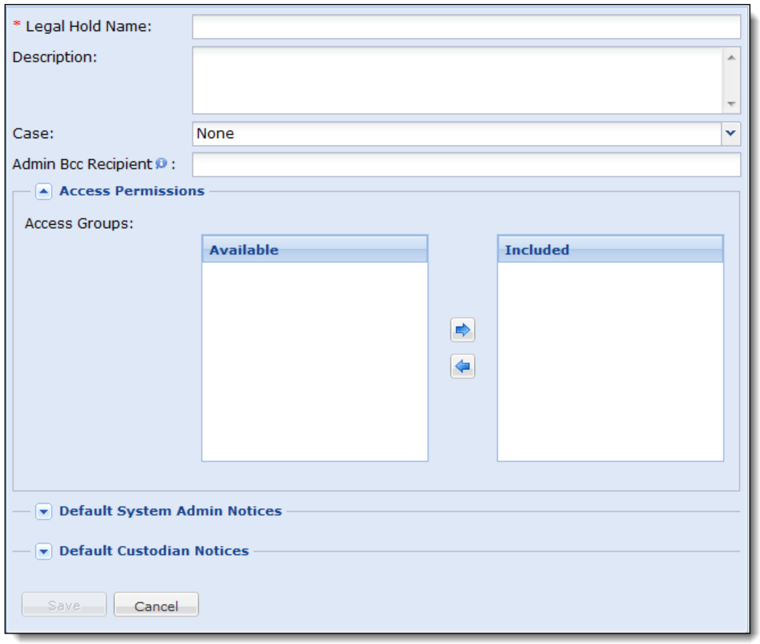
To create a Legal Hold

1. From the navigation bar, do one of the following:
   A. Select a case, and click **Legal Holds**. If no legal holds exist, click **Create Legal Hold**.
   B. (With no case selected) click **All Legal Holds**, then click **Add**. (The main Legal Holds screen is blank until you begin adding Legal Holds for a specified case.)

   Later, use the **Filter List** menu to view by name (*Legal Holds*), *Description*, or *Notices*. You can also search by keywords that your selected filter does (or does not) contain or match, or select parameters to search between.

   If a user has access to a legal hold which is associated with a case, and if the user does not have access to that case, then the All Legal Holds page does not display information related to that case.

The Legal Holds screen is displayed.



2. Do one or both of the following:

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

Legal Hold Information

Field	Description
*Legal Hold Name	Enter a name for this hold.
Description	Enter a description for this hold (up to 255 characters).
Case	Enter or select the case name.
Admin Bcc Recipient	Enter the email address of the administrator to receive copies of all notifications associated with this hold. **Note:** The admin will receive copies of all notifications, including holds, reminders, escalations, status reminders, and release notices. Separate multiple email addresses by commas. The maximum number of recipients is 5. The maximum number of Admin Bcc recipients that can be entered is configurable by the setting: *esa.icp.litholds.AdminRecipients_Max*.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the Legal Hold being added to all groups. Keep only those groups in the **Included** column in which you want to add the Legal Hold and move all the remaining groups to the **Available** column. If the Legal Hold is not added to any group, then that Legal Hold will be available to all users. The System Manager or any administrator with the **Allow user management** and **Allow group management** rights manages the access groups and its members.

(Optional) To change the default admin recipient or default reminder message text on the legal hold system level, you may customize the default settings (see *"Customize Administrator Settings" on page 25*). To change the default notification text sent to administrators for System Admins and/or Custodians notifications for this hold:

- Click to expand the *Default System Admin Notices* option or the *Default Custodian Notices* option and change/enter or format text for one or more of the available notification types:
  - Default Reminder Notice
  - Default Escalation Notice
  - Default Hold Release Notice
  - Default Repeating Status Reminder Notice

3. Click **Save** to submit the hold (and notification information, if applicable), or click **Cancel** to discard your changes.

   These settings will only reflect in this hold's subsequent notices after your settings have been saved.

Creating a Legal Hold Notice

Depending on the recipient's role, there are two types of hold notices you can create: Custodian notices and System Administrator notices. Using the employee data obtained from Active Directory discovery, all potential recipients are listed in the Employee List—those available to be sent a legal hold notice. In Veritas eDiscovery Platform's Legal Hold module, when you create your notices, you can distinguish employees in the Custodian table as System Administrators.

Legal Hold Notice Settings

By default, all notices reflect the notification text set and saved by the Legal Hold administrator for the parent hold. (You must have administrator privileges to modify the default text.)

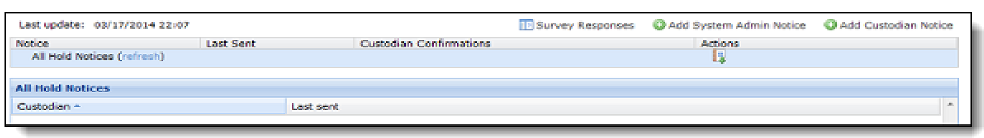
TIP: If you plan to create both types of notices, best practice is to create the System Administrator notice first so that the custodians you select will be pre-populated in the Custodian notice.

To create a Legal Hold Notice

1. From the Legal Holds main screen, click the Legal Hold under which you want to add a notice.

   Note: You can customize settings for the default text in legal hold notices at any time, but the changes will not reflect until the notices are sent.

   For the selected Legal Hold, the main screen displays two tables for notices created for the hold; by individual notice, and for all hold notices. In the All Hold Notices table, notices can be sorted by custodian, and date/time a notice was last sent.



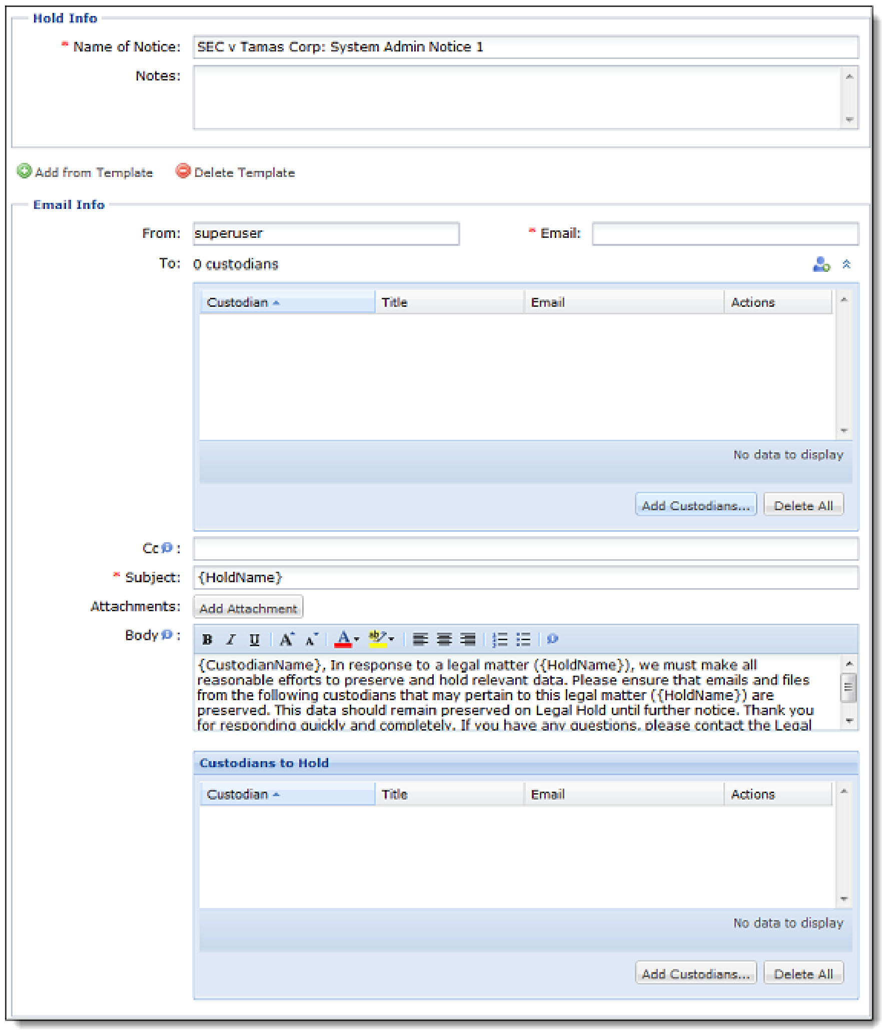
2. Determine which notice you want to add:

   A. System Administrator Notice (continue to step 3 of *"Add a System Administrator Notice" on page 29*.)

   B. Custodian Notice (see step 4, in *"Add a Custodian Notice" on page 34*.)

Add a System Administrator Notice

3. Click **Add System Admin Notice** above the Notices table.

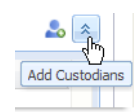


By default, the notice is named for the Legal Hold matter followed by the notice type (System Admin), in sequence. You can edit this text as necessary. See the following table for details.

Note: If you are creating this notice from an existing template, click **Add from Template**. For information about templates, see *"Creating/Saving Notices as Templates" on page 41*. (Alternatively, click **Delete Template** to delete the template you previously added.)

A. In each of the sections of the notice, specify the following information. An asterisk (*) indicates a required field.

System Admin Notice Specifications

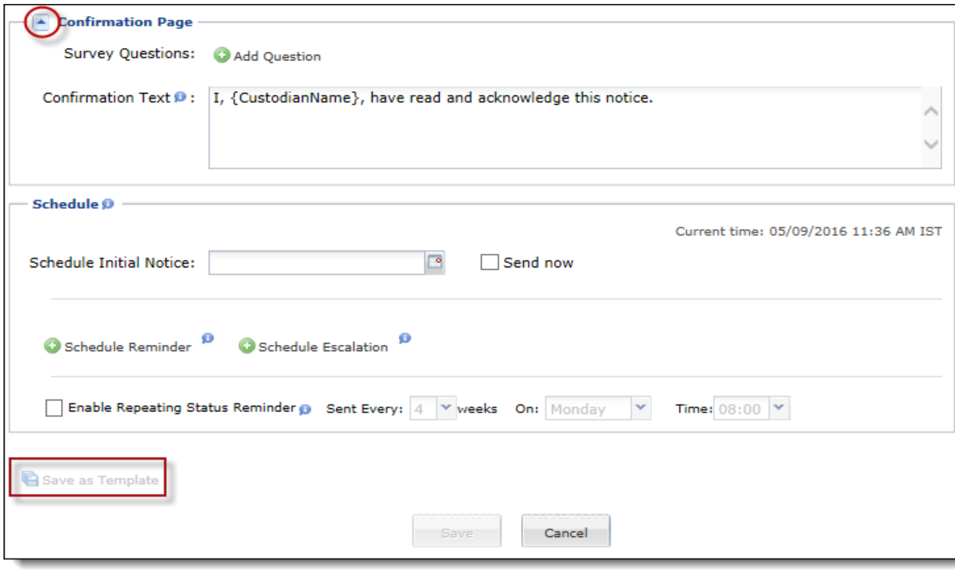
Section	Field	Description
Hold Info	Name of Notice*	To change the default, enter another name for the system admin notice (up to 35 characters).
	Notes	Enter any notes for this notice (up to 255 characters).
Email Info	From	To change/edit the sender, type another name to be displayed to recipients. (By default, the name of the logged on legal hold administrator/user is shown.)
	Email*	Enter the email account to which the recipient's response/ confirmation will be returned.
	To [# of custodians]	If you created the Custodian Notice for this legal hold first, your selected custodians already appear in the list, showing the total number of custodians to receive the notice. To add custodians to this notice, click the **Add Custodians** button to add recipients of this notice. To remove any custodians from the notice, select the name and click the icon. The Custodians table appears, allowing you to select the system administrators from the list, according to which ones should receive the hold notice. With all selections highlighted, click **Select**. To collapse this table, click the arrows next to the icon above the Custodian table. 
	Cc	Enter the email addresses of the recipients who need to be copied. **Note:** The Cc recipients will receive copies of System Admin Notices and replies when the custodian uses "reply to all". Separate multiple email addresses by commas. The maximum number of recipients is 5. The maximum number of recipients can be configured by the setting esa.icp.litholds.CcRecipients_Max. **Note:** Legal Hold System Admin Notices created prior to upgrading are editable to add the Cc recipient field. Legal Hold Notices created prior to upgrade will have blank Cc recipients, but these notices will be editable.
	Subject*	By default, the initial notice subject text from the global hold setting is shown. Alternatively, type another subject title for this notice. For example, "Legal Hold Notice: RESPONSE REQUIRED".
	Attachments	To include an attachment with the hold notice, click **Add Attachment**. The Attachments field appears. Enter the filename, or click **Browse** to the location. (Click **Remove** to delete the attachment from the hold.) **Note:** The maximum number of file attachments per notice is set to 10 while the maximum size of an individual attachment is set to 3 MB by default. The maximum size of a message including attachments depends on the Maximum send message size (MB) limits configured on your Exchange server.

System Admin Notice Specifications (Continued)

Section	Field	Description
(Email Info. Cont...)	Body	To change/edit the default body text provided, type the text you want to appear in the body of the email notice (up to 13000 characters which also includes the characters used by the HTML editor for tagging). When adding or editing Holds or templates, you can use the "Mail Merge" fields which will dynamically insert (auto-replace) these values into the text. These variable fields are demarcated with braces **{ }**. The variable fields include: • **{CustodianName}** - name of the custodian who is receiving the email • **{HoldName}** - name of the Legal Hold • **{NoticeName}** - name of the Notice • **{ClearwellAdminName}** - the default sender's name • **{ClearwellAdminEmail}** - the default sender's email address on the Legal Hold) Each of these variables is replaced with the appropriate value for each notice a custodian or admin receives. The demarcation characters will not show up in the notice a custodian or admin receives. **Note:** You do not need to change/edit the variables in brackets. The Legal Hold module uses the mail merge feature to automatically replace the variables with each variable name where appropriate. You can format the "Mail Merge" fields. To apply formatting to a "Mail Merge" field, it is recommended to select the entire "Mail Merge" field, including the demarcation { } characters.
	Custodian to Hold	Click the **Add Custodians** button to add the custodians whose data and files will be asked to preserve in the system administrator notice. To remove any custodians from the notice, select the name and click the icon.

Note: To save this legal hold notice as a template, below the Body section, click **Save As Template**. For details, see *"Creating/Saving Notices as Templates" on page 41*.

System Admin Notice Specifications (Continued)



Add System Admin Notice (showing Confirmation Page and Schedule Sections)

Section	Field	Description
Confirmation Page (click on the triangle icon to expand)	Survey Questions	Click **Add Question** to include and customize one or more survey-style questions in this notice. See *"Adding Survey Questions" on page 44*. The length of a survey question should not exceed 4096 characters which also include the characters used by the HTML editor for tagging.
	Confirmation Text	To change/edit the default confirmation text provided, enter the text you want the system administrator to view when required to confirm compliance to the legal notice. **Note:** The "{CustodianName}" will be automatically replaced with each custodian, using mail merge.

System Admin Notice Specifications (Continued)

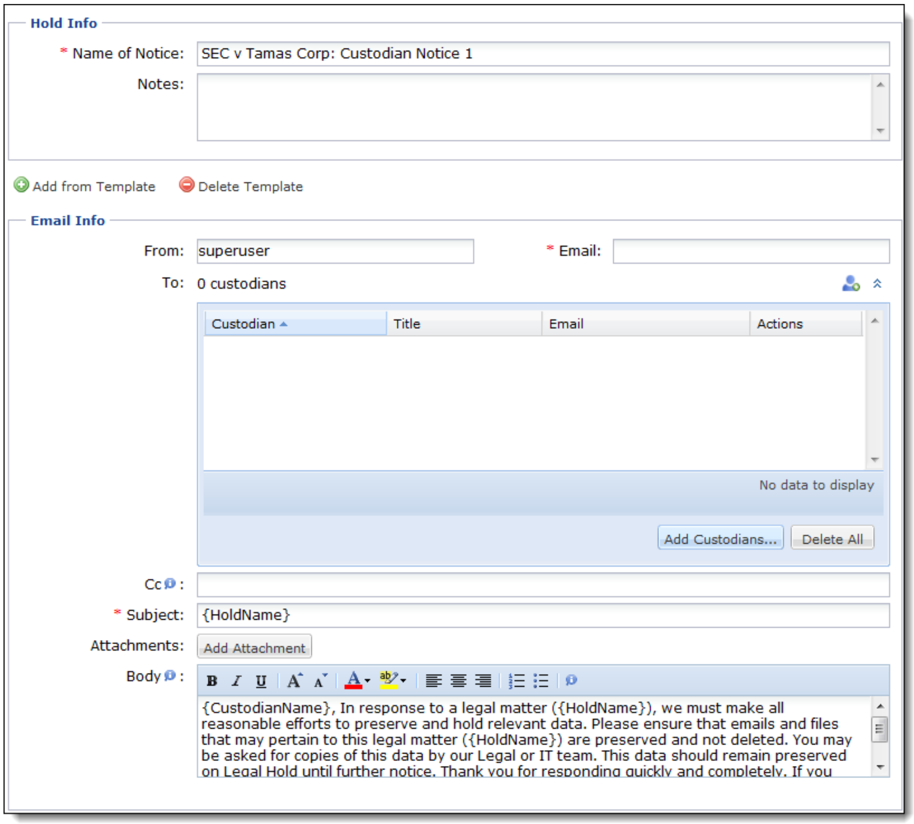
Section	Field	Description
Schedule	Current Time	(Your local date [mm/dd/yy] and time is shown. This reflects your system's configured date/time, and format.)
	Schedule Initial Notice	Schedule this notice to go out at a later date/time. Alternatively, select the option to **Send Now**. See *"Sending/Scheduling Notices" on page 45*.
	Schedule Reminder / Schedule Escalation	To send a reminder or escalation, see *"Sending Reminders or Escalations" on page 46*.
	Enable Repeating Status Reminder	Set recurring status notices to send automatically to all active custodians as a reminder that the hold is still active. Active custodians include the custodians on hold who have not acknowledged their notice as well as the custodians who have already acknowledged their notice. The notice is only a reminder notice, and it does not request reconfirmation. When enabled, select week, weekday, and time of recurrence. **Note:** The default message can be customized in the **Legal Hold** > **Settings** screen.

B. Click **Save** to create the system admin notice, or click **Cancel** to discard your changes.

Add a Custodian Notice

4. Click **Add Custodian Notice** above the Notices table.

   The Add Notice form displays, showing the first two (of four) sections on screen to complete:



   By default, the notice is named for the Legal Hold matter followed by the notice type (Custodian), in sequence.

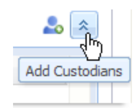
   Note: To create this notice from an existing template, click **Add from Template**. For information about templates, see *“Creating/Saving Notices as Templates” on page 41*. (Alternatively, click **Delete Template** to delete the template you previously added.)

5. In each of the sections of the notice, specify the following information. An asterisk (*) indicates a required field.

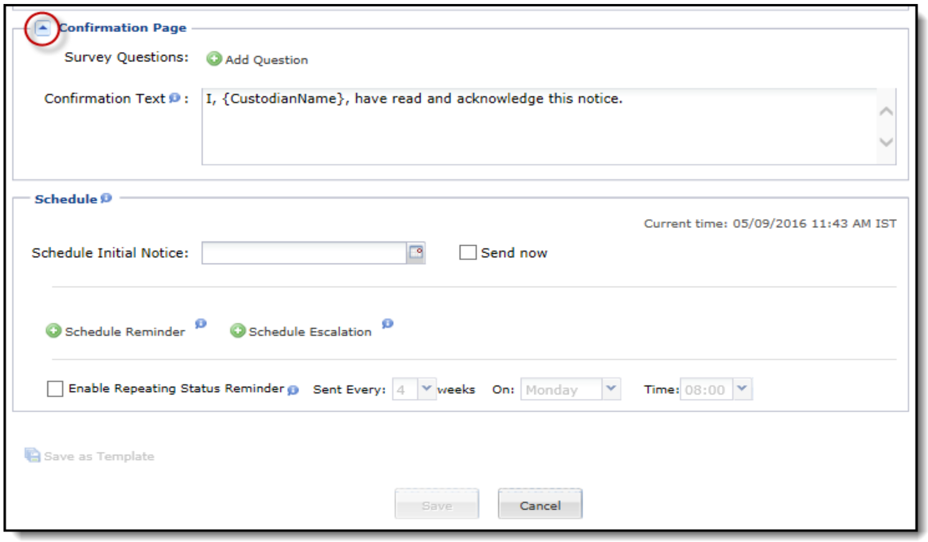
Custodian Notice Specifications

Section	Field	Description
Hold Info	Name of Notice*	To change the default, enter another name for the custodian notice (up to 35 characters).
	Notes	Enter any notes for this notice (up to 255 characters).

Custodian Notice Specifications (Continued)

Section	Field	Description
Email Info	From	To change/edit the sender, type another name to be displayed to recipients. (By default, the name of the logged on legal hold administrator/user is shown.)
	Email*	Enter the email account to which the recipient's response/confirmation will be returned.
	To [# of custodians]	If you created the System Admin Notice for the same legal hold first, your selected custodians already appear in the list, showing the total number of custodians to receive the notice. To add custodians, click the **Add Custodians** button to add the recipients of this notice. To remove any custodians from the notice, select the name and click the icon. The Custodians dialog appears, allowing you to select custodians from the list. With all selections highlighted, click **Select**. To collapse this table, click the arrows next to the icon above the Custodian table. 
	Cc	Enter the email addresses of the recipients who need to be copied. **Note:** The Cc recipients will receive copies of Custodian Notices and replies when the custodian uses "reply to all". Separate multiple email addresses by commas. The maximum number of recipients is 5. The maximum number of recipients can be configured by the setting esa.icp.litholds.CcRecipients_Max. Legal Hold Custodian Notices created prior to upgrading are editable to add the Cc recipient field. Legal Hold Notices created prior to upgrade will have blank Cc recipients, but these notices will be editable.
	Subject*	By default, the name of the notice is shown for the subject. Alternatively, type another subject name for this notice. For example, "Legal Hold Notice: RESPONSE REQUIRED".
	Attachments	To include an attachment with the hold notice, click **Add Attachment**. The Attachments field appears. Enter the filename, or click **Browse** to the location. (Click **Remove** to delete the attachment from the hold.) **Note:** The maximum number of file attachments per notice is set to 10 while the maximum size of an individual attachment is set to 3 MB by default. The maximum size of a message including attachments depends on the Maximum send message size (MB) limits configured on your Exchange server.
	Body	To change/edit the default body text provided, type the text you want to appear in the body of the email notice (up to 13000 characters which also includes the characters used by the HTML editor for tagging). **Note:** You do not need to change/edit the variables in brackets. The Legal Hold module uses the mail merge feature to automatically replace the variables with each variable name where appropriate. You can format the "Mail Merge" fields. To apply formatting to a "Mail Merge" field, it is recommended to select the entire "Mail Merge" field, including the demarcation { } characters.

Custodian Notice Specifications (Continued)



Add Custodian Notice (showing Confirmation Page and Schedule Sections)

Section	Field	Description
Confirmation Page (click on the triangle icon to expand)	Survey Questions	Click **Add Question** to include and customize one or more survey-style questions in this notice. See *"Adding Survey Questions" on page 44*. The length of a survey question should not exceed 4096 characters which also include the characters used by the HTML editor for tagging.
	Confirmation Text	To change/edit the default confirmation text provided, enter the text you want the custodian to view when required to confirm compliance to the legal notice. **Note:** The "{CustodianName}" will be automatically replaced with each custodian, using mail merge.

To save this legal hold notice as a template, above the Schedule section, click **Save As Template**. For details, see *"Creating/Saving Notices as Templates" on page 41*.

Custodian Notice Specifications (Continued)

Section	Field	Description
Schedule	Current Time	(Your local date [mm/dd/yy] and time is shown. This reflects your system's configured date/time, and format.)
	Schedule Initial Notice	Schedule this notice to go out at a later date/time. Alternatively, select the option to **Send Now**. See *"Sending/Scheduling Notices" on page 45*.
	Schedule Reminder / Schedule Escalation	To send a reminder or escalation, see *"Sending Reminders or Escalations" on page 46*.
	Enable Repeating Status Reminder	Set recurring status notices to send automatically to all active custodians as a reminder that the hold is still active. When enabled, select week, weekday, and time of recurrence. **Note:** The default message can be customized in the **Legal Hold** > **Settings** screen.

A. Click **Save** to create the new custodian notice, or click **Cancel** to discard your changes.

Depending on when you chose to send the notice, your selected custodians will receive an email notification to which each individual must respond accordingly. For information on their custom views, see *"Receiving Notification" on page 51*.

To track responses to notices, see *"Tracking and Reporting" on page 59*.

Customizing and Sending Notices

This section describes how to create/save your notices as templates, edit existing notices, and send, or schedule notices to be sent automatically.

- *"About Customizing your Notices" in the next section*
  - *"Creating Templates and Editing Notices" on page 40*
  - *"Adding Survey Questions" on page 40*
  - *"Scheduling Notices, Reminders, and Escalations" on page 40*
- *"Creating/Saving Notices as Templates" on page 41*
  - *"Create a Template" on page 41*
  - *"Apply Templates to a Notice" on page 42*
- *"Adding Survey Questions" on page 44*
- *"Sending/Scheduling Notices" on page 45*
- *"Sending Reminders or Escalations" on page 46*
- *"Resending Notices" on page 48*
- *"Releasing Notices" on page 49*
- *"Deleting Notices" on page 49*

About Customizing your Notices

The Legal Hold module allows you to customize and manage the notices you create, using its template, survey, and scheduling features.

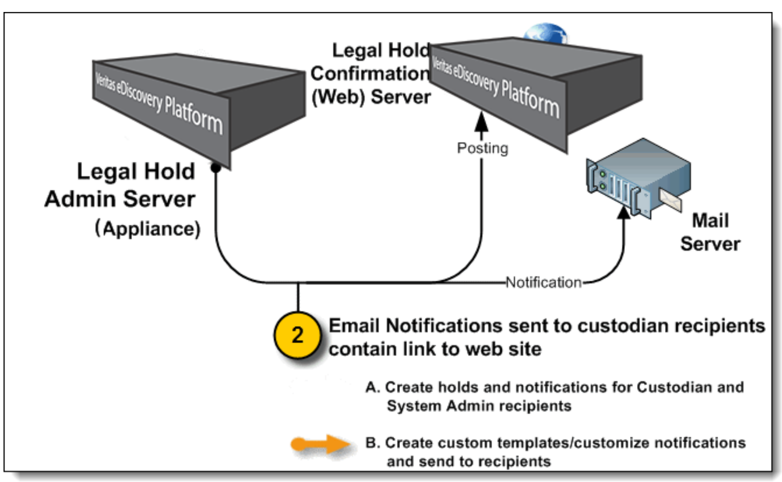


Figure: Legal Hold Process—Step 2 (B): Customizing and Sending Notices

Creating Templates and Editing Notices

In Legal Hold, you can save your notices as templates so that creating and sending notifications is quick and efficient, especially when you repeatedly use the same notice text and survey questions in different legal matters. Further, you can edit any notice you create. When you edit a notice that has not been sent, you can edit the recipient's email information and the sender's name and email address. When the notice has already been sent, you can edit the sender's name and email address and the recipient's email information where you can only edit Cc list and add custodians but you cannot remove the existing custodians. See *"Creating/Saving Notices as Templates" on page 41*.

Adding Survey Questions

For specific notices, depending upon the recipient, you may want custodians or system administrators to respond to a survey, or even require specific recipients to an answer a question upon confirmation. A set of survey-style questions can be added when you create a legal hold notice. See *"Adding Survey Questions" on page 44*.

Scheduling Notices, Reminders, and Escalations

You can also schedule a notice to be sent at a later date, for example, when you want to resend a notification as a reminder if the recipient has not yet responded or confirmed. In some cases, if multiple notifications have been sent, or a response is long overdue, you can send an alert to the recipient's manager. Recurring status notices can also be enabled to send automatically to all active custodians as a reminder that the hold is still active. See *"Sending/Scheduling Notices" on page 45* and *"Sending Reminders or Escalations" on page 46*.

Creating/Saving Notices as Templates

When creating notices for multiple recipients, or you simply need to send notifications quickly, you can create and apply a template. With a customized template, one for Custodians and another for System Administrators, you can pre-populate the subject, body, customize the confirmation text, and add survey questions.

Note: You must first create a Legal Hold, before creating/saving associated notices as templates. (See *"Create a Legal Hold" on page 25*.)

Create a Template

Follow the set of steps in this section depending on which notice template type you want to create, typically when creating a notice. (To apply a template to an existing notice, see *"Apply Templates to a Notice" on page 42*.)

To create a notice template

1. From the navigation bar, click **Legal Holds**.

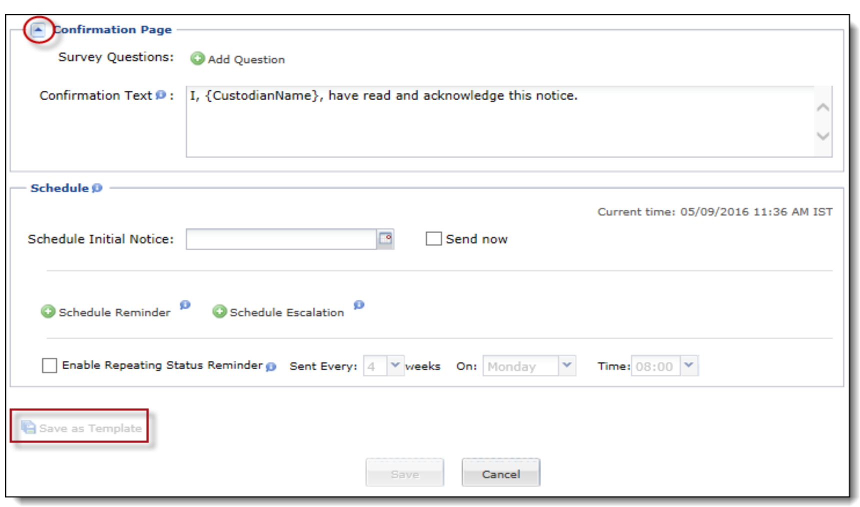
2. Select the Legal Hold for which you want to create a notice template.

3. To create a template:

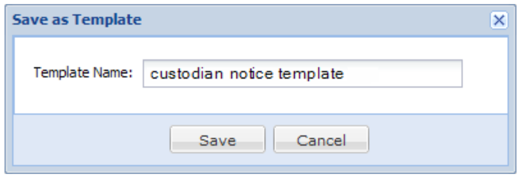
   A. Click **Add System Admin Notice** or **Add Custodian Notice** and complete the Hold Info, Email Info, and Confirmation Page sections (for use as a template) as described in *"Creating a Legal Hold Notice" on page 28*.

   Note: You do not need to change variables. Veritas eDiscovery Platform's Legal Hold module uses "Mail Merge" fields which dynamically insert (auto-replace) the variable values into the text. These "Mail Merge" fields are indicated with braces **{ }**, such as **{CustodianName}**, **{HoldName}**, **{NoticeName}**, **{ClearwellAdminName}**, and **{ClearwellAdminEmail}**.

   B. After the Confirmation Page and Schedule sections, click **Save as Template**.



The Save as Template dialog appears.



C. Enter a name for the template.

D. Click **Save** to create the template. A confirmation dialog appears when the template was saved successfully.

To apply this template when creating other legal hold notices, continue to the next section *"Apply Templates to a Notice" on page 42*.

Apply Templates to a Notice

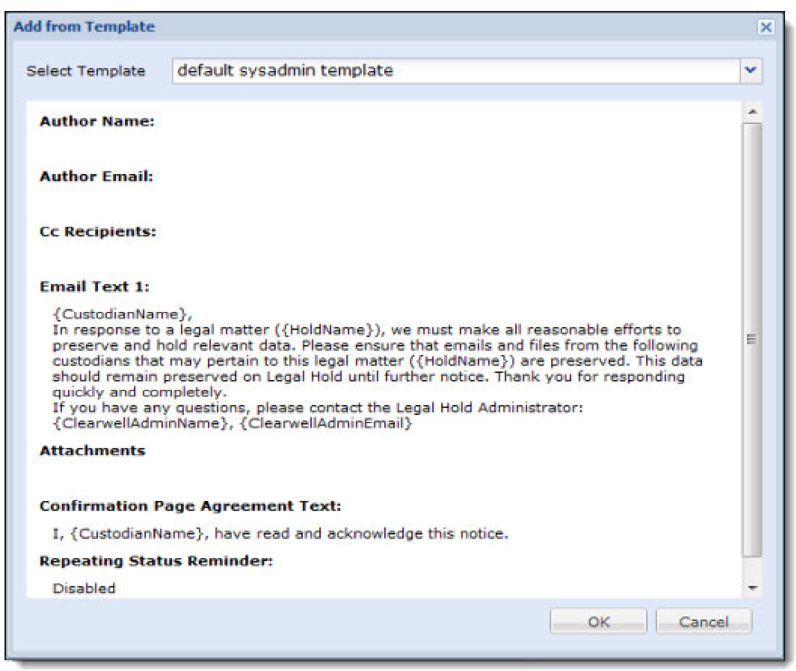
When you create a new notice, as described in *"Creating a Legal Hold Notice" on page 28*, you can immediately apply any template for the selected notice type.

To apply a template

1. With either a System Admin or Custodian notice open, click **Add from Template** to select from a list of created templates.

   The Add from Template dialog opens.

2. Select a notice template.



The author name, author email, Cc recipients, Email Body, Confirmation Page text, and Repeating Status Reminder is displayed for the selected template. Changes can be made to this text from the notice itself.

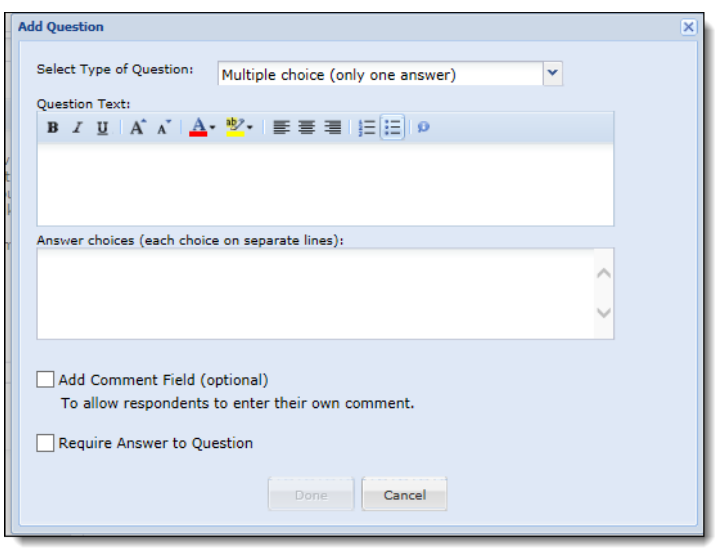
3. Click **OK**.
4. To make any changes/modify this template, click **Save as Template**.
5. Complete the notice as needed, and click **Save**.

Adding Survey Questions

Follow the set of steps in this section depending on which notice you created, and to which you want to add survey questions.

To add a survey question to a notice

1. From the **Legal Holds** module, select the Legal Hold under which you want to create or customize a notice.
2. Create a new notice or customize an existing notice:
   A. To create a new notice, click **Add System Admin Notice** or **Add Custodian Notice** and complete the Hold Info, and Email Info sections (for use as a template) as described in *"Creating a Legal Hold Notice" on page 28*. (Later, you will be able to apply this template by clicking "Add from Template". For more information, see *"Apply Templates to a Notice" on page 42*.)
   B. To select an existing notice to customize, click to edit the information. You can also edit the sender's name and email address in the existing notices that are sent.
3. In the Confirmation Page section, click **Add Question**.
4. On the Add Question dialog, select the question type from the menu.
5. Type the question you want selected custodians for this notice to answer. You can format the question text using the formatting toolbar. The question text does not support image and image hyperlinks.
   The length of a survey question should not exceed 4096 characters which also include the characters used by the HTML editor for tagging. List all possible answers. Each answer must be on a separate line. (Both fields are required.)



6. If you want the recipient to be able to provide additional information, select the option to **Add Comment Field**.

7. If this notice requires the recipient to answer upon confirmation of their notice, select the option to **Require Answer to Question**.

8. When finished, click **Done**.

Sending/Scheduling Notices

Either when creating or editing a notice, you may choose to either send it immediately, or schedule the notice to be sent at a later date/time. You can also change your sending options on any notice that has not yet been sent by editing the notice. (To edit a notice, click the icon next to the notice to be sent or scheduled).

Note: You should not edit the scheduled Legal Hold emails from the **System** > **Schedules** page as these changes does not reflect in the Legal Hold notice.

Send or Schedule a Notice

To send a notification

1. From the **Legal Holds** module, select the Legal Hold containing the notice you want to send or schedule.

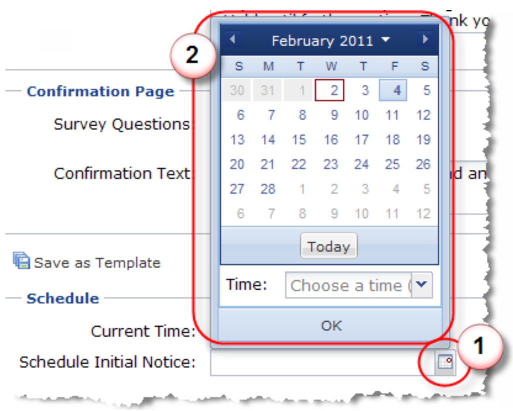
2. Select the notice you want to send now (when creating or editing the notice). For more information, see *"Creating a Legal Hold Notice" on page 28*. To edit the notice, click the icon next to the notice to be sent or scheduled. See also *"Creating Templates and Editing Notices" on page 40*.

3. Select the **Send Now** option in the Schedule section of the notice. When you click **Save**, the notification will be sent.

4. Click **Save** to send the notice immediately to your selected recipients as an email message.

To schedule a notification

1. With the notice open, in the Schedule section, click to select the date and time you want to schedule the notice to be sent. (Selecting the time is optional. Times are shown according to the 24-hour clock, in 15-minute increments.)



2. Click **OK** to close the calendar. (In this example, today's date is the 2nd, and the notice is set to go out on the 4th.)

3. Click **Save**.

Sending Reminders or Escalations

Reminder notices or escalations can be scheduled and sent automatically to custodians who have not yet responded to or confirmed their legal hold notice, and further action is needed. You can also set up automatic recurring status reminders to be sent to custodians with active holds.

When custodians have not responded to all prior legal hold notice reminders, it may be necessary to escalate their failure to respond to their managers. Just as you can schedule a reminder notice, you can also schedule an escalation. As with regular reminders, escalations are automatically sent to custodians who have not yet responded or confirmed by the time of the escalation reminder.

Note: Refer to the Custodians table (**All Cases > Employee List**) to view a summary of legal holds for any custodian. Clicking the custodian displays hold details, including the custodian's escalation manager.

> **Tip:** Default text for reminders, escalations, and status reminders can be customized on the Legal Hold Settings screen.

To send a reminder notice

1. From the **Legal Holds** module, select the Legal Hold containing the notice you want to re-send.

2. Select the notice you want to resend as a reminder. (To edit the notice, click the icon next to the notice to be scheduled. See also *"Creating Templates and Editing Notices" on page 40*.)

3. With the notice open, at the bottom of the Schedule section, click Schedule Reminder .

4. A field "Reminder 1 Date" is added. Click to select the date and time you want to schedule the notice to be sent. (Selecting the time is optional. Times are shown according to the 24-hour clock, in 15-minute increments.)

5. Click **OK** to close the calendar.

6. Repeat these steps for each subsequent reminder you want to schedule. (Alternatively, to delete a reminder, click the icon next to the scheduled reminder you want to delete.)

7. Click **Save**.

To send an escalation notice

1. From the **Legal Holds** module, select the Legal Hold containing the notice you want to re-send.

2. Select the notice you want to escalate. (To edit the notice, click the icon next to the notice to be scheduled. See also *"Creating Templates and Editing Notices" on page 40*.)

3. With the notice open, at the bottom of the Schedule section, click Schedule Escalation .

4. A field "Escalation 1 Date" is added. Click to select the date and time you want to schedule the escalation notice to be sent. (Selecting the time is optional. Times are shown according to the 24-hour clock, in 15-minute increments.)

5. Click **OK** to close the calendar.

6. Repeat these steps for each subsequent scheduled escalation. (Alternatively, to delete a reminder, click the icon next to the scheduled escalation you want to delete.)

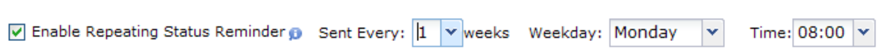
7. Click **Save**.

To send a status reminder notice

1. From the **Legal Holds** module, select the Legal Hold containing the notice you want to add a status reminder to, and set a recurring schedule.

2. Select the notice you want to add to/edit. (To edit the notice, click the icon next to the notice to be scheduled. See also *"Creating Templates and Editing Notices" on page 40*.)

3. With the notice open, at the bottom of the Schedule section, select the option to **Enable Repeating Status Reminder**.

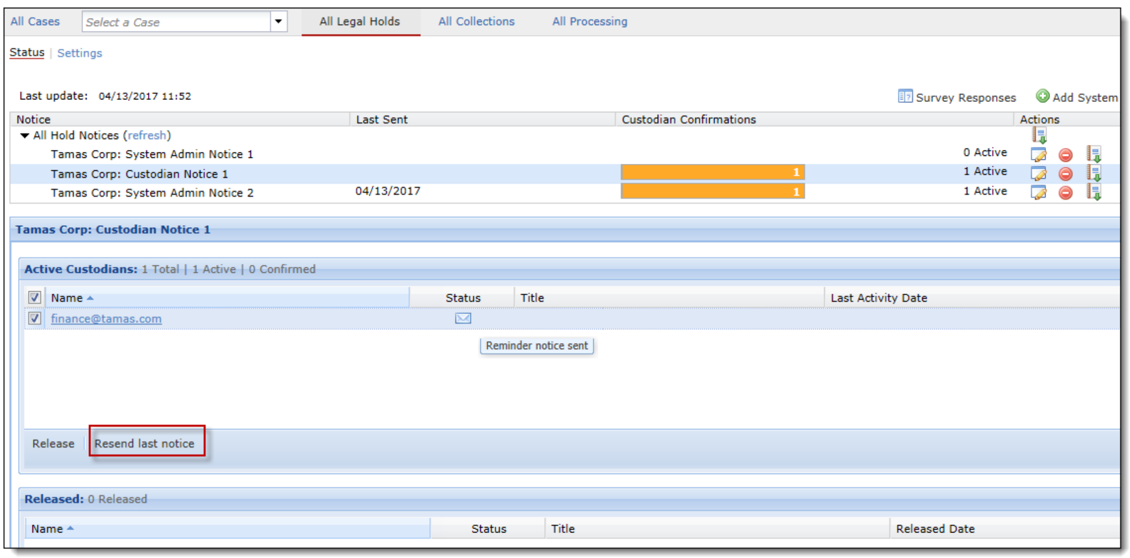


4. Select the number of weeks, the Weekday, and the Time you want the status reminder notice to be sent. the date and time you want to schedule the notice to be sent. (Times are shown according to the 24-hour clock, in 30-minute increments.)

5. (Optional) To customize the default message, go to **Legal Holds > Settings**.
6. Repeat these steps for each subsequent status reminder you want to schedule.
7. Click **Save**.

Resending Notices

Starting with release 8.3, the resend legal hold notice functionality is enhanced where the status of the notice on the UI is consistent with the notice that is sent to the custodian. With the "**Resend last notice**" option, resending a legal hold notice is associated with the last notice sent. For example, if the last notice is a reminder, then on resending the last notice, the custodian receives only a reminder notice instead of an initial notice. The status on the UI is displayed as “Reminder notice sent.”



Releasing Notices

Custodians can be obligated to a legal hold for any length of time, and released at any time, whether or not they have confirmed or responded to one or more legal hold notices. You may either want to keep custodians on a legal hold indefinitely, without releasing them, or as long as necessary to ensure that data is preserved. However, when potential custodians are no longer considered relevant to a legal matter, or you no longer need to preserve the data associated with them, you can release the custodians from the hold.

> **Tip:** Default text for release notices can be customized on the Legal Hold Settings screen.

To release a custodian

1. Select the hold.
2. Select the notice from which to release the custodian.
3. Click the (broken chain link) icon next to the custodian's name.
4. Click the **Confirm** button in the dialog box to confirm that you want to release the custodian from the hold.

Deleting Notices

You can delete any notice that has not yet been sent. To delete a notice, select the hold containing the notice you want to delete. Then click the icon next to the notice. At the "Delete Notice" confirmation dialog prompt, click **OK** to confirm deletion of the selected notice.

Receiving Notification

This section describes how recipients receive, view, and respond to legal hold notices.

- *"Customized Notification and Web Portal Views" in the next section*
  - *"Receiving Email Notification" on page 51*
  - *"Viewing and Responding to Legal Hold Notices" on page 54*

Customized Notification and Web Portal Views

Veritas eDiscovery Platform's Legal Hold module connects with a Legal Hold Confirmation server which hosts a custom Web Portal used exclusively for recipients of Legal Hold notices.

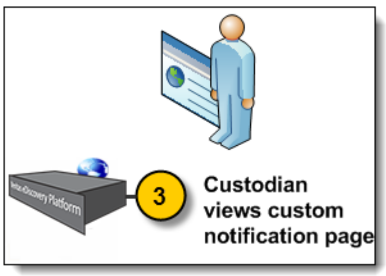


Figure: Legal Hold Process—Step 3: Receiving Notices: Views and Responses

Note: For more information on the supported browsers, refer to *Browser Compatibility Charts*.

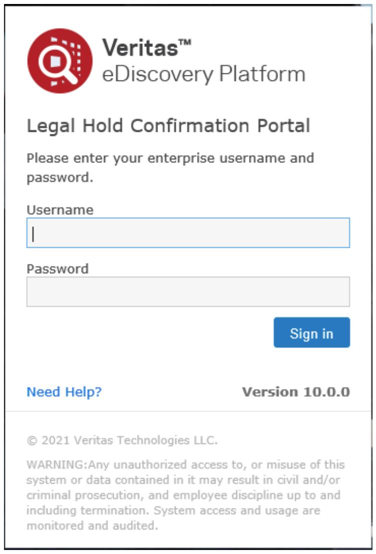
Receiving Email Notification

The notice is received as an email in the custodian's or system administrator's email Inbox.

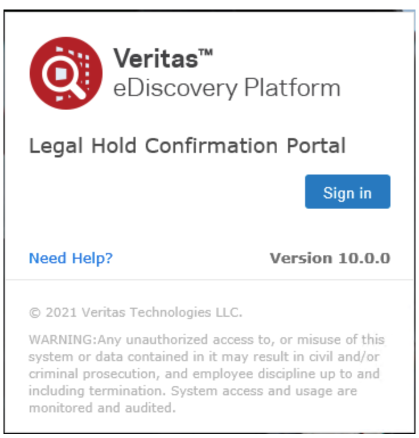
A custodian can receive both types of notices, notices that require authentication and the notices that do not require authentication. The system asks the custodians to log in using their enterprise user name and password to view and respond to the legal hold notices that require authentication.

When a custodian attempts to access a notice which is not intended for him, the system warns such a custodian that he is not the intended recipient of the legal hold notice and only those notices are displayed that the custodian is authorized to view.

When a recipient clicks a link in the email for a notice that requires authentication, the recipient is directed to the Legal Hold Confirmation Portal. The user needs to use their enterprise user name and password to view and respond to the notice.



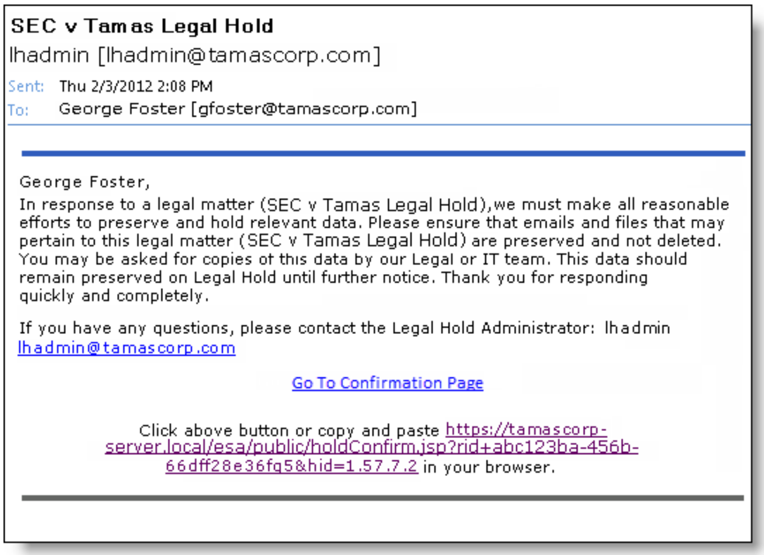
When eDiscovery Platform is configured for Single Sign-On, users do not need to provide their login credentials whereas they are directly logged into eDiscovery Platform.
For details, see *"Single Sign-On for Legal Hold using IWA or Header-based authentication" on page 19*.



The following email examples show both types of Legal Hold notices received.

Custodian Notification Email

The custodian receives an email notifying him of the obligation to hold all data related to the legal matter. He clicks the "Go To Confirmation Page" link to view the notice and respond.



SEC v Tamas Legal Hold

lhadmin [lhadmin@tamascorp.com]

Sent: Thu 2/3/2012 2:08 PM

To: George Foster [gfoster@tamascorp.com]

George Foster,

In response to a legal matter (SEC v Tamas Legal Hold),we must make all reasonable efforts to preserve and hold relevant data. Please ensure that emails and files that may pertain to this legal matter (SEC v Tamas Legal Hold) are preserved and not deleted. You may be asked for copies of this data by our Legal or IT team. This data should remain preserved on Legal Hold until further notice. Thank you for responding quickly and completely.

If you have any questions, please contact the Legal Hold Administrator: lhadmin lhadmin@tamascorp.com

Go To Confirmation Page

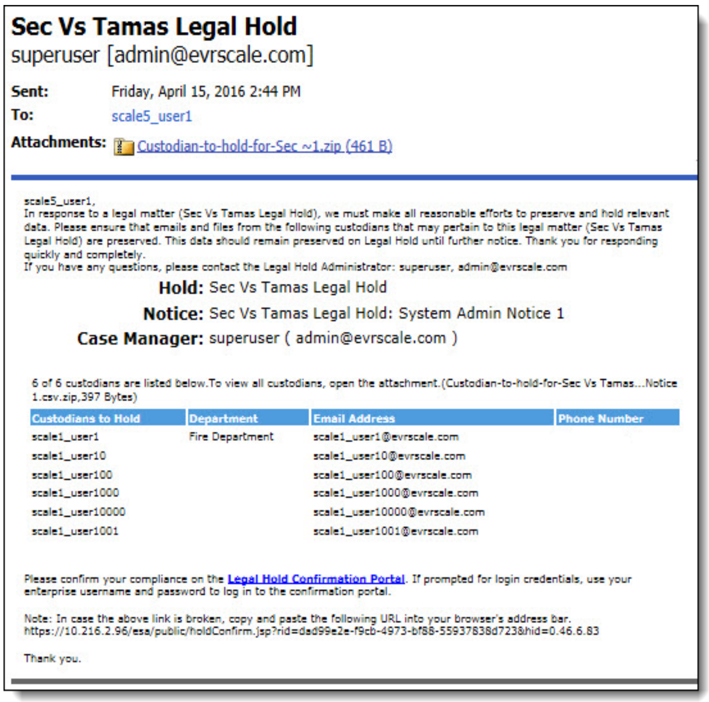
Click above button or copy and paste https://tamascorp-server.local/esa/public/holdConfirm.jsp?rid+abc123ba-456b-66dff28e36fg5&hid=1.57.7.2 in your browser.

Figure: Custodian Notification Email Example

System Administrator Email

The system administrator’s email notifies him to hold all data for the list of the custodian(s) involved related to the legal matter, then clicks “Go To Confirmation Page” to respond.

Note: The system displays the first 50 of the custodians on the system administrator’s notice email and provides an attachment file that contains the complete list of custodians whose data and files must be preserved. The custodian might need to log in using their enterprise user name and password to view the secured legal hold notice if LDAP authentication is enabled.



Sec Vs Tamas Legal Hold
superuser [admin@evrscale.com]

Sent: Friday, April 15, 2016 2:44 PM
To: scale5_user1
Attachments: Custodian-to-hold-for-Sec ~1.zip (461 B)

scale5_user1,
In response to a legal matter (Sec Vs Tamas Legal Hold), we must make all reasonable efforts to preserve and hold relevant data. Please ensure that emails and files from the following custodians that may pertain to this legal matter (Sec Vs Tamas Legal Hold) are preserved. This data should remain preserved on Legal Hold until further notice. Thank you for responding quickly and completely.
If you have any questions, please contact the Legal Hold Administrator: superuser, admin@evrscale.com

Hold: Sec Vs Tamas Legal Hold
Notice: Sec Vs Tamas Legal Hold: System Admin Notice 1
Case Manager: superuser (admin@evrscale.com)

6 of 6 custodians are listed below.To view all custodians, open the attachment.(Custodian-to-hold-for-Sec Vs Tamas...Notice 1.csv.zip,397 Bytes)

Custodians to Hold	Department	Email Address	Phone Number
scale1_user1	Fire Department	scale1_user1@evrscale.com	
scale1_user10		scale1_user10@evrscale.com	
scale1_user100		scale1_user100@evrscale.com	
scale1_user1000		scale1_user1000@evrscale.com	
scale1_user10000		scale1_user10000@evrscale.com	
scale1_user1001		scale1_user1001@evrscale.com	

Please confirm your compliance on the Legal Hold Confirmation Portal. If prompted for login credentials, use your enterprise username and password to log in to the confirmation portal.

Note: In case the above link is broken, copy and paste the following URL into your browser's address bar.
https://10.216.2.96/esa/public/holdConfirm.jsp?rid=dad99e2e-f9cb-4973-bf88-55937838d723&hid=0.46.6.83

Thank you.

Figure: System Admin Notification Email Example

Viewing and Responding to Legal Hold Notices

Depending on whether the recipient is a custodian or system administrator (tasked with placing holds on custodian accounts), each will see a customized Web page view showing the holds and history of responses and/or holds requiring their response.

Custodians can save their responses to unconfirmed legal hold notices as a draft and then submit the responses by confirming the compliance at their convenience. If a custodian navigates away from a browser or closes it, the system displays a warning to confirm whether the user wants to save the response as a draft. Custodians must answer all mandatory survey questions to be able to confirm their compliance.

The survey response saved as a draft is not included in any legal hold reports.

When a user clicks on the checkbox to acknowledge the notice, if a mandatory question is unanswered, the panel gets expanded and scrolled automatically to the first mandatory unanswered question. Also, these mandatory questions are highlighted with a rectangular box until user answers these questions.

The following Web page views are examples of each type of Legal Hold notification.

Custodian Notice View

In the Web page, two tabs appear at the top, showing the custodian's Active and Pending Holds, as well as those from which he has been released, if applicable.

Click on the triangle icon to expand the survey questions.

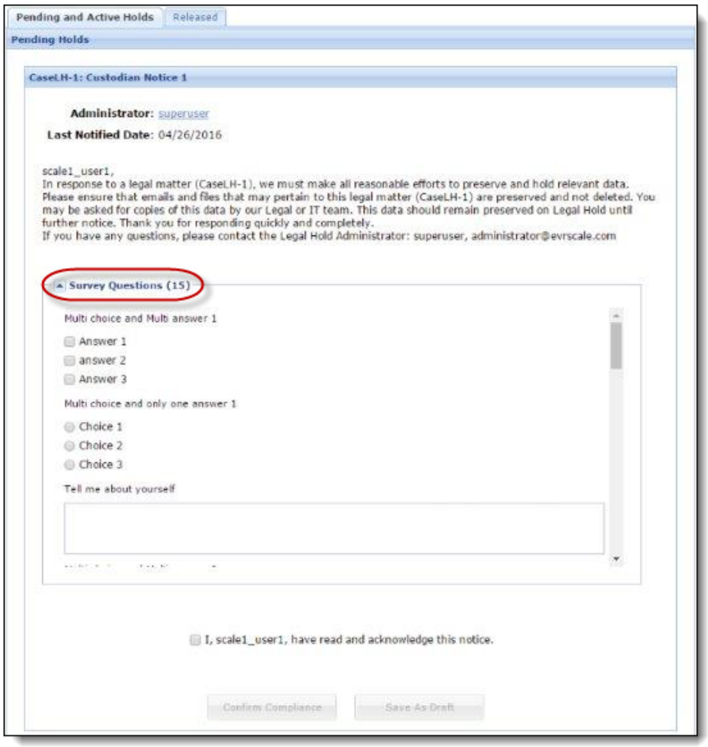


Figure: Custodian Notification Web Page View Example

In this example, the custodian has no pending holds. He has already responded to the active hold, showing two survey questions he previously answered. However, he has the option of providing additional information, even after originally responding to an active hold, by resubmitting the survey.

Note: Surveys in progress are not saved until the notification is submitted. For example, if a recipient has begun to answer survey questions, but did not complete it at the time of a network interruption or browser timeout, the custodian must re-open the notice and start again.

System Admin Notice Confirmation Page

The legal hold notification web page for a system administrator includes a list of custodians for which documents must be held.

Note: The system displays the first 50 of the custodians on the system administrator's notice confirmation page and provides a link to get the complete list of custodians whose data and files must be preserved. You might need to log in using your enterprise user name and password to view the secured legal hold notice if LDAP authentication is enabled.

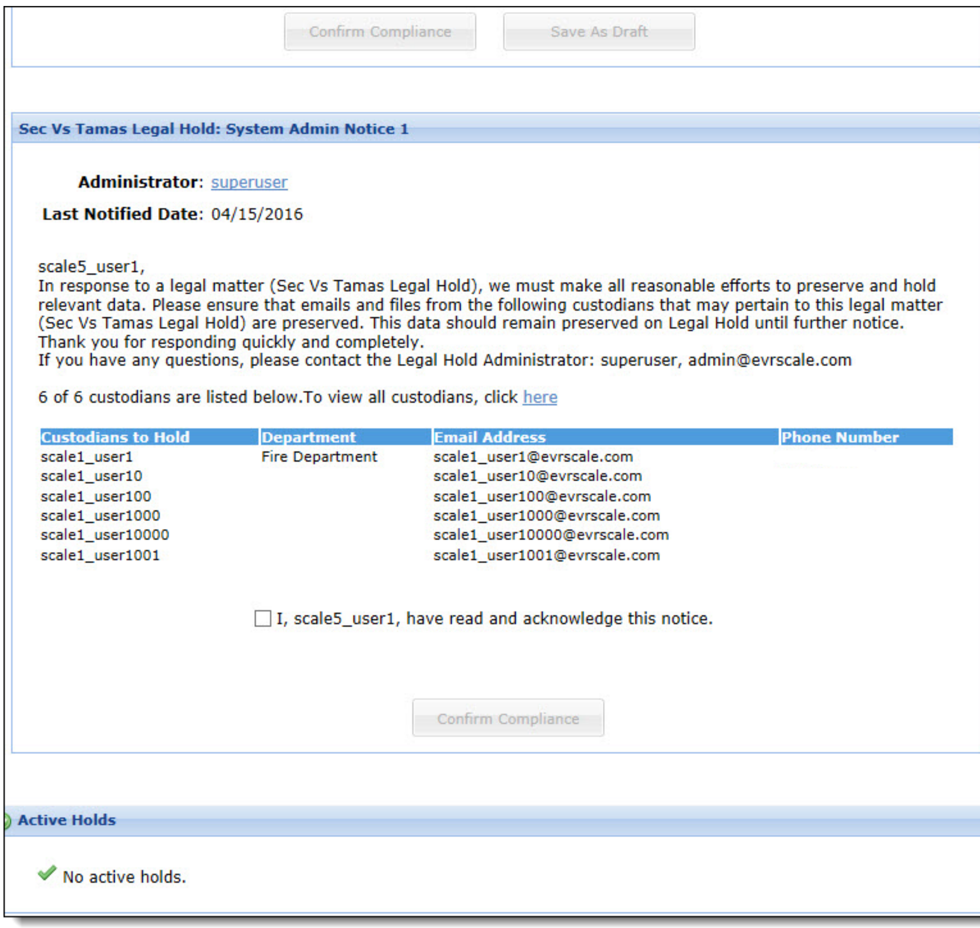


Figure: Example: System Admin Notice Confirmation Page

In this example, the system administrator just received a hold, pending his acknowledgment. He is required to respond by clicking "Confirm Compliance". He must then hold all emails and files from the listed custodian in the SEC v Tamas Corp legal matter.

As the legal hold administrator, you can also view each custodian's pending and active holds, directly from the main dashboard of the selected hold. See *"Tracking and Reporting" on page 59* to track responses and monitor activity on all legal hold notifications.

Tracking and Reporting

This section describes how to view your legal holds and associated notices to monitor recipient confirmations and check survey responses.

About Legal Hold Tracking and Reporting

Once your legal hold notices have been sent, you can start tracking custodian responses. From the Legal Holds main page, you can view the status of all notifications and response activity of each recipient, including survey results and any additional comments provided.

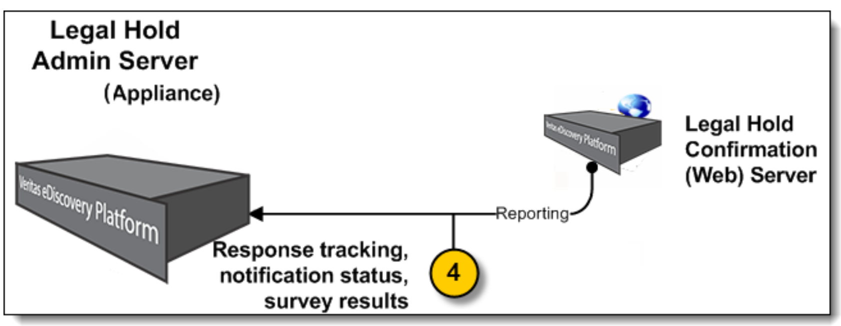
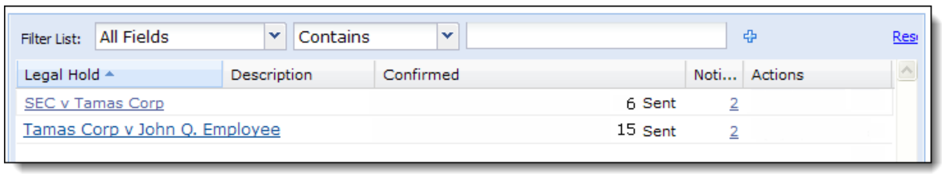


Figure: Legal Hold Process—Step 4: Tracking and Reporting Notification Activity

Viewing Holds and Notices

As custodians or system administrations respond to/confirm their hold notices, a brief view of activity is shown on the main page for all legal holds. Refer to this section to view details of all notifications for each hold, monitor response activity, and review survey results.



Viewing All Notices and Activity for a Single Hold

To monitor activity in detail, you can view a Legal Hold report showing which custodians have, or have not yet confirmed/responded to their notices. You can also check whether notices were sent successfully, or if an error occurred in sending the notice.

A two-table dashboard view shows all holds above, with the list of associated custodians for the hold in the "All Hold Notices" table below.

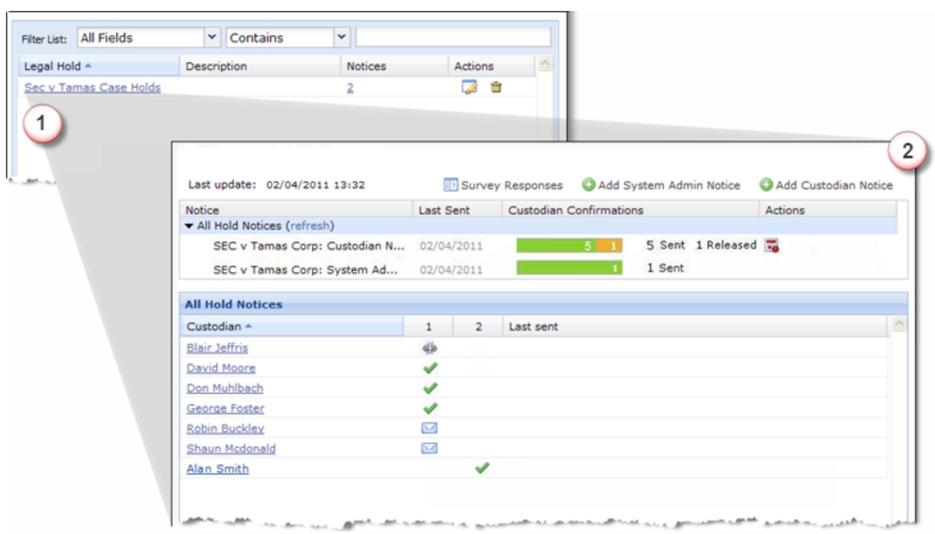


Figure: Viewing Notification Activity for a Single Hold

From the Legal Holds menu, select a hold to check notification activity for a specific hold and view further detail (1). Viewing a single Legal Hold shows all notifications associated with that legal hold, and a summary (graphic bar) showing the number of responses received out of the total sent (2).

The top box shows a summary view of each notification created for the selected hold. A progress bar displays the number of notices confirmed out of the total sent, followed by the possible actions you can take on any active holds.

The All Hold Notices table below the hold summary provides a detailed view of the notices, shown sorted by custodian. Each column corresponds to the notice order in the top box. (For example, Custodian Notice 1 is column “1”, followed by System Admin Notice 1 in column “2”, regardless of the numbered label of the notice).

> **Tip:** Click the right end of the column header to sort by ascending or descending order, or to change which columns you want to view.

The last column shows the date each was last sent. A “Mail” icon indicates that the notification was sent successfully. For all notifications, “confirmation” icons appear next to the custodians who have confirmed their notices, as well as responses still pending.

Note: If any error occurred in sending notifications, a failed email icon would appear indicating which were unsuccessful.

Viewing Custodian Activity for a Single Notice within a Hold

In the top summary box, click one of the notices for the selected legal hold to view more detail.

The table below shows all active custodians and the status of their hold notices. The bottom table displays those custodians released from the hold.

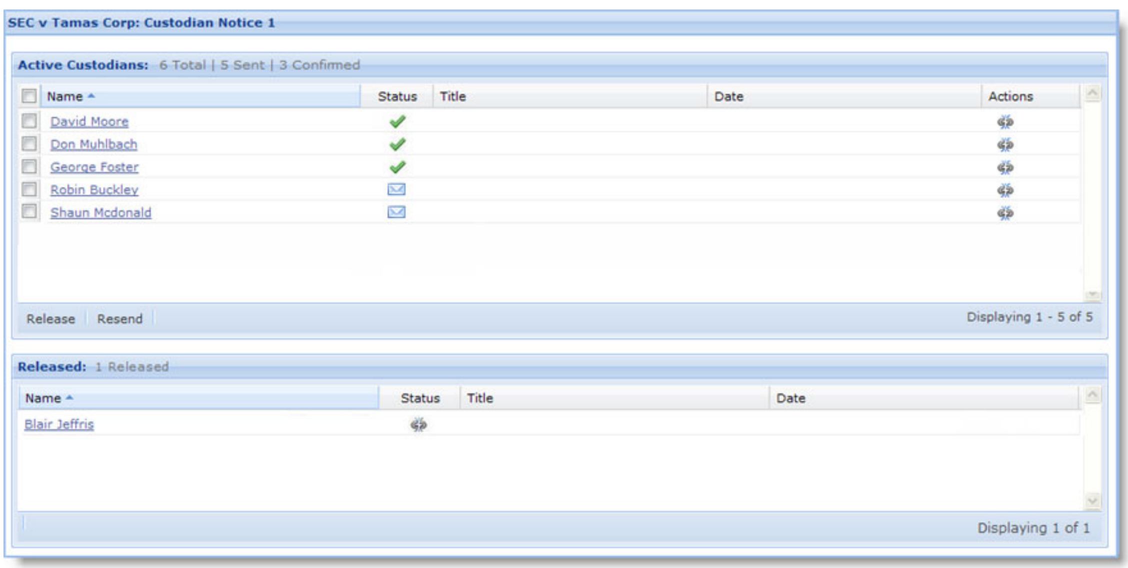


Figure: Viewing Hold Notice Detail within a Legal Hold

The far right column contains icons for the possible actions you can take on each custodian. Select one or more boxes next to a custodian to take action. Clicking the check box in the Name column header selects all custodians at once.

Viewing Notices for Individual Custodians

To see the custodian’s (Web page) view of the legal hold notification sent, click an individual custodian’s name in the “All Hold Notices” table.

The Web page confirmation page opens, showing the total pending and active holds for the selected custodian.

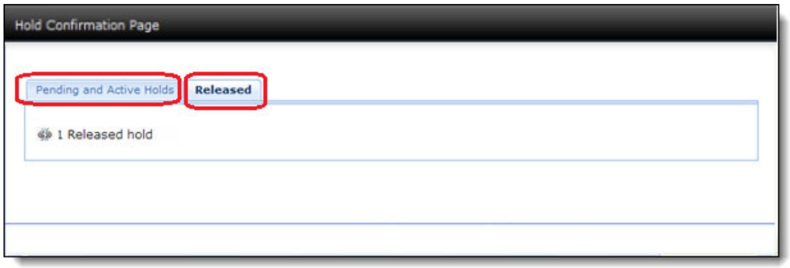


Figure: Custodian Web Page Notification Summary: Legal Hold Admin View

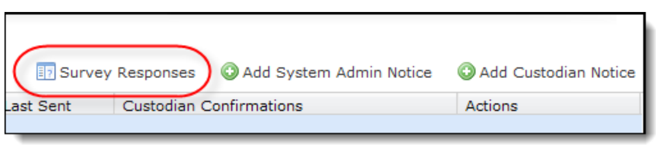
Click the **Released** tab to view the holds from which the custodian has been released. When finished, click to close the window.

Viewing Survey Responses

Depending on whether questions were added to the notice, the custodian may also provide additional potentially important case information by answering a survey (optionally required) as part of their obligation to respond. (See *"Adding Survey Questions" on page 44*.) You can view a report of these answers either collectively, or by individual survey responses.

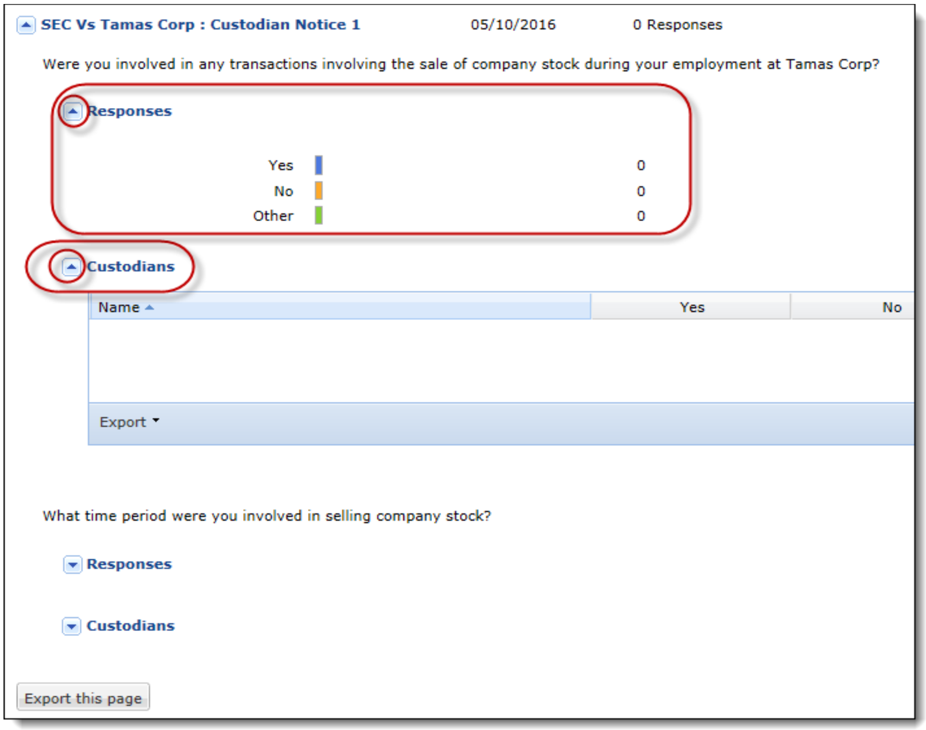
To view custodian survey responses

1. From the **Legal Holds** module, select the legal hold containing the notices you sent with survey questions.
2. Select a notice with survey responses.
3. On the top right of the page, click **Survey Responses**.



The Survey Responses page for the selected hold appears showing all respondents and their tallied results summarized in bar graph format.

Note: A bar graph appears only for *multiple choice* survey questions. For *freeform text* survey questions, a bar graph for responses does not appear.



4. To view response detail (see responses for individual custodians), click on the triangle next to "Custodians" in any section.

5. When finished viewing, click the breadcrumb links at the top of the page to navigate back to the selected legal hold, or all main legal holds page.

   You may want to check back periodically as custodians either submit their responses for the first time, or resubmit surveys to provide additional information, not previously submitted with prior notifications.

   Note: To export custodian detail, click **Export**, and select an export format (CSV or XLS). See *"Export Legal Hold Data" on page 66*.

Generating Reports and Exporting Legal Hold Data

Legal Holds reports allow users and legal representatives to increase the defensibility and tracking of legal holds. You can either generate a Legal Hold Defensibility report and a Legal Hold Report by Custodian report, or export data from various pages/views in the Legal Hold module.

You can generate or export reports for a single notice or all legal holds within a case (Case Home view), or export data for all legal holds across all cases (System view).

Generate the Legal Hold Defensibility Report

A Legal Hold Defensibility report provides a summary of legal hold information including Case name, Legal Hold name and type, Cc recipients, Admin Bcc recipients, and custodian details. The report provides evidence of all legal hold activity or for a single notice within a case (also referred to as “LH Activity Report” or “Legal Hold Notice Summary Report”). Report data for a single legal hold notice for example, includes when the notice was sent, to which custodians (including status and email addresses), as well as an audit trail showing recent activity of and responses to the legal hold notice.

To generate Legal Hold Defensibility report

1. From the **Legal Holds > Status** screen (within a specific case), click the report icon to download the Legal Hold Defensibility (notice summary) Report for all legal holds in the case, or for a selected legal hold notice.

   Veritas eDiscovery Platform generates the report as a legal hold job.

   Note: The report job is not saved in Veritas eDiscovery Platform for later retrieval. Clicking on the “X” next to an item in the Jobs window deletes that job. To download report information at a later date requires running a new job.

2. Click the **Jobs** link to view status, and download the report.

3. On the Download window, choose to **Open** or **Save** the report. Note that the filename “Legal Hold Defensibility Report” is appended with the legal hold notice name, and an ID number.

Generate the Legal Hold Report by Custodian

The **Legal Hold Report by Custodian** report provides a summary of custodians in an organization that are put on hold across cases and legal holds.

This report provides:

– List of all custodians on legal hold and the corresponding list of legal hold notices, legal holds and cases.

– Status of the custodians on hold and the date the last message was sent to the custodian.

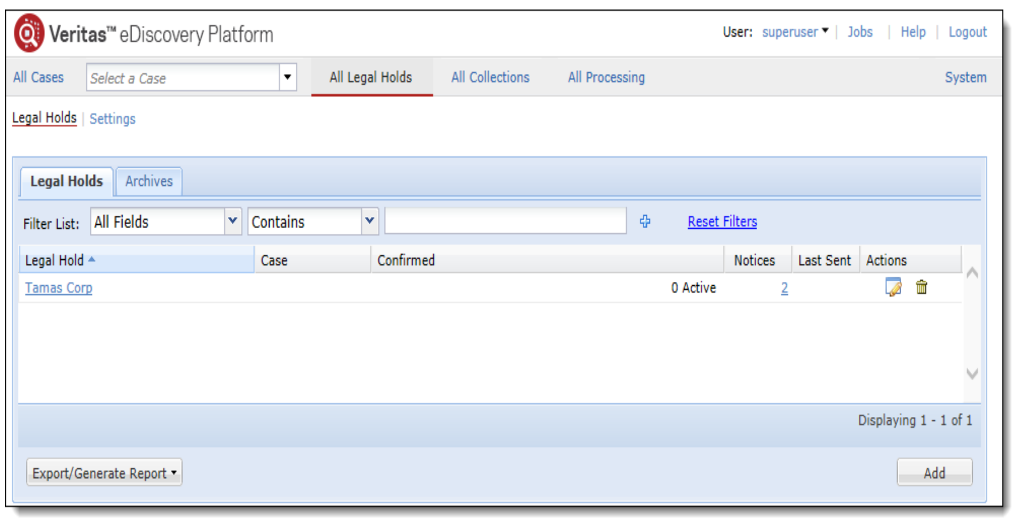
This report helps administrators by following up with any custodians who are not responding to a notice or reminder. Also, the global view of the custodians provides for effective reporting and tracking of custodians.

Note: Only users with the System Manager or Legal Hold Admin privileges can generate this report. Users can only generate this report pertaining to the access groups that they have access to. By default, all the accessible legal holds and cases are included in this report.

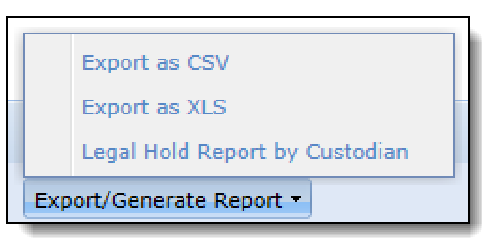
The **Legal Hold Report by Custodian** report includes custodian information such as name, department, location, and email address, information related to the cases and legal holds, including the current status of the notice and email ID of the author of the notice. The report is predefined and sorted out by **Custodian** column, by default.

To generate the Legal Hold Report by Custodian report:

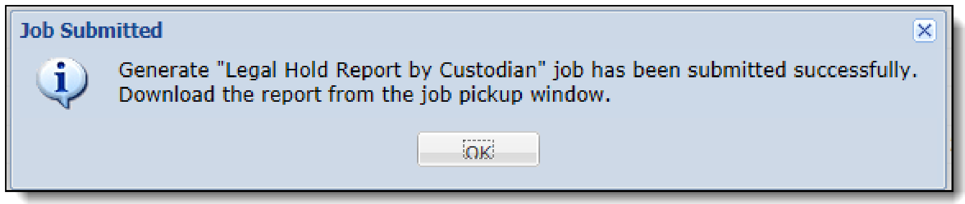
1. From the **System** view, click **All Legal Holds**. The Legal Holds screen appears showing all legal holds across all cases.



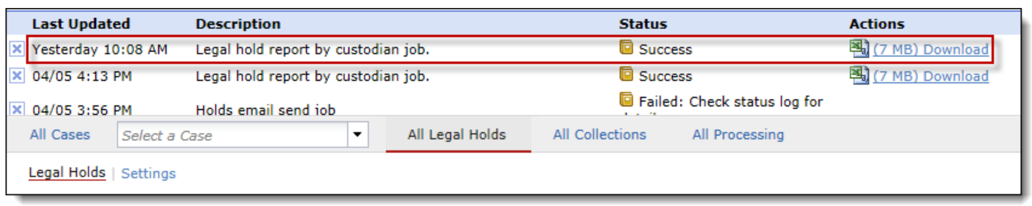
2. Click **Export/Generate Report**, and then click **Legal Hold Report by Custodian**.



3. A Job Submitted window appears. Click **OK**.

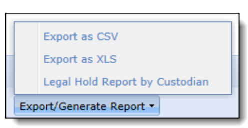


4. Click the **Jobs** link to view status, and download the report.



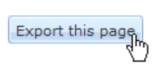
5. On the Download window, choose to **Open** or **Save** the report.

Export Legal Hold Data



There are two ways to export legal hold data, depending on your requirements, user role and case access, and your current view of the legal holds (System or Case Home):

1. Simple Export. Click **Export this page**, for pick up from the *Jobs* window, or



2. Direct Export. Click (**Export/Generate Report > Export as** [**CSV** or **XLS**].

For simple export (Case view)

- From the Case Home view (within a selected case), on the **Legal Holds** > **Status** screen, click **Export this page**. (This option is also available from the survey responses page, overview.)

  Veritas eDiscovery Platform generates the report as a legal hold job, for viewing and download from the Jobs window.

For direct export

- From the **System > All Legal Holds** view, click **Export/Generate Report**, and select **Export as CSV** or **Export as XLS**. (This option is also available from the survey responses page, under the Custodian detail view.)

  The CSV file option allows you to include tabular data (comma delimited data format). Alternatively, select the XLS format to export your data as a Microsoft Excel spreadsheet.

- At the prompt, click to **Open** or **Save** the file.

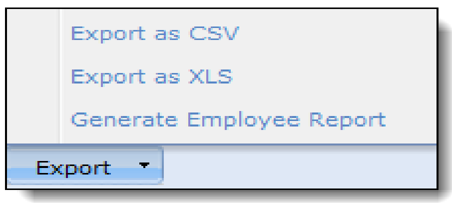
Note: Export of data or records in legal hold survey response report is limited by the maximum number of rows and columns supported by Microsoft Excel.

Generate Employee Report

You can generate reports for custodians' legal hold activities across all cases.

To generate Employee Report

1. From the **All Cases** view, click **Employee List**.
2. Select the employee(s).
3. Click **Export**.



4. Select **Generate Employee Report**.
5. Download the generated report from the Jobs window.

Administration and Maintenance

This section describes how to manage and maintain your legal holds in Veritas eDiscovery Platform.

Note: For information about global user accounts, any other user account types, or general account administration on the appliance, refer to *"Managing User Accounts" in the System Administration Guide*.

About Legal Hold User Privileges

A user's account and its associated user role determine the level of legal hold administration tasks that the user can perform.

A Legal Hold Administrator, *Legal Hold Admin*, by default can manage all legal hold administrative tasks (but not collections, unless explicitly granted) within the system.

The system administrator can create access groups and associate the users, Legal Holds, sources, locations, collection sets, and cases for these access groups. Users can view only those legal holds that are added in their associated access groups or the legal holds that are open. Consult the *Identification and Collection Guide* section "*Managing Access Group Permissions*" for details.

Administrator-level users can edit/define Legal Hold Admin options to only allow legal hold viewing access to legal holds, and/or allow or restrict case processing. To edit the Legal Hold Admin role, see *"Viewing/Editing the Legal Hold Admin Role" on page 73*.

If you are upgrading from a previous version, in which the Collections Admin role was used for Legal Hold administration, the Collections Admin role will only have privileges to view/manage collections upon upgrade. To grant Legal Hold privileges to the same user, you can create a new role based on Legal Hold Admin privileges and add collection rights as necessary. Alternatively, you can assign the eDiscovery Admin role to a user to automatically grant both Legal Hold and Collections rights, among other default privileges.

Assign Legal Hold User Privileges

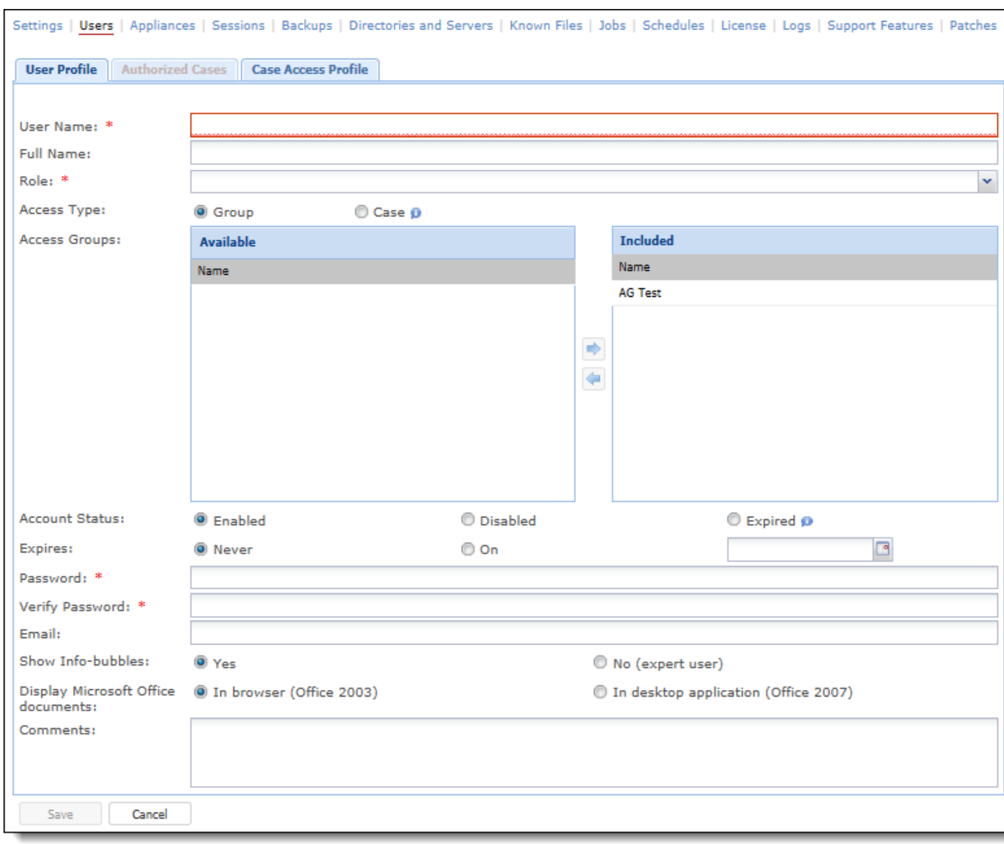
Assign privileges to an existing user, or create a new user and add legal hold user privileges using the Collections Admin role to use the Legal Hold module.

Note: Only a system administrator with the role management privilege can create and assign user roles.

To add legal hold user privileges

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:

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



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

Legal Hold Admin Account

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 the Legal Hold Admin role to specify the user's level of access. The predefined role (which includes the Legal Hold module) is: • **Legal Hold Admin**. Allows access to the legal hold module, for holds and notices management. To customize access privileges for this role, see *"Viewing/Editing the Legal Hold Admin Role" on page 73*. For information about defining other general user roles, refer to the *"Managing User Accounts" in the System Administration Guide*.
Access Type	Select the access type to allow the user to either access groups or cases. If "Group" is selected, then the user becomes part of an access group and gets access to all entities that are associated with that access group. A user which is part of an access group is still restricted by his/her role. If "Case" is selected, the user gets access to specific cases only. The Access Group permissions are disabled for case type users.
Access Groups	By default, all access groups are listed in the **Included** column which results in the users being added to all access groups. Keep only those groups in the **Included** column in which you want to add the user and move all the remaining groups to the **Available** column.
Account Status	Select whether the account is enabled or disabled. Disabling an account prevents users from logging in and removes the account 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	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 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).
Comments	Enter additional comments about the account.

Note: To limit access to specific cases (all cases are authorized by default), click the **Cases** tab, click **Selected Cases**, select the appropriate cases in the left column, and click to move them to the Authorized Cases list. For information on how to override the case access rights, or define new access profiles, refer to *"Managing User Accounts" in the System Administration Guide*.

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

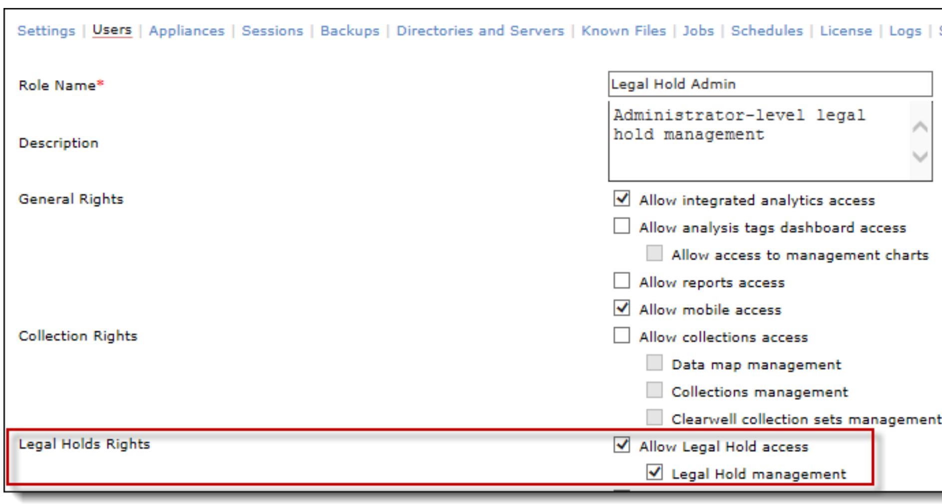
4. To change or enable/disable an account, click the account name, change the account settings, and click **Save**.

Viewing/Editing the Legal Hold Admin Role

As with other user accounts, the Legal Hold Admin role specifies a set of access permissions that can be assigned to the specified user's account. However, you can edit the role if you want to restrict administrator privileges, and only allow user read-only access to view legal holds in the Legal Hold module. (Alternatively, you can create a custom user role based on the Legal Hold Admin but, for example, restrict or allow other permissions that are, by default, not defined by the Legal Hold Admin role.

Note: You cannot edit the default user roles that are defined by the system. You can only edit the user roles that are created manually.

Only a system administrator with the role management privilege can create and assign user roles. To assign a user role to a Legal Hold Admin account, refer to *"Assign Legal Hold User Privileges" on page 70*. Among other user roles listed, the **Legal Hold Admin** role, by default, allows legal hold access and management rights.



Follow the steps in this section to define the Legal Hold Admin role by editing permissions from the Edit Role page.

To view and edit the Legal Hold Admin role

1. From the **System** view, click **Users**.
2. Click the **Roles** tab to view the list of user roles.
3. To view the Legal Hold Admin user role:

   A. Click **Legal Hold Admin**. The following information is displayed.

   Note: Only the rights that are predefined for the Legal Hold Admin role are listed here. For details, refer to the *System Administration Guide*.

Legal Hold Admin Role Details - Editing for the Legal Hold User

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	
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 Hold Rights	
Allow Legal Hold access	Allow **read-only** access to Legal Holds module.
Legal Hold management	With access to Legal Holds module, management includes creation and administration of Legal Holds, and Legal Holds notices.
System Administration 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 support, case, and user functions listed below. **Note:** If case management also is not allowed for any cases, **Case Home** is not displayed. **Note:** This privilege allows users to manage jobs and schedules for ALL cases. See *"Managing Schedules and Jobs" in the System Administration Guide*.

Populating the Employee List

The Legal Hold module uses Active Directory (or other archive source) discovery to populate your Custodian table in the Legal Hold module using employee data, called “custodians” when associated with one or more legal matters or cases in Veritas eDiscovery Platform.

To set up a periodic discovery task, see *“Schedule Discovery” on page 87*.

To update employee information, refer to the steps in *“Adding Custodians to Your Data Map” on page 75*.

Adding Custodians to Your Data Map

There are several ways to add custodians: synchronize the entire Active Directory with the Employee List, or import using a CSV or Script file. To import using CSV or script, refer to the format requirements in this section.

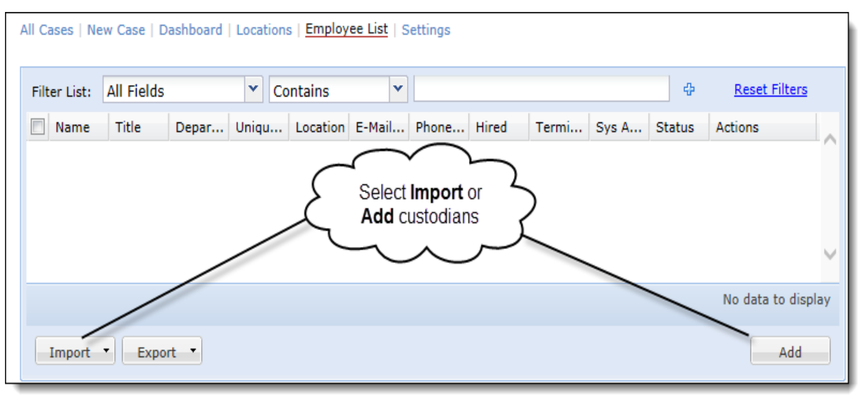
Note: Custodians in the Processing and Review (PAR) module are *not* case-sensitive. As a result, custodians in the Identification and Collection (IC) module may be merged with similar custodian names in PAR. For example, the IC custodians “joe admin”, “Joe admin”, and “Joe Admin”, who are all considered unique in IC, are treated as the same custodian in PAR. Thus, when you add a collection set (created in IC) containing the custodian “joe admin” to a PAR case that contains another custodian “Joe Admin” they are merged as one custodian. However, if that same PAR case contained no similarly-named custodians, and all three IC custodians were added to the case, they will be considered unique. In any case, to ensure your IC custodians remain unique, you can either specify custodian names with a numeric designation, or simply unmerge custodians in PAR.

Merging/Unmerging Custodians

Later, after your selected custodians have been added to a case, you can use the “Custodian Merge” feature to resolve any same-name, or similarly-named custodians (that represent the same source or individual). Alternatively, use the “Unmerge” feature to keep Collection Set custodian names unique if similarly-named (representing other individual) custodians already exist. For more information, refer to *"Merging Custodians" in the Case Administration Guide*.

To add custodians

1. From the **All Cases** view, click **Employee List**.



(Alternatively, within a case under the **Collections** module, click **Sources**, then from the **Custodian** box, click **Edit Custodians**, then **Add**. Refer to the Identification and Collection guide.

2. From the Employee List, determine if you want to:

   A. Import multiple custodians. See *“Add Custodians by Bulk Import” in the next section*.

   B. Add custodians individually. See *“Add Custodians” on page 80*.

Add Custodians by Bulk Import

To add custodians by bulk import (option A)

1. From the **Custodians** window, click **Import** and select one of the following options:

   A. Active Directory:

   › **Synchronize Now with Active Directory** (synchronize the entire Active Directory with the Employee List)

   Note: On selecting **Synchronize Now with Active Directory**, the system submits the employee synchronization job.

   B. From File (see *"Importing from CSV or Script" on page 76* for format requirements):

   › **From CSV** (enter CSV file name and path, or browse to location)

   › **From Script** (enter Script file name and path or browse to location)

   Note: You can save the CSV file anywhere in preparation for import. However, the script file must be placed only in the default folder: **`D:\customerScript\bulkImport`** for Veritas eDiscovery Platform to locate and import the file.

2. Upon discovery, click **Import All Shown**.

3. If your import was successful, all custodians you selected to add or import appear in the list of custodians. Click **Save** to associate the new custodians to the selected source, or click **Cancel** to discard your changes.

Importing from CSV or Script

The Collections Admin can automatically populate the Employee List by providing a CSV or script file which meets specific requirements for bulk import into Veritas eDiscovery Platform. Before importing your custodians, ensure your CSV file or script meets the following requirements.

Note: When importing custodians from a file, the names are added in the system similar to a processed job. To view the status of your CSV or Script file import, click the **Jobs** link at the top of the screen. If an error occurs during import, a warning icon appears next to the link. Click the book icon in the Status column to view details in the job status log.

CSV Import Format Requirements

The CSV file should be provided in the following format:

1. **Header row** - First row of the file, consisting of the column names (in any order), separated by commas. The following column names should be specified:

   Note: The * indicates required fields.

CSV Import Format Requirements

Column Name	Format	Max Limit	Example
Name	UTF-8	255	John Doe
Domain	UTF-8	255	Veritas
File owner name	UTF-8	255	John Doe
File owner SID	UTF-8	255	1122
Title	UTF-8	255	Analyst
Division	UTF-8	255	Sales
Location	UTF-8		California
Phone Number	UTF-8	No limit	555 1234567
Hired Date	MM/DD/YYYY	10	05/02/2010
Terminated Date	MM/DD/YYYY	10	08/10/2011
Email	UTF-8		John@Veritas.com johnie@Veritas.com
Primary Email	(Integer) Index	255	0 **Note:** Email with index 0 in the list of emails will be displayed as primary: John@Veritas.com
Escalation Manager Unique ID	UTF-8	255	5599
System Admin	TRUE/FALSE (FASLE by default)	5	FALSE
Unique ID	UTF-8		1133

2. **Employee Record** - Each of the following rows will be interpreted as an employee record, with each attribute separated by a comma. The number of fields in each row must match the number of columns in the header row.

   The following rules apply to attributes or columns in a CSV file for Employee List bulk import:

CSV Import Format Requirements

Attribute or Column	Rule(s)
Column names	• Case-Sensitive; (must be typed) • Can be written in any order
“Domain” Column	• (Optional) Must be present with "File owner name" column (or both columns must be absent). Cannot be individually selected. • Values must also be consistent in both columns if present (empty or populated).
“File owner name” Column	(Same rules apply as for “Domain” column.)

CSV Import Format Requirements

<table>
<tr><th>Attribute or Column</th><th>Rule(s)</th></tr>
<tr><td>Fields containing line breaks (CRLF), double quotes, and commas</td><td>Must be enclosed in double quotes. (")
If using double quotes to enclose fields, a double quote appearing inside a field must be preceded with another double quote.
Example:
“employee one”,”mc””adams”.</td></tr>
<tr><td>Adding multiple values</td><td>When adding multiple values to a field, the values should be separated by commas (,)
Example:<table><tr><th>Name</th><th>Phone Number</th><th>Unique ID</th></tr><tr><td>John Doe</td><td>"555 8901234, 5550984321"</td><td>2</td></tr></table></td></tr>
<tr><td>Unique “Domain” and “File owner name” values</td><td>Domain and File Owner Name pairs must be unique across all employees. This does not apply to records with empty Domain and File Owner Name values.</td></tr>
<tr><td>Unique IDs</td><td>If an employee entry contains the same Unique ID as another employee entry, the following rules will apply:
New employee’s “Email”, “File owner name”, “File owner SID”, and “Domain” column fields will be appended to the existing employee’s entry.
All other columns will be replaced.
Example:<table><tr><th></th><th>Name</th><th>Email</th><th>Unique ID</th></tr><tr><td>Existing entry in Employee List</td><td>John Doe</td><td>JohnDoe@JohnDoe.com</td><td>1</td></tr><tr><td>New entry from CSV</td><td>Johnnie Doey</td><td>JohnnieDoey@JohnnieDoey.com</td><td>1</td></tr><tr><td>Resulting entry</td><td>Johnnie Doey</td><td>JohnDoe@JohnDoe.com, JohnnieDoey@JohnnieDoey.com</td><td>1</td></tr></table></td></tr>
</table>

Script Import Requirements

An asterisk (*) indicates a required field.

Script Import File Format Requirements

Column Name	Format	Max Limit	Example
Name*	UTF-8	255	John Doe
Domain	UTF-8	255	Veritas
File owner name	UTF-8	255	John Doe

Script Import File Format Requirements (Continued)

Column Name	Format	Max Limit	Example
File owner SID	UTF-8	255	1122
Title	UTF-8	255	Analyst
Division	UTF-8	255	Sales
Location	UTF-8		California
Phone Number	UTF-8	No limit	555 1234567
Hired Date	MM/DD/YYYY	10	05/02/2010
Terminated Date	MM/DD/YYYY	10	08/10/2011
Email	UTF-8		John@Veritas.com johnie@Veritas.com
Primary Email	(Integer) Index	255	0 **Note:** Email with index 0 in the list of emails will be displayed as primary: John@Veritas.com
Escalation Manager Unique ID	UTF-8	255	5599
System Admin	TRUE/FALSE (FASLE by default)	5	FALSE
Unique ID*	UTF-8		1133

Script File Format and Location

All CSV formatting requirements also apply to those used for bulk import. However, to ensure security while running executable (.exe) files, all scripts must be stored in the folder: "D:\customerScript\bulkImport". Appliance users should ensure that access to this folder is restricted to authorized users to protect against security threats to the system.

Note: Unless the file is an executable (.exe), then it should contain the location of the executable used to run it (as shown in the first line of the following example).

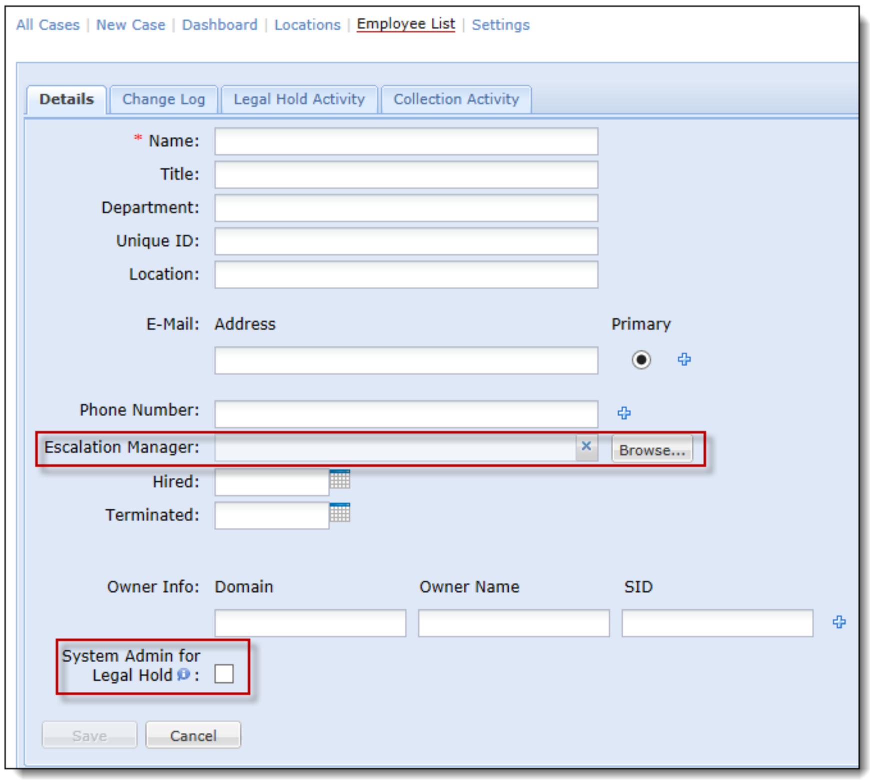
Example script:

```
#!c:\Perl\bin\perl.exe

print "Name,Email,Unique ID\n";

print "John Doe,JohnDoe\@johnDoe.com,1122\n";

print "Johnnie Doey,JohnnieDoey\@johnnieDoey.com,1122";
```

Add Custodians

To add a custodian individually (option B)

1. From the **All Cases** > **Employee List** window, click **Add**.



Note: The bottom section will be visible only if your enterprise has a Legal Holds module license installed, and the logged on user must have appropriate permissions.

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

Adding a Custodian

Field	Description
Name*	Enter the name of the custodian (up to 35 characters). The name is not case sensitive.
Title	Enter the custodian's title (if applicable).
Department	Enter the custodian's division or department (if applicable).
Unique ID	Enter an identification number or code unique to this custodian.
Location	Enter a location.

Adding a Custodian

Field	Description
E-Mail	Enter the custodian's email account. (Example: jsmith@acmemail.com). By default, the icon is selected to indicate that this is the primary address. Click the icon to add additional addresses for this custodian.
Phone Number	Enter a phone number for the custodian. Click the icon to add additional phone numbers for this custodian.
Escalation Manager (Legal Hold users only)	Enter or browse for the name of this custodian's manager to whom legal hold notifications should be escalated.
Hired / Terminated	Enter the date of hire and termination, or click the calendar icon to select a date.
Owner Info. (Domain, Owner Name, SID)	Enter the Domain name, owner name, and the Security Identifier. **Note:** The owner name will only be collected (when filtering for collection) if the Windows user for the collection is running as the source account (or *EsaApplicationService* user if there is no account on the source), and it is in the domain where the owner name is kept.
System Admin for Legal Hold (Legal Hold users only)	Select this check box if this custodian's role is a System Administrator, for use in customizing Legal Hold notifications.
Legal Hold History (Legal Hold users only)	Displays summary of Legal Hold activity associated with this custodian. (Includes names of Legal Holds and Notifications, and date notifications were last sent.)

3. Click **Save** to associate the new custodian to the selected source, or click **Cancel** to discard your changes.
4. Click **Close** to close the Custodians window.

Performing Backups

To ensure your legal hold notification information is preserved, and the custodian data associated with your holds is saved, Veritas recommends performing a full node backup either on-demand, or scheduled to run periodically. You can also perform a Legal Hold and Collections backup. When a Legal Hold and Collections backup is performed, the system is automatically backed up (and recommended). If necessary, this allows administrators to restore the Legal Hold data from the last run backup. Legal Holds and Collections Backups should not be used for portability across appliances. For portability of Legal Hold and Collections backups, a full node backup should be used.

Note: If you encounter issues, or your confirmation server must be restored from a backup, see *"Troubleshooting Backup/Restore for Legal Hold" on page 85*.

Full Node/Appliance Backups

To perform a full node (appliance) backup, refer to the section *"Backup and Restore" in the System Administration Guide*.

Note: Veritas recommends performing a full node backup before any other backups.

Run an On-Demand Backup

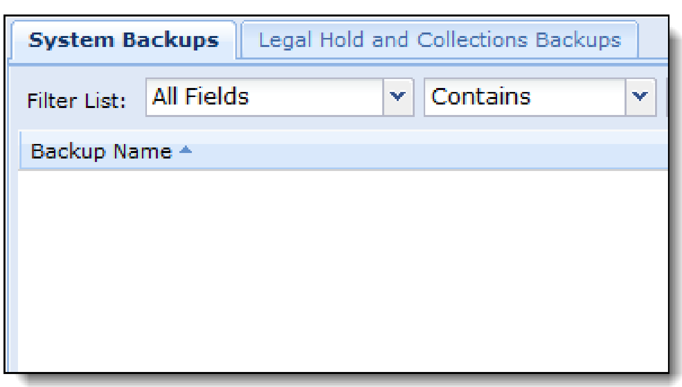
On-demand backups are a convenient way to save data should your data become unusable or source data unavailable. It is typical to perform an on-demand backup after new data (and before data collection or the case management workflow begins).

Note: You must perform a backup of the Administration server first, then run one on the Legal Hold Confirmation server (using the steps in this section), in this order. (When restoring data, this order is reversed.) See *"About Restoring Legal Hold Data" on page 84*.

To back up legal holds on demand

Before you begin: Verify that no one is currently accessing the Legal Hold module. To back up your system, you must have the System Manager role with collection management permissions (for Legal Hold).
Best Practice: Do not use Legal Holds and Collections Backups for portability across appliances. For portability of Legal Hold and Collections backups, be sure to use a full node backup.

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



The Backups page displays, open to the **System Backups** tab, showing any backups previously performed.

2. Click the **Legal Hold and Collections Backups** tab.
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 Veritas eDiscovery Platform system will not be available during a system backup. Veritas eDiscovery 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 system backup depends on the size of all holds 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.

Schedule a Backup

Scheduled system backups help you maintain a set of up-to-date backups on all legal hold data.

Note: When scheduling a backup for legal hold, be sure to back up the Administration server first, then the Legal Hold Confirmation server (using the steps in this section), in this order.

Each scheduled backup overwrites the most recent backup with the same backup name. If you need to preserve multiple copies of a system 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 backup

Before you begin: To schedule a backup, you must have the System Manager role with collection management permissions (for legal hold).

1. From the **System** view, click **Schedules**.
2. At the bottom of the Schedule pane, click **Add.**

3. On the Add Schedule page, 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 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 data backup, choose either all, or selected cases that you want to backup.

   Note: If the backup name is changed after setting up a backup schedule, the new name is automatically added to the schedule, and the data 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 backup.

    Best Practice: Only use alphanumeric characters in backup names.

    Note: The Veritas eDiscovery Platform system will not be available during a system backup. Veritas delays user-performed operations that impact the system until the backup completes.
11. Click **Save**. The new 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 system backup schedule

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

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

About Restoring Legal Hold Data

In the event that legal hold data must be restored, perform the restore in the reverse order of backup. Thus, restore data on the Legal Hold Confirmation server first, then on the Administration server. Repeat these steps for either on-demand, scheduled, or full node backups.

Troubleshooting Backup/Restore for Legal Hold

If any issues occur while attempting to back up or restore your legal hold data on the server, or if the Legal Hold Confirmation server and the Administration server are not in sync, or if you want to use a different confirmation server, you must clear the Legal Hold Confirmation server information.

Clearing the Confirmation Server

There are two cases when clearing the Confirmation server is necessary. 1) If the state of legal holds and notices on the Administration server are not in sync with the Legal Hold Confirmation server. 2) If you want to switch your setup (use another server as your Legal Hold Confirmation server). If you want to use a new server, see the setup instructions in *"Option A: Separate Server Setup" on page 98* in the Appendix. Once complete, return to the steps in this section to perform backups on the Legal Hold Confirmation server you set up.

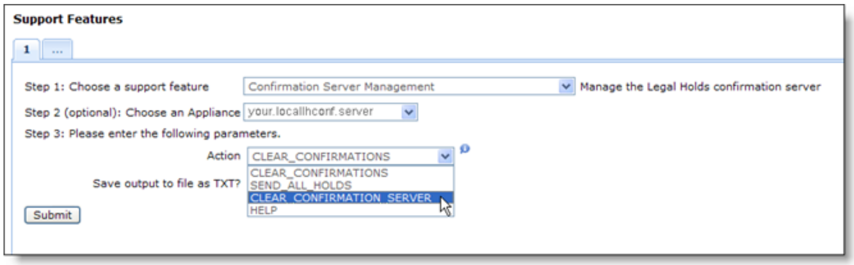
The **Confirmation Server Management** feature includes three support features:

- **CLEAR_CONFIRMATIONS**: This feature is used to clean up already processed confirmation packages. After a response is confirmed, it creates a package in the Confirmation Server database and marks it as unprocessed. The Administration server periodically queries the Confirmation Server for unprocessed packages, retrieves and processes them, and then marks them as processed on the Confirmation Server. These previously processed packages never get cleaned up, and depending on the age and volume of legal hold usage, it can start to slow down the Confirmation Server. This feature can be used to clean up these packages and restore performance.
- **CLEAR_CONFIRMATION_SERVER**: This feature completely wipes the Confirmation Server database. After running this feature, all previous links in the legal hold notices are invalid until the data is repopulated by using the SEND_ALL_HOLDS feature. This feature is most often used when moving or replacing a Confirmation Server or troubleshooting inconsistent data on a Confirmation Server. This feature is always followed by the SEND_ALL_HOLDS feature.
- **SEND_ALL_HOLDS**: This feature sends all legal hold packages to the Confirmation Server to repopulate the database. This feature is commonly used to ensure consistent data on the Confirmation Server after clearing the Confirmation Server or after moving or replacing a Confirmation Server.

Note: The "CLEAR_CONFIRMATIONS" and "CLEAR_CONFIRMATION_SERVER" support features target the database of the appliance the support feature is being run on. If a separate Confirmation Server is used and if you run these features from the Administration server, then these features do not target the database of the separate Confirmation Server. In this case, you must log on to the separate Confirmation Server and then run these features there.
The "SEND_ALL_HOLDS" feature repopulates all the hold data on the Confirmation Server irrespective of whether the Confirmation Server resides on the Administration server or on a separate server.

To clear the Confirmation Server

1. Go to **System > Support Features**, and select the **Confirmation Server Management** feature.

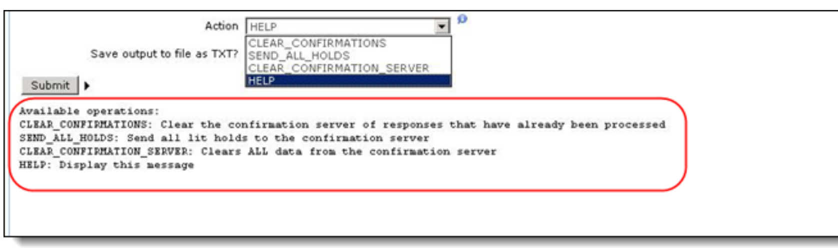


2. From the Actions drop-down menu, select **CLEAR_CONFIRMATION_SERVER**, and click **Submit**.

3. After clearing the confirmation server, return to the Confirmation Server Management support feature and select the **SEND_ALL_HOLDS** action, then click **Submit**.

4. [As needed]: Select the **CLEAR_CONFIRMATIONS** action, then click **Submit**.

   Note: Veritas recommends performing this action periodically, or when necessary to clear the confirmation response queue.



   Note: For more information about the appropriate actions to take, from the Action drop-down menu, select **HELP**.

For all other backup/restore information, refer to the section *"Backup and Restore" in the System Administration Guide*.

Schedule Discovery

As employee data changes, your list of custodians from your initial Active Directory (or other archive source) discovery may be affected. Periodically, you may want to schedule updates to ensure you are using the latest available custodian data for your legal holds. You can also schedule a bulk custodian or bulk source import (to occur once, daily, or weekly).

To schedule Discovery

Before you begin: To perform a discovery, you must have the Collection Admin role with applicable administrative 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 a task type (Example: **Active Directory Discovery**).
4. Set the Initial Run Date, and Start Time.
5. Choose whether discovery should be run once, daily, or weekly.
6. Click **Save**.

Archiving, Restoring, and Deleting Legal Holds

Occasionally, you may want to remove old legal holds from view that are no longer necessary, such as when a case containing a legal hold has expired, or when any related collections are no longer active. Alternatively, you may simply want to release custodians and/or reduce the custodian license count, thus increase your quota by archiving inactive holds. Collection Admins can archive legal holds in an effort to manage hold data and optimize license capacity.

Archiving versus Deleting Legal Holds

Whether archiving or deleting a legal hold, both remove the hold from active view or use, but only archived holds can be restored or recovered at a later date. Whether archiving or deleting a legal hold, either action releases associated custodian licenses (if they are unique in the system), allowing you to reuse the custodian licenses for other holds.

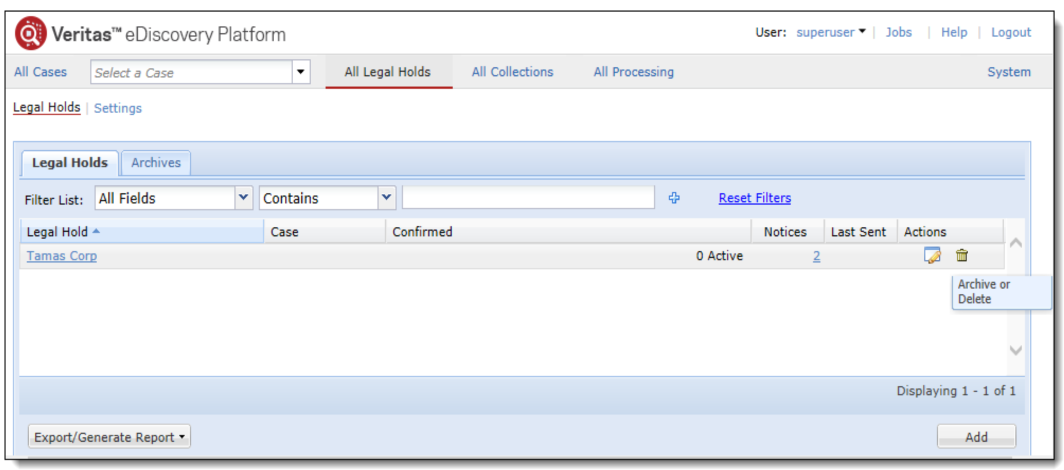
When a legal hold is deleted, its contents (notices) are removed from Veritas eDiscovery Platform. The data itself is not actually deleted or moved, but cannot be recovered from its current location. (The default destination for the selected legal hold's data is provided. For example: D:\CaseData.)

Note: Veritas does not recommend deleting a legal hold unless you are certain the data is no longer needed. While the information is not permanently deleted, it cannot be restored in the same way as an archived hold, and may require assistance from Technical Support to recover the data.

To archive or delete a legal hold

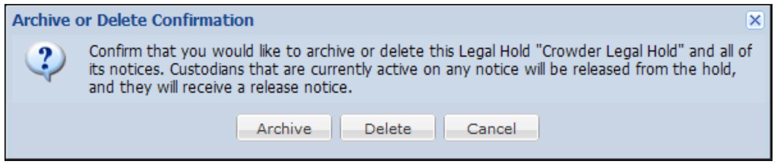
1. From the **System** view, click **All Legal Holds**.

   The Legal Holds screen appears showing all legal holds across all cases.



2. Click the (archive or delete) icon under the Action column for the legal hold you select.

3. A warning appears with the option of either archiving or deleting the selected legal hold.



Confirm your action:

A. To remove the legal hold (which can be restored later), and release one or more associated custodians, click **Archive**.

   Note: Any custodians still active in this legal hold will be released from the hold and will receive a release notice. The custodian license is released only if the custodian is unique in the system, and not associated with any other active holds.

B. To remove the legal hold (including its notices, which will not be permanently deleted or moved, but cannot be restored), and release custodian licenses, click **Delete**.

   CAUTION: Consider your action carefully before deleting a legal hold. Even though the data is not permanently deleted or moved, and is still in the system, it is not easily readily recoverable, and may require Technical Support’s assistance.

Your archived legal hold now appears on the **Archives** tab, from where it can later be restored. The associated custodians are no longer counted against your custodian license. Further, any active custodians contained in the hold are now released.

To check your custodian license count, go to **System > License** to view the number of custodian licenses in use. You may need to click **Update License** to view the new (increased) total. See *“Managing Your Legal Holds License” on page 91*.

Restoring an Archived Legal Hold

Archived legal holds can be restored from the "**Archives**" tab. The legal hold you select will be listed among your active Legal Holds.

Note: You must have administrator-level privileges to restore archived legal holds.

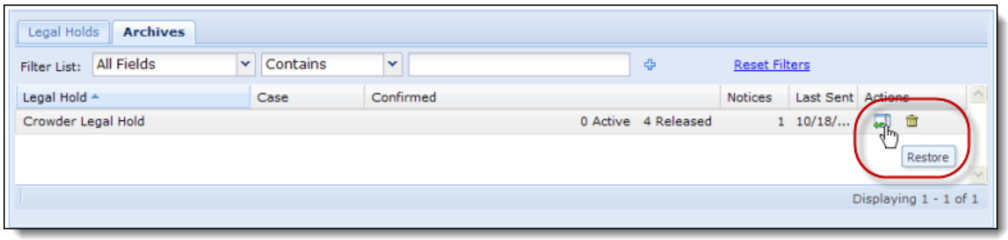
The custodians associated with the legal holds you restore will be counted against your license. Once restored, the holds still show the number of custodians as 0, leaving the license number unchanged. Even after a hold is restored, you cannot add new custodians to the existing notices contained in the hold. To resend the same hold, you must first create new custodian and/or system admin notices.

Restoring a Legal Hold from a Backup

When restoring a legal hold from a backup, any custodians who were previously released after the backup will remain as active custodians on hold once again. However, after restore, a reminder notice is not automatically sent to the custodians who were back on legal hold. If you want to send a reminder notice to previously released custodians alerting them they are back on hold, you must manually send (or schedule) the reminder notice. See *“Sending Reminders or Escalations” on page 46*.

To restore an archived legal hold

1. From the **System** view, click **All Legal Holds**.
2. On the Legal Holds screen, click the **Archives** tab.
3. Click the  (restore) icon for the selected legal hold you want to archive.



4. At the prompt, click **Yes, Restore** to continue with restoring the selected legal hold.

Your legal hold is now restored, and reappears on the **Legal Holds** tab, where it is available for active use. The custodians do not count toward your custodian license even after the restore while they are still in the released state. Only when new notices with custodians are added and the hold is resent will the custodian license count against the total number of licenses available.

To check, go to **System > License** to view the reduced number of custodian licenses in use. You may need to click **Update License** to view the new total. See *"Managing Your Legal Holds License" on page 91*.

Managing Your Legal Holds License

Your Legal Holds license key is supplied by Veritas Technical Support based on the terms of your license agreement. For new appliances, or for more information about your general Veritas license, refer to the *"Managing Your License" in the -System Administration Guide*.

About Reusable Licenses

The custodian license becomes reusable in two cases: (1) If the custodian was released from a legal hold, and was not assigned to any other active holds, and (2) if the custodian was associated with a hold which was archived (thus released from the hold), and is not associated with any other active holds. (In this case, the custodian is sent a notice of release. Upon restoring the hold, the same custodian, if involved in the matter, must be sent a new legal hold notice.)

Updating Your License

Use the License screen to view the license information and to update your Legal Holds license. On the associated Detail screen, you can view how much of your licensed capacity each case currently uses. The Legal Holds license is based on a per-custodian use. Updating your license requires license information either to be pasted using the Ctrl+v keys, or uploaded from a .zip or SLF file. Have this information handy before you choose to update.

To view or update license information

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

   Note: Custodian licenses for Legal Holds are reusable. When custodians are released from a legal hold notice, the custodian count becomes available again for re-use.

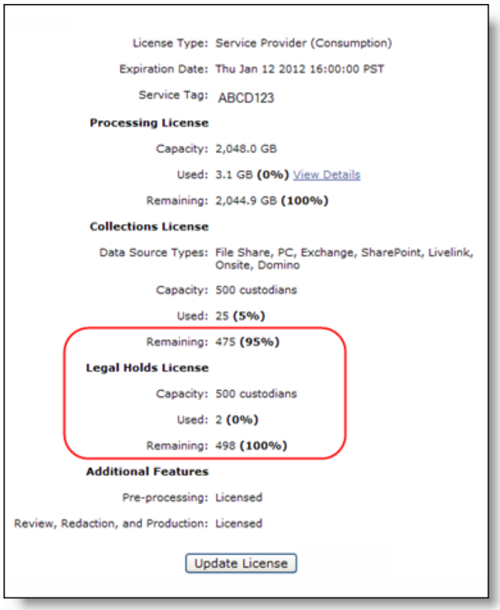
   In this example, the current consumption is for 500 custodians. Periodically note this count, particularly each time you release a custodian from a legal hold.

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.

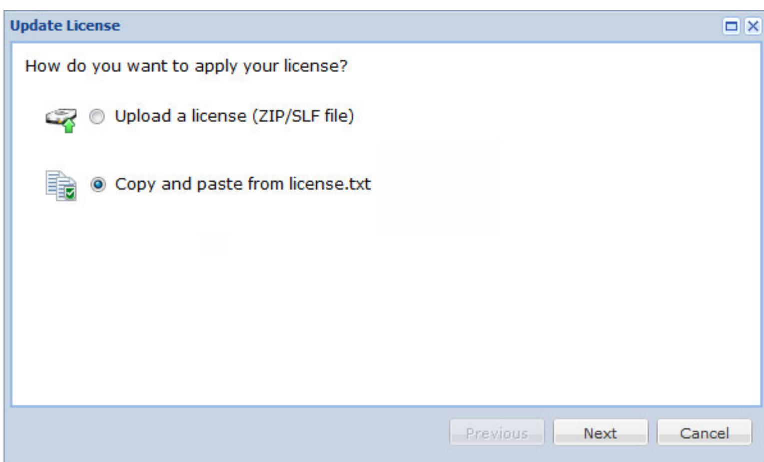
3. To update the license, click **Update License**.



The Update License Wizard opens.

4. Select the method you want to use to update your license. Copying/pasting a file will *replace* the license information with the new license on the server where it is installed. Uploading a file will add to your existing license.

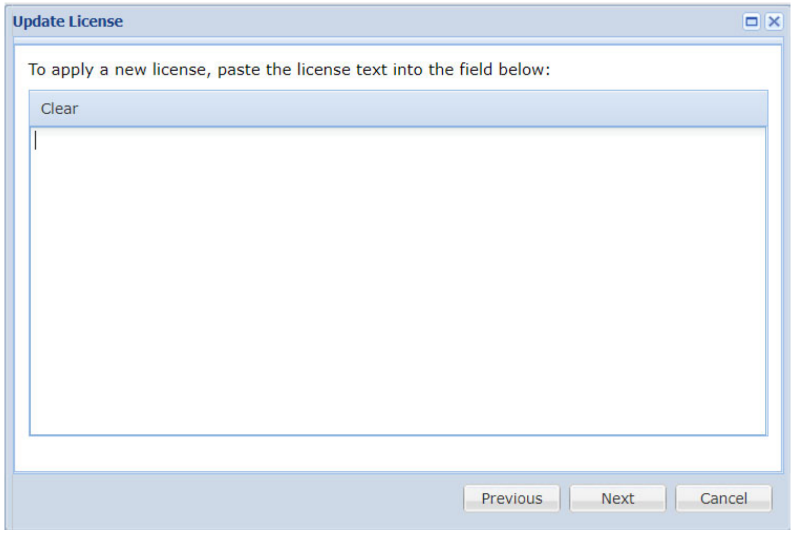
   (As shown in this example, you can choose to copy and paste the license information, "license.txt" file, attached in an email message you received.)



   Click **Next**.

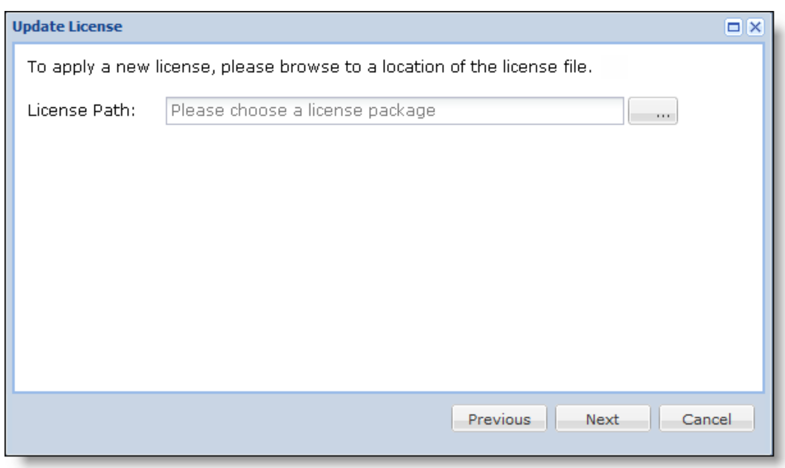
5. Do one of the following:

   A. If copying/pasting the license information, press Ctrl+V to the place the copied text into the window. (Click **Clear** to delete.)

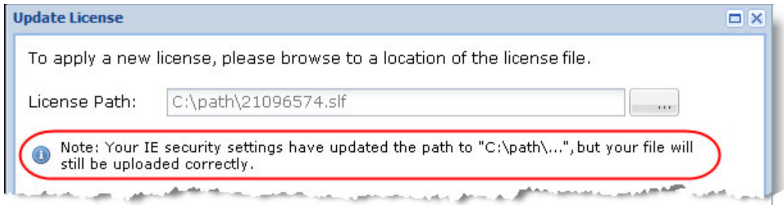


Note: Depending on your browser's security settings, pressing Ctrl+V may prompt you to allow access to the System Clipboard. Clicking "**Allow access**" is safe and will stay in effect until the page is refreshed again.

   B. If uploading a license (from a ZIP or SLF file), browse to the location of the license package.



Note that when you select the path, your browser security settings are updated to that location, though your license file will still be properly uploaded.

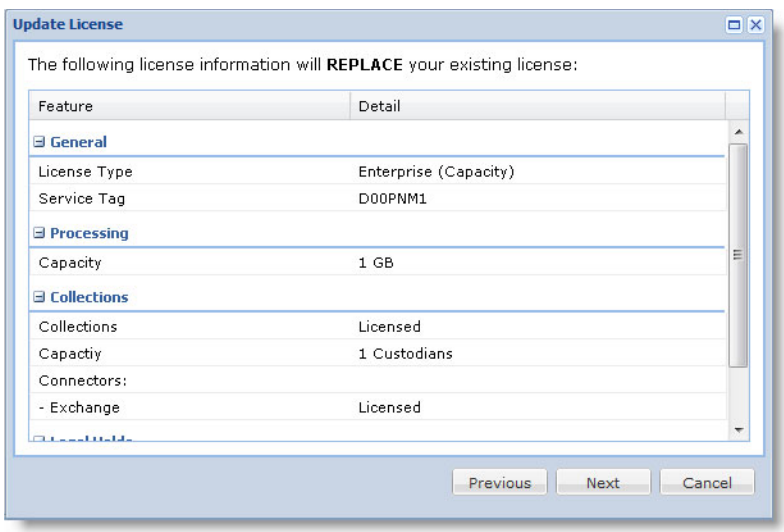


Note: Uploading a file will *add/merge* the license information with the current license on the server where it is installed.

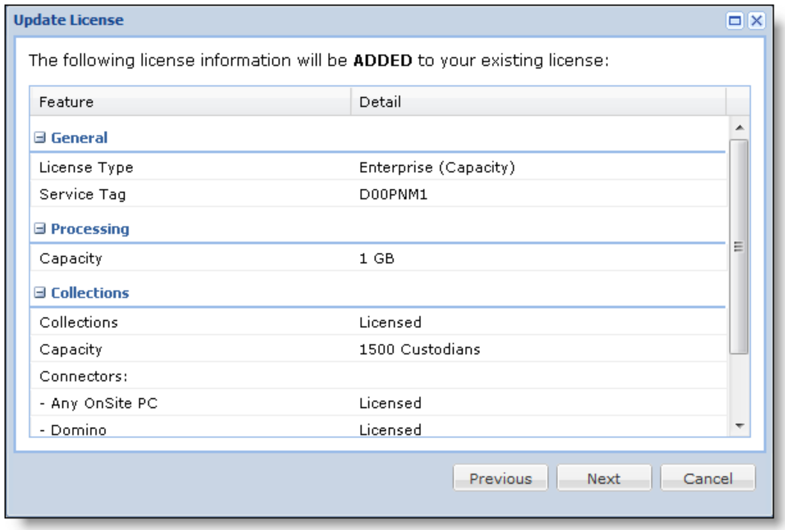
Click **Next**.

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

   A. If you copy/pasted in your license (you received a license.txt file via email), note that the information, as shown, will *replace* your existing license:

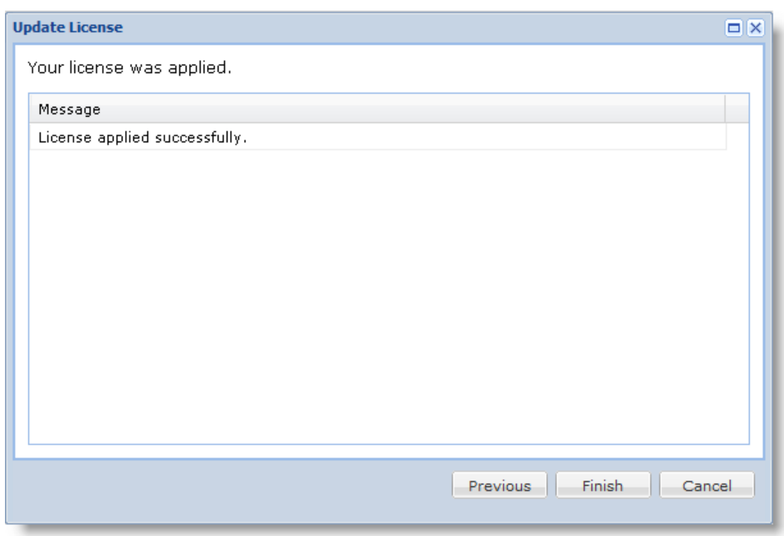


B. If you uploaded your license (from a ZIP or SLF file), note that the information, as shown, will be *added to* your existing license:



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.



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

Appendix A: Setup Requirements

This information is intended for system administrators tasked with setting up and enabling the Veritas eDiscovery Platform environment to send and receive notifications in response to a legal hold.

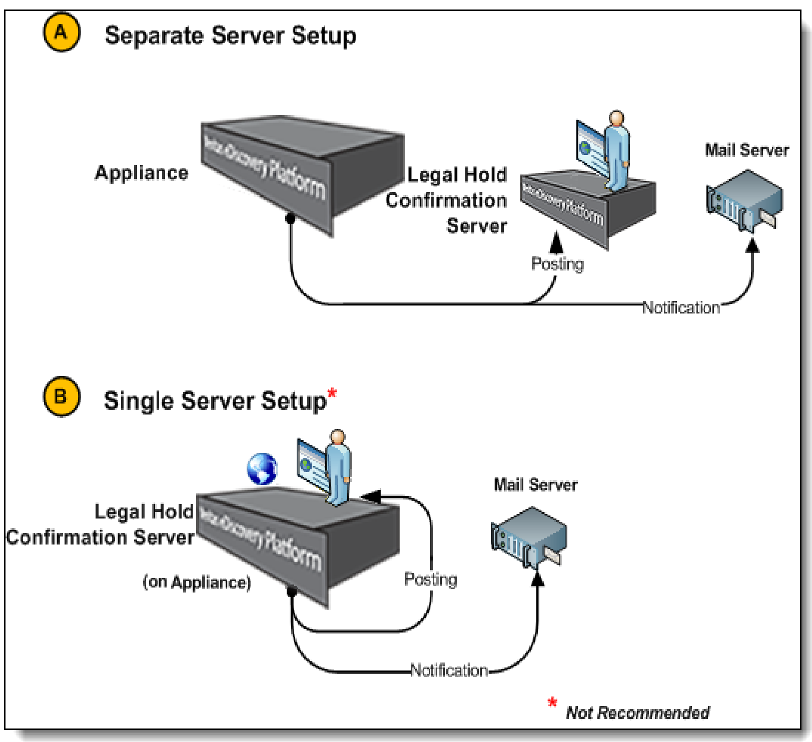
The following sections in this Appendix outline the basic requirements for ensuring your appliance is set up for use with the Legal Hold module:

- *"Determine Your Setup" in the next section*
- *"Setup Checklist" on page 98*

Depending on your setup, follow the checklist to ensure you have properly designated and configured a *Legal Hold Confirmation Serve*r for custodian use to view and respond to hold notifications.

Determine Your Setup

There are two possible ways to setup your Legal Hold Confirmation Server: Separate Sever Setup or Single Server Setup.



While you can use your admin server as your Legal Hold Confirmation server, best practice is to use a separate server (Option A).

Note: To maintain proper load balancing and a secure legal hold environment, Veritas strongly recommends that a server other than the Admin server be designated as a confirmation server. Determine the type of confirmation server setup before installing or configuring the eDiscovery Platform system for Legal Hold. If a separate confirmation server setup is required or anticipated based on scale growth in the future, the separation of the confirmation server from the Admin server must be done before creating the Legal Hold notices in the eDiscovery Platform system.

Setup Checklist

Follow these steps to set up and configure your Legal Hold server ("Confirmation Server") for your chosen setup, before you begin sending Legal Hold notices.

- *"Option A: Separate Server Setup" in the next section*
  - *"Step 1: Install Legal Hold Confirmation Server" on page 98*
  - *"Step 2: Verify your Server Setup" on page 100*
  - *"Step 3: Validate HTTP protocol" on page 101*
  - *"Step 4: Configure custom certificates (Optional)" on page 101*
  - *"Step 5: Restart Services" on page 101*
- *"Option B: Single Server Setup" on page 102*
  - *"Step 1: Install Veritas eDiscovery Platform and Set Server Properties" on page 102*
  - *"Step 2: Configure System Settings" on page 103*
  - *"Step 3: Restart Services" on page 103*

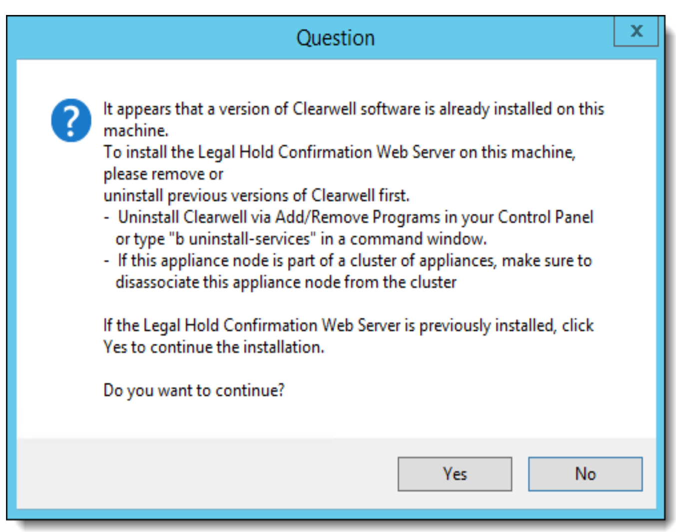
Option A: Separate Server Setup

Perform the following steps to install and run the confirmation server, and then verify your setup. Make sure that you have read the *"Determine Your Setup" on page 97*.

Step 1: Install Legal Hold Confirmation Server

To run the Legal Hold Confirmation Server installer and install the server

1. Locate and open the Confirmation Server installer file on your system.
2. When the installer opens, the Confirmation Server welcome page appears, prompting you to start the install. Click **Next**.
3. If you have an older version of eDiscovery Platform already installed on your system, you must uninstall previous versions first. Follow the instructions on the dialog, then click **Yes**.



Click **Next** to continue.

Note: If you are upgrading your Confirmation server to release 9.0, you get an option to keep the existing security certificate. This option should only be selected if you are using a third party certificate.

4. On the Choose Destination Location page, enter or click **Browse** to find the location where you want to install the Confirmation Server. Click **Next** to continue.

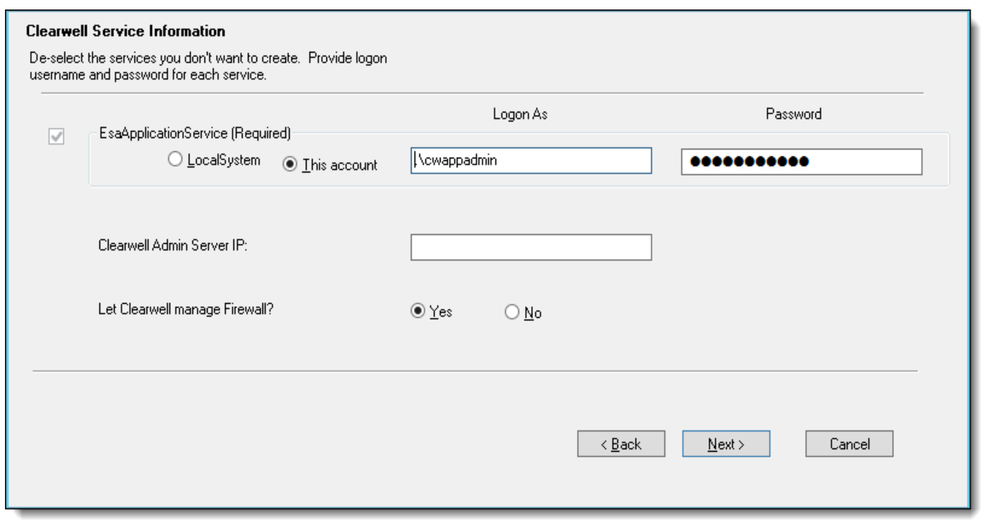
5. On the Setup Type page, select **Complete**. Click **Next** to continue.

6. On the Select Features page, be sure Veritas eDiscovery Platform is selected.

   Note: Features that are not selected may already be installed on your system. Otherwise, do not clear any other features unless you have been instructed to do so.

   Storage space requirements are shown at the bottom, with the amount of available space on your system. Click **Next** to continue.

7. Enter your Veritas eDiscovery Platform service information. The *EsaApplicationService* is required. By default, "This account" is selected. Type your logon username and password, then enter your Admin Server IP address. (Later, this appears in your settings to verify the address.)



   By default, Veritas will manage the firewall for this setup. Click **Next** to continue.

8. To complete your installation, click **Next** to start copying the necessary program files to the Confirmation Server.

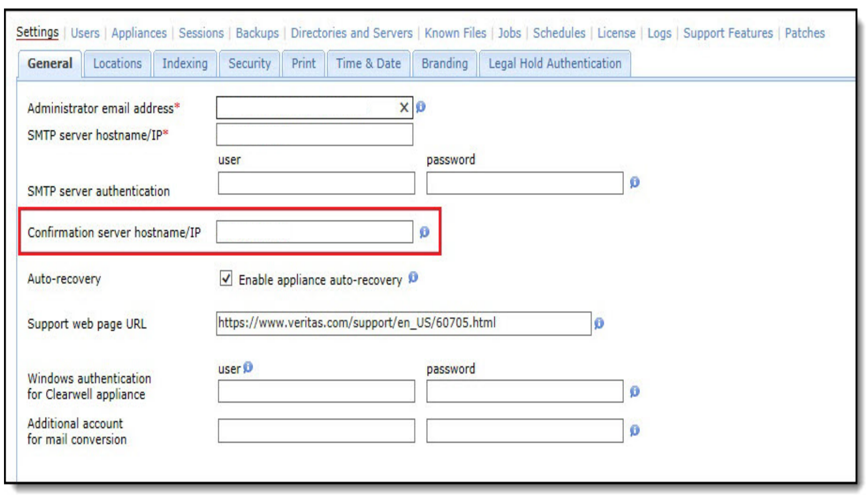
9. Your installation is complete. Select to view the install log files, and/or open your browser to log on to the Confirmation Server. (The location of the log file is shown at the bottom.) Click **Finish**.

Step 2: Verify your Server Setup

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].

To verify your Legal Hold Confirmation Server hostname/IP address

1. After the Confirmation Server is setup, log on to your main Veritas eDiscovery Platform administrative appliance.
2. Under the **System** tab, select **Settings**.
3. Under the **General** tab, check that the correct hostname/IP address is entered for the Legal Hold Confirmation Server.

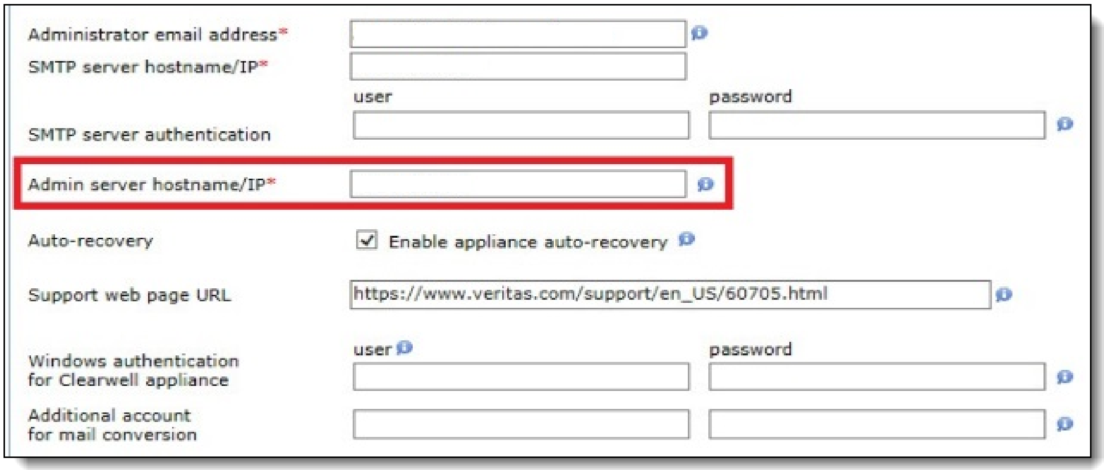


Note: Ensure that you have entered the fully-qualified domain name.

4. Click **Save**.

To verify your Admin Server hostname/IP address

1. After installing Veritas eDiscovery Platform on the confirmation server appliance, log on to your Confirmation Server appliance.
2. Under the **System** tab, select **Settings**.
3. Under the **General** tab, check that the correct hostname/IP address is entered for Admin Server.



Note: Ensure that you have entered the fully-qualified domain name.

4. Click **Save**.

Step 3: Validate HTTP protocol

1. From **System** > **Support Features** > **Property Browser** support feature, type the following property name to change (Case-sensitive), and then set its value to **FALSE**.

   esa.icp.confirmation.webservices.useHttps

   Note: The admin server and the external confirmation server must use a common protocol, either HTTP or HTTPS. If the admin server uses HTTPS, then you must set the value of the ***esa.icp.confirmation.webservices.useHttps*** property to "**TRUE**" so that the URL in the notification email will use HTTPS. When the admin server and the confirmation server use different protocols, then the URL in the notification email displays an error message for an invalid link.

2. Select both check box options to confirm your changes, and then click **Submit**. You will need to restart the *EsaApplicationService* for your changes to take effect. See the next step.

Step 4: Configure custom certificates (Optional)

If you need to use either a Clearwell Commander-generated certificate or a provider-generated certificate, then you need to perform the steps described in the *Certificates* section in the *System Administration Guide 9.0* on both Admin server appliance and the confirmation server appliance.

Step 5: Restart Services

For your configuration settings to take effect, you must restart the *EsaApplicationServer* from your Windows environment.

Option B: Single Server Setup

Veritas provides a Confirmation Server installer, which sets these properties for you. However, if you have a single confirmation server setup (in which the administration server is also your confirmation server), you must follow these steps to ensure that your server is set with both the administration server hostname/IP, and the confirmation server hostname/IP.

Step 1: Install Veritas eDiscovery Platform and Set Server Properties

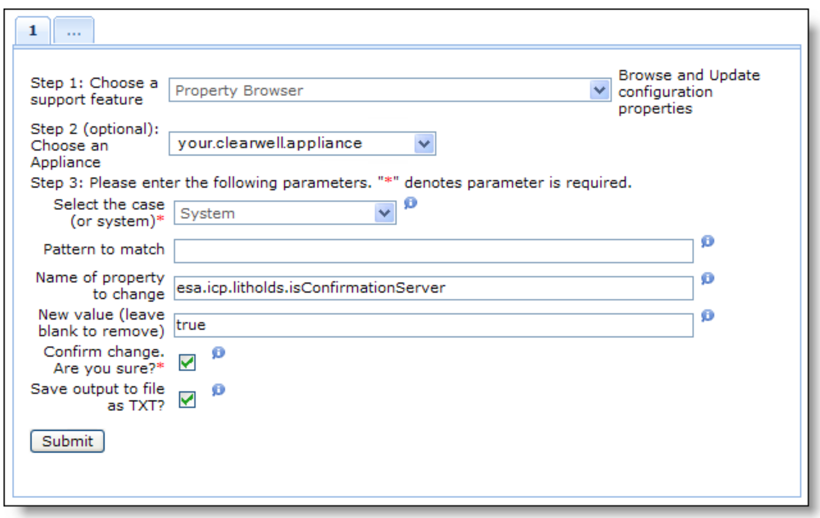
Note: You will only need to modify properties if you are setting up a single Legal Hold Confirmation Server (that is, the administration server and confirmation server are the same server).

To install Veritas eDiscovery Platform and set Legal Hold Confirmation Server properties:

1. Refer to the *Veritas eDiscovery Platform Installation Checklist*, then follow the installation instructions in the *Veritas eDiscovery Platform Installation Guide*.

2. In the Veritas eDiscovery Platform user interface, click **System** and select **Support Features**.

3. On the Support Features screen, select the **Property Browser** support feature, then select an appliance.



4. For the Name of property to change, type the following property. (Case-sensitive):
   `esa.icp.litholds.isConfirmationServer`

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

   TIP: If a property is entered with the incorrect case, it must be removed first, then set again using the correct case.

5. For the New Value, type:
   `true`

6. Select both check box options to confirm your changes, and to save your settings to a text output file.

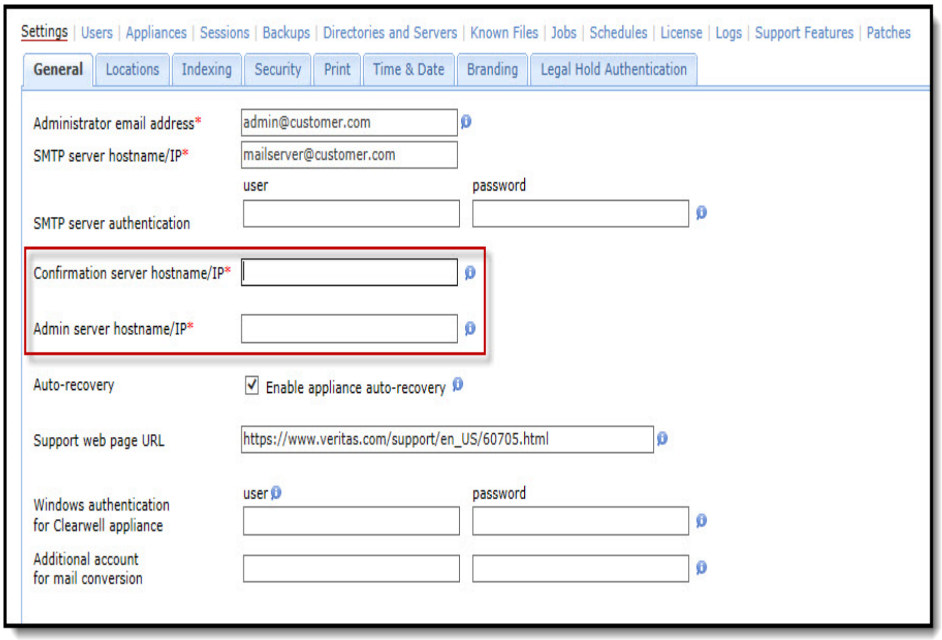
7. Click **Submit**. You will need to restart the *EsaApplicationService* for your changes to take effect. (See *"Step 3: Restart Services" on page 103*.)

Step 2: Configure System Settings

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].

To set the Admin Server Hostname:

1. In **System**, select **Settings**.



2. Under the **General** tab, type your administrator email and mail server host addresses.
3. Type your Confirmation server hostname/IP address. (For this setup type, the administration server hostname is same as the Confirmation server hostname).
4. Enter any usernames and passwords to be used for mail server and Windows authentication.
5. Click **Save**.

Step 3: Restart Services

For your configuration settings to take effect, you must restart the *EsaApplicationServer* from your Windows environment.

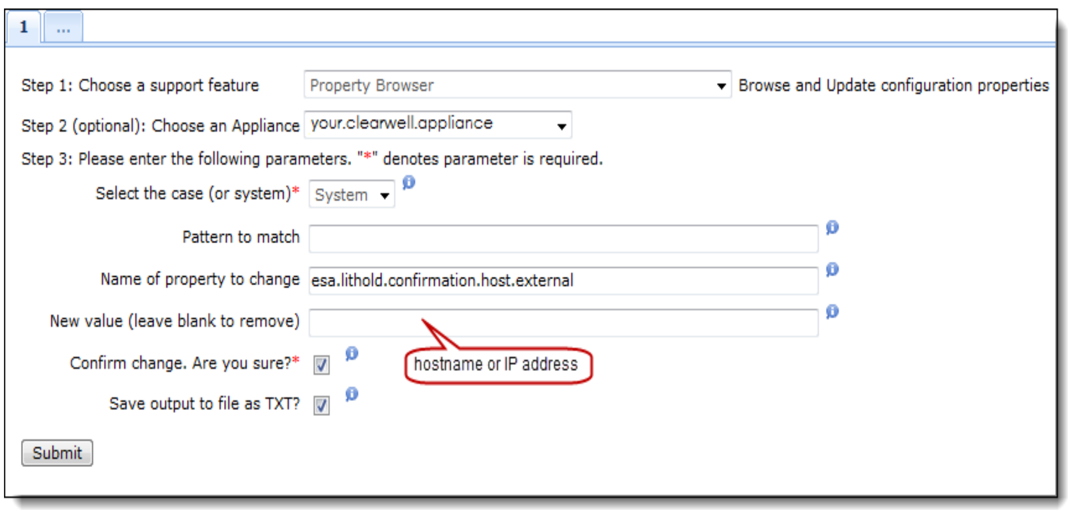
Additional setup requirements

Using an external IP address for the confirmation link

Veritas eDiscovery Platform now supports the ability to use an external IP address and an internal IP address for the same appliance. You can use the external IP address for the confirmation server link in the notification and communicate with the internal IP address using the **esa.lithold.confirmation.host.external** property. The URL in the notification email will use the external IP address instead of the confirmation server hostname.

To set an external IP address for the confirmation link:

1. In the Veritas eDiscovery Platform user interface, click **System** and select **Support Features**.
2. On the **Support Features** screen, select the **Property Browser** support feature, then select an appliance.



3. For the Name of property to change, type the following property. (Case-sensitive): **esa.lithold.confirmation.host.external**
4. For the New Value, type the Hostname or IP address that you want to use for the confirmation link.
5. Select both check box options to confirm your changes, and to save your settings to a text output file.
6. Click **Submit**. You will need to restart the *EsaApplicationService* for your changes to take effect.

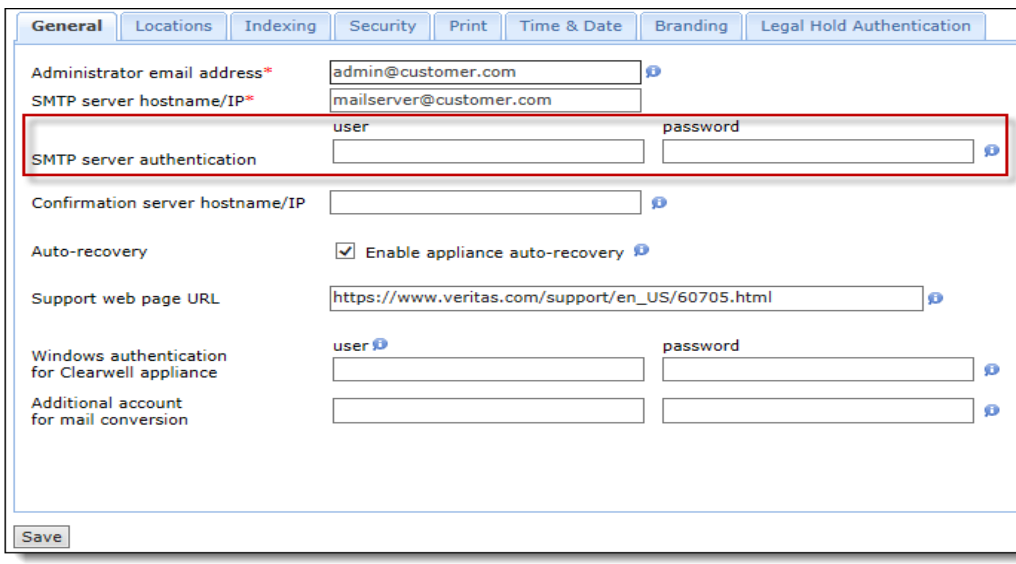
Setting up SMTP server for Legal Hold

If you use Exchange 2010 or later, you should not provide username and password for SMTP server authentication. Keep these credentials blank and enable anonymous logon on your Exchange SMTP server to be able to send Legal Hold notices.

If you use Exchange 2007 server, you should be able to send Legal Hold notices irrespective of whether username and password is provided or not for SMTP authentication.

To configure SMTP server authentication:

1. Under the **System** tab, select **Settings**.
2. Click the **General** tab to view the settings.



3. For SMTP server authentication, do one of the following depending on the Exchanger server you use.
   - For Exchange 2010 or later server, keep the user and password fields blank with anonymous logon enabled on your Exchange SMTP server.
   - For Exchange 2007 server, either enter the user and password credentials or keep these fields blank.
4. Click **Save**.

Appendix B: Product Documentation

The table below 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
User Guide	Describes how to perform searches, analysis, and review, including detailed information and syntax examples for performing advanced searches

Veritas eDiscovery Platform Documentation

Document	Comments
Imaging Tool Upgrade Guide	Provides details about the Imaging Tool Upgrade feature and how to perform Imaging Tool Upgrade after the eDiscovery Platform appliance is upgraded to version 10.1, workflows affected when the cases are upgraded or not upgraded, and frequently asked questions (FAQs).
Export and Production Guide	Describes how to use and produce exports, productions, and logs (privilege and redaction logs)
Transparent Predictive Coding User Guide	Describes how to use the 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