Introduction to Enterprise Vault.cloud™

Administration Console

Introduction to Enterprise Vault.cloud™ Administration Console

Last updated: 2020-04-23

Legal Notice

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

Veritas Technologies LLC

2625 Augustine Drive

Santa Clara, CA 95054

http://www.Veritas.com

Table of contents

Overview

This document is intended for AdvisorMail customers transitioning to Veritas Advanced Supervision. This document provides a summary of some of the new management functions that you can access in Enterprise Vault.cloud.

Introduction

With your transition from AdvisorMail to Veritas Advanced Supervision, your organization benefits from powerful new features that were previously only available to the Enterprise Vault.cloud^{TM} customers. Advanced Supervision is now a part of the Enterprise Vault.cloud (EV.cloud) archiving platform. This transition offers you access to Enterprise Vault.cloud's Administration Console - commonly referred to as Manage.

Veritas recommends you refer to the EV.cloud user guides, Help documentation, and release notes, available at http://evcnews.veritas.com.

About EV.cloud Administration Console

The Administration Console is a web-hosted interface that enables administrators to configure and manage Enterprise Vault.cloud. The Administration Console lets administrators perform the following tasks:

- Configure account management for the company.
- Add/Edit account details.
- Enable access to services.
- Assign roles to users to administrate and manage the company.
- Configure how users can access services.
- Set Trusted Networks.
- View Reports and Notifications.

Configuring the account management

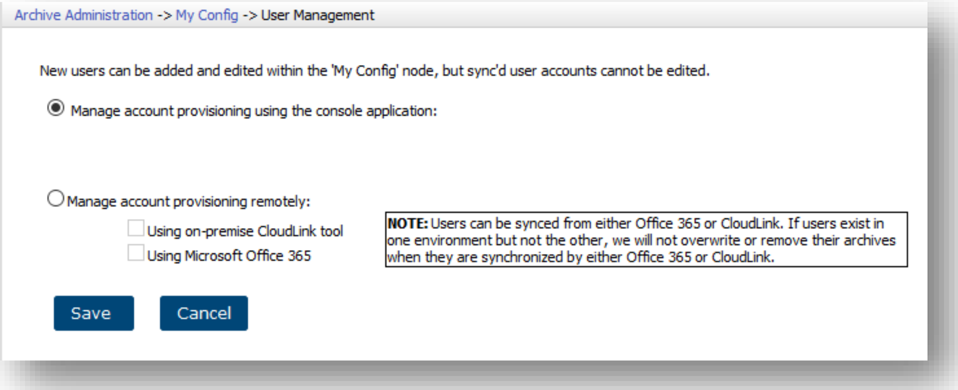
Your existing accounts from AdvisorMail will be migrated to EV.cloud. However, any new employee joining the company need to be manually created or synched[1] . The User Management section provides the ability to select how to provision users with the following options:

- Manual provisioning option: Provision users using the Administration Console.
- Automatic provisioning options:
  - Using on-premise CloudLink: This option lets you use the separately installable CloudLink tool to manage the provisioning of Microsoft Active Directory users in Enterprise Vault.cloud (including Advanced Supervision users).
  - Using Microsoft Office 365 Sync: This option provides automatic provisioning for Microsoft Office 365 accounts. It is a section within Manage that synchronizes from Office 365 into Enterprise Vault.cloud (including Advanced Supervision users).

Provisioning accounts

To select how to provision accounts:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **My Config**, click **User Management**.
3. On the **User Management** page, select one of the following provisioning options:
   - Manage account provisioning using the console application
   - Manage account provisioning remotely



Archive Administration -> My Config -> User Management

New users can be added and edited within the 'My Config' node, but sync'd user accounts cannot be edited.

● Manage account provisioning using the console application:

○ Manage account provisioning remotely:

□ Using on-premise CloudLink tool

□ Using Microsoft Office 365

NOTE: Users can be synced from either Office 365 or CloudLink. If users exist in one environment but not the other, we will not overwrite or remove their archives when they are synchronized by either Office 365 or CloudLink.

4. If you selected the option to manage account provisioning remotely, select **Using on-premise CloudLink tool**, or **Using Microsoft Office 365**, or both.
5. Click **Save**.

[1] Please refer to the EV.cloud Archive Administration Guide for additional information on selecting EV.cloud user management options - CloudLink and Office 365 Sync.

Adding and editing accounts

The Account Management section of the Administration Console lets you update the account details. However, if accounts are provisioned using any of the sync tools, some details might be read-only.

Adding a new account

To add a new account:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **My Config**, click **Account Management**.
3. At the top of the **Account Management** page, click **Archives** and then click **New Archive**. The **Archive Detail** form is displayed.
4. Enter the required details for the accounts, such as:
   - Email Address, First and Last Name, User Name, and Password
   - Select the proper Status options
   - Select the services that you want to enable for the archive account
   - Enter an alias email addresses that you want to associate with the archive account
5. Click **Save**.

   Note: After the account is saved, the History panel displays a summary of the most recent changes.

Editing an existing account

To edit an existing account:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **My Config**, click **Account Management**.
3. In the accounts list, click the archive account to display the details of the account. The Archive Detail form is displayed.
4. To edit the details, at the bottom-right of the account details page, click **Edit**.
5. Update the account details, such as:
   - Email Address, First and Last Name, User Name, and Password
   - Select the proper Status options
   - Activate/Deactivate Services Access
   - Add/Remove Aliases

     Note: Primary alias cannot be deleted.
6. Click **Save**.

   Note: After the account changes are saved, the History panel displays a summary of the most recent changes.

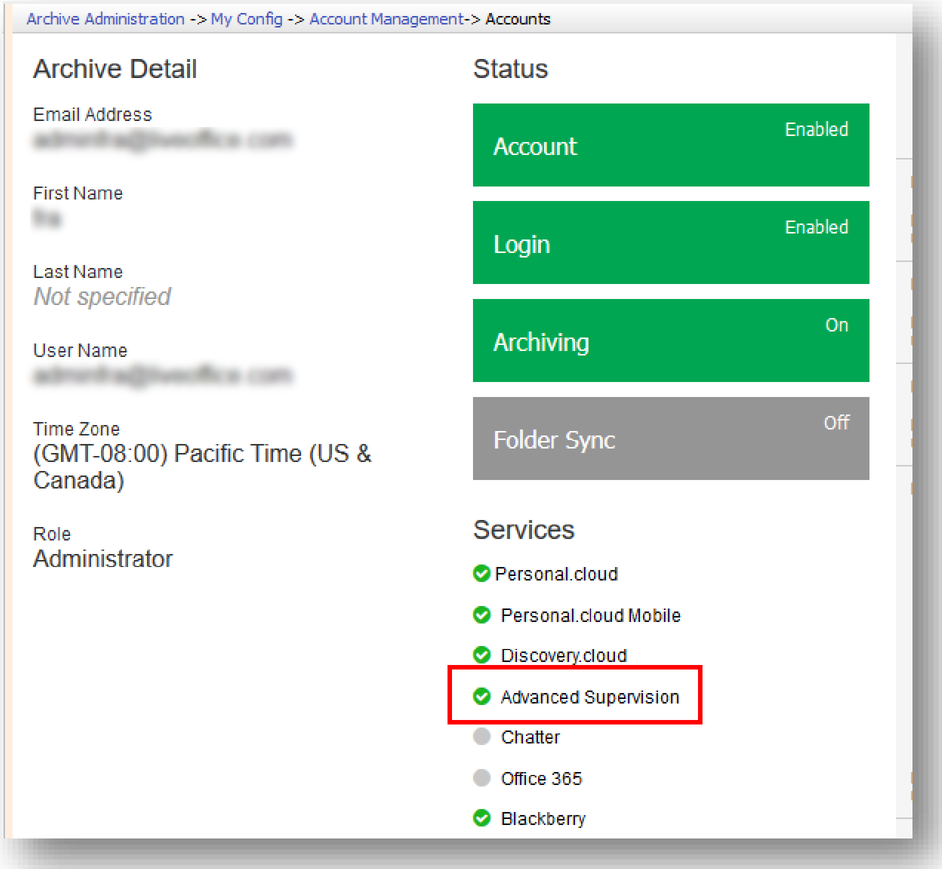
Managing access to Advanced Supervision

Your existing accounts from AdvisorMail will be migrated to EV.cloud while retaining your existing access and permissions. However, you will have the option to enable or remove access to Advanced Supervision, if required. Only the users who are granted access to Advanced Supervision from Administration Console (Manage) can be added as reviewers or administrators within Advanced Supervision.

Enabling or disabling the access to Advanced Supervision

To enable or disable the access:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **My Config**, click **Account Management**.
3. Select the account you want to grant access to Advanced Supervision.
4. After the account details are displayed, click **Edit**.



Archive Administration -> My Config -> Account Management-> Accounts

Archive Detail

Email Address
[redacted]

First Name
[redacted]

Last Name
Not specified

User Name
[redacted]

Time Zone
(GMT-08:00) Pacific Time (US & Canada)

Role
Administrator

Status

Account	Enabled
Login	Enabled
Archiving	On
Folder Sync	Off

Services

- ✓ Personal.cloud
- ✓ Personal.cloud Mobile
- ✓ Discovery.cloud
- ✓ Advanced Supervision
- ○ Chatter
- ○ Office 365
- ✓ Blackberry

5. Under the **Services** section, select or clear the **Advanced Supervision** option as required.
6. Click **Save**.

This action allows the user to grant or revoke access to Advanced Supervision, either as Administrator or as Reviewer within a Department; however, it does not remove the application or department permissions.

Assigning administrative roles

Administrative roles allow you to change a user role from Account to Reviewer or Administrator. Administrators synched to Advanced Supervision get assigned the System Admin role, which allows them to manage compliance rules. A role must be assigned to be able to manage the company.

Roles allow the user to manage different sections within the Administration Console. Each built-in role has privileges to allow the user to configure specific areas. Additionally, the administrator can also create custom roles for added customization.

Following are the built-in roles that can be assigned to accounts:

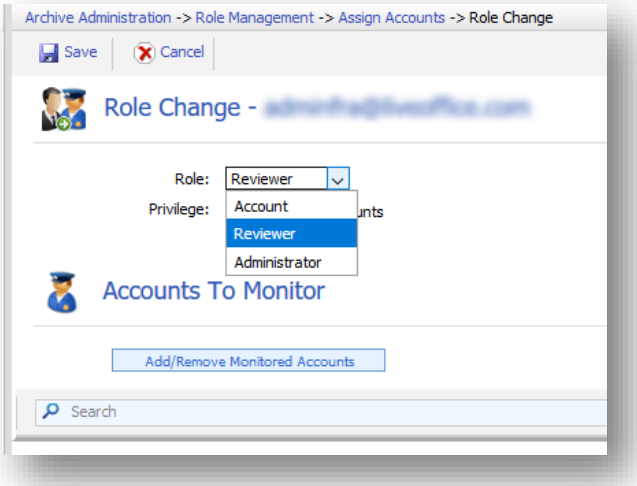
Built-in Role	Description
Account Manager	Manage users, aliases, settings, and password.
Role Manager	Configure administrator roles and permissions for archive account.
Policy Manager	Specify archiving options and settings.
Retention Manager	Specify archive retention policies and settings.
Continuity Manager	Manage email continuity feature (only available if your organization subscribes to email continuity service).
Discovery Administrator	Configure and manage Enterprise Vault Discovery.cloud usage.
System Administrator	Manage and configure all sections within Archive Administration. This role has all permissions.
Archive Collectors Manager	Configure and manage archiving from the third-party content sources.
Classification Administrator	Configure and manage classifications tags.

Assigning user's role

To assign user's role:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **Role Management**, click **Assign Accounts**.
3. Search for the account to be updated, then click the account row to view the account details. The Role change form is displayed.

4. In the **Role** field, select **Administrator**.


Archive Administration -> Role Management -> Assign Accounts -> Role Change
Save
Cancel
Accounts To Monitor
Add/Remove Monitored Accounts
Search

Role Change - [redacted]

Role: Reviewer

Privilege: Account | Reviewer | Administrator ...unts

5. Optional: If required, select **Monitor All Accounts** to let the selected account view the archived messages of all other archive accounts.

   Note: This option is only available if your organization subscribes to Enterprise Vault Discovery.cloud. Administrators can monitor all accounts in Discovery.cloud. An administrator can grant access to a reviewer to monitor either all accounts or a subset in Discovery.cloud.

6. Select the built-in roles or custom roles to assign.
7. Click **Save**.

Setting up Password Policies and Single Sign-On

Password Policies or Single Sign-On helps to enforce your organization's specific security parameters in terms of how your users sign into applications.

Setting up a password policy

To set up a strong password policy:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **Policy Management**, click **Password Policy**.
3. In the **Password Policy** section, under **Advanced Password Policy**, select the requirements you want to include in your password policy.

   Note: The **Password Policy** page will be visible only if Authentication Management is set to **Cloud Archive Database**.
4. If required, select **Enforce the password policies for all users** if you want to require all users to change their passwords during their next login.

   Note: If you select this option, all users must change their password during their next login even if the password meets the specified requirements. If you do not select this option, users do not have to change their password until it expires even if the password does not meet the specified requirements.
5. Click **Save**.

Setting up Single Sign-On authentication

To set up Single Sign-On Authentication:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **Policy Management**, click **Authentication Management**.
3. In the **Authentication Type** field of the **Setup Authentication** section, select **Single Sign-On ADFS** or **Single Sign-On SAML 2.0**.
4. Select **I have read the instructions for setting the provided Entity ID and created my public key for upload** after you review the provided instructions.
5. In the **Upload Your Public Key** section, click **Browse and Upload**.
6. In the window that displays, navigate to the file location of the token-signing certificate that you generated.

   Note: The token-signing certificate that you upload must have a *.cer* file extension.
7. In the **Public Key Upload** confirmation window, click **Return to Setup** to proceed to the next step.
8. In the **Validate Relying Trust** section, enter the Identity Provider URL for your organization in the **Identity Provider URL** field.
9. Click **Validate**.
10. After the **Validation Successful** message displays, click **Save** to proceed to the next step.
11. In the **Activate SSO** section, click **Activate SSO**.
12. After the **Activation Successful** message displays, you will be able to sign in using the Customer ID associated within your configuration. You only need to append the CID that is displayed to the Advanced Supervision URL provided to you: *https://ThisIsAdvancesSupervisionURL?CID= XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX*

Setting up trusted networks

By default, users can access Enterprise Vault.cloud from any Internet Protocol (IP) address. From the **Set Trusted Networks** page, you can restrict access to specific address ranges. For example, if you want your employees to access EV.cloud from their office network only, you can restrict the IP address to just your office network.

Configuring trusted networks

To configure trusted networks:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **Policy Management**, click **Set Trusted Networks**.
3. In the **Starting** field, enter the starting IP address of the address range.
4. In the **Ending** field, enter the ending IP address of the address range.
5. Select the check box for the Enterprise Vault.cloud products that you want access restricted.

   Note: Selecting **Manage** restricts access to the Archive Administration and selecting Discovery/Personal restricts access to Discovery.cloud and Personal.cloud. This feature is not supported for Advanced Supervision.
6. To add the address range restriction, click **Add**.
7. Click **Save**.

Note: After you add an address range restriction, click **Edit** to make changes or **Delete** to remove the restriction.

Viewing reports

From the Reports and Notifications section, you can access the logs and reports that provide information about your organization's Enterprise Vault.cloud usage. Additionally, you can export the logs and reports in various file formats.

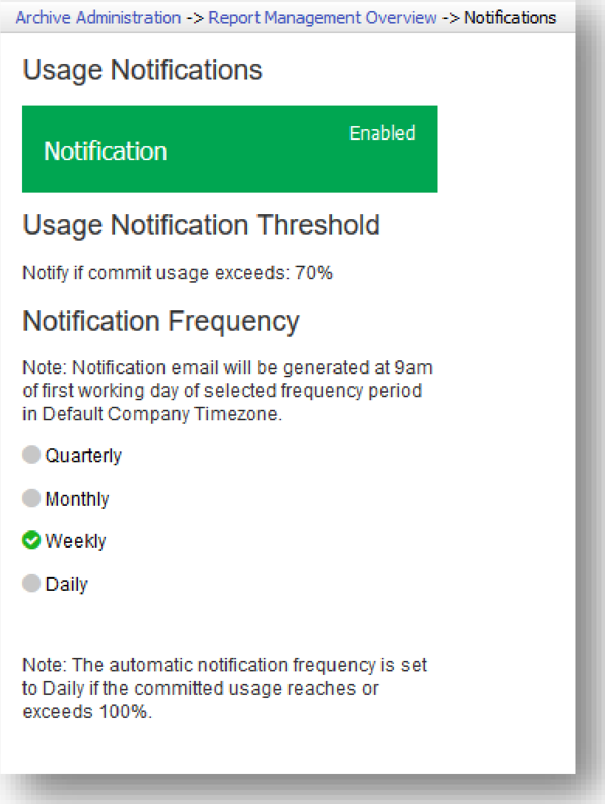
Reports that are available in each section are listed below:

- **Logs**
    - **Activity Log** - The Activity Log displays all events that occur in Enterprise Vault.cloud including user logins, password resets, and user role changes. From the **Activity Log** page, you can view the full log or filter the log by date range, user name, events, or event details.
    - **Message Log** - The Message Log displays information about the archived messages in Enterprise Vault.cloud. From the **Message Log** page, you can view the full log or filter the log by date range, message sender, message recipient, or subject.
    - **Usage Log** - The Usage Log displays information about Enterprise Vault.cloud usage, such as number of messages that have been archived, average size of messages or the total storage in use.
    - **Retention Log** - A Retention Log Report displays usage information for retention policies. From the **Retention Log** page, you can create a report with the full log. You can also filter the log by date range, user name, action type, or policy name.
    - **Mobile Browser Log** - The Mobile Browser Log displays information about Enterprise Vault.cloud Mobile Web Access usage. From the **Mobile Browser Log** tab, you can view the full log or filter the log by date range. If your organization has purchased Personal.cloud, refer to this report.
    - **Personal Browser Log** - The Personal Browser Log displays information about Enterprise Vault Personal.cloud usage. From the **Personal Browser Log** tab, you can view the full log or filter the log by date range. If your organization has purchased Personal.cloud, refer to this report.
    - **Discovery Browser Log** - The Discovery Browser Log displays information about Enterprise Vault Discovery.cloud usage. From the **Discovery Browser Log** tab, you can view the full log or filter the log by the date range.
- **Reports**
    - **Messaging Reports** - The Messaging Report displays information about Enterprise Vault.cloud usage based on certain parameters, such as message size, number of messages by user, attachment size, search speed, and email imported.
    - **Personal Archive Report** - The Personal Archive report displays information about Personal.cloud usage based on certain parameters, such as user logins, tags created, tags applied, search performed, search speed, and search string. If your organization has purchased Personal.cloud, refer to this report.
    - **Mobile Web Access** - The Mobile Web Access report displays information about usage based on certain parameters, such as, user logins, search performed, and search strings. If your organization has purchased Personal.cloud, refer to this report.

To generate a report, navigate to the corresponding section in the left navigation pane of Archive Administration, and then introduce the parameters or wait for the report to load.

Seting up usage notifications

With usage notifications, you can send emails to selected people when a certain percentage of committed usage is exceeded. By default, emails are sent when 80 percent of committed usage is reached. You can change the percentage at which emails are sent and the frequency of notification emails. The notification frequency options are quarterly, monthly, weekly, and daily. The default frequency is weekly.



Archive Administration -> Report Management Overview -> Notifications

Usage Notifications

Notification Enabled

Usage Notification Threshold

Notify if commit usage exceeds: 70%

Notification Frequency

Note: Notification email will be generated at 9am of first working day of selected frequency period in Default Company Timezone.

○ Quarterly

○ Monthly

✓ Weekly

○ Daily

Note: The automatic notification frequency is set to Daily if the committed usage reaches or exceeds 100%.

Enabling or disabling usage notifications

To enable or disable usage notifications:

1. Sign in to Manage.
2. In the left navigation pane of Archive Administration, under **Reports and Notifications**, click **Notifications**.

   The **Notifications** option appears only if you are logged in with a System Administrator role.
3. Click **Edit**.
4. Under **Usage Notifications**, click **Enabled** or **Disabled**.

   Note: If you disable notifications, the notification threshold and frequency are reset to the default settings.
5. Under **Usage Notification Threshold**, in the **Notify if committed usage exceeds** option, select a new percentage.
6. Under **Notification Frequency**, select the interval you want to use.
7. Under **Notification Emails**, type an email address, and then click **Add** or click **X** next to each email address that you want to remove.
8. Click **Save**.