Veritas Data Insight Self-Service Portal Help

6.1.4

March 2019

VERITAS™

Veritas Data Insight Self-Service Portal Help

6.1.4.0

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

.

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

Contents

Chapter 1

Overview

This chapter includes the following topics:

About the Self-Service Portal

Data Insight enables you to monitor the data on Network Attached Storage (NAS) and helps you to identify the data owner of files and folders based on the access history. It lets you carry out forensics in the form of various pre-canned and custom reports.

Data Insight also lets you manually tag users in your organization as being responsible for the resources in your storage environment. Such users are called custodians and are responsible for remediating these resources.

Data Insight integrates with Data Loss Prevention (DLP) to help security administrators and the information security teams in your organization to monitor and report on access to sensitive information. A Data Insight lookup plug-in retrieves information from the DLP Enforce Server about confidential information on the shares being monitored by Data Insight. DLP creates an incident for every file that violates configured DLP policies. The DLP Network Discover incident report lists such file system shares. The usage information that Data Insight collects automatically feeds into the incident detail of files that violate DLP policies. Data Insight identifies the data owners to notify about these incidents. This method enables users to identify sensitive data along with the responsible users to enable more efficient remediation and data management.

Data Insight also enables you to review permissions on files and folders and remediate excessive permissions. Analyzing the permissions on resources ensures that only users with the business need have access to the data.

Thus, Data Insight supports large-scale business owner-driven remediation processes and workflows. You can create workflows from the Data Insight

Management Console, and submit these workflows for further action by selected custodians or configured data owners.

The Self-Service Portal provides you an interface to complete the remediation workflows. When you submit a workflow from the Data Insight console, on the start date of the workflow an email is sent to the custodians of the selected resources. The email includes a link to the Self-Service Portal. The custodians can then do the following tasks on the portal:

- Launch the portal using the link in the email, and log in to the portal with their Active Directory credentials.
- View the resources that need to be remediated.
- Apply configured actions on the resources that are assigned to them.
- Submit the requests for execution to the DLP Enforce Server, Enterprise Vault server, or the Data Insight Management Server, depending on the type of workflow request.

The files on which an action is submitted no longer appear on the portal. The summary of the total files awaiting remediation is also updated to show the number of remaining files. You can view the number of submitted files and the files on which an action is pending at the top-right corner of the page.

If you fail to take action on the paths that are submitted for your attention within the stipulated time, the workflow is canceled.

The Self-Service Portal is available beginning Veritas Data Insight version 4.5. You can use the portal for remediating incidents beginning Symantec Data Loss Prevention version 12.5.

Chapter 2

Using the Self-Service Portal

This chapter includes the following topics:

What you can do with the Self-Service Portal

Table 2-1 describes the tasks that custodians and data owners can accomplish using the Self-Service Portal.

Table 2-1 What you can do with the Self-Service Portal

Task	Description
Entitlement Review	Review the user permissions on the resources that the custodians own, attest to the permissions, or suggest changes to the permissions. See "Using the Self-Service Portal to review user entitlements" on page 9.

Table 2-1 What you can do with the Self-Service Portal *(continued)*

Task	Description
Remediate Data Loss Prevention (DLP) incidents	Data Insight uses DLP FlexResponse plug-ins to fetch incidents on sensitive paths on the NAS devices that Data Insight monitors. Security administrators create workflows to distribute incidents to custodians for the purpose of remediation. The custodians or data owners receive email alerts to remediate the resources that violate configured DLP policies. The custodians can then log in to the portal, view sensitive paths that are assigned to them and the policies that these files violate, and take configured actions on the incidents assigned to them Once the custodians submit the request for remediation, the DLP engine executes the request, and sends a response back to the Data Insight Management Console. **Note:** Data Insight does not let you create an incident remediation workflow for sensitive paths that are imported into Data Insight using a CSV file because the workflow requires information about the DLP incident ID and severity for a path that violates a policy. See "Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents" on page 11.
Confirm ownership of resources	Custodians are assigned the data resources that they own for the purpose of remediation from the Data Insight console. The Ownership Confirmation workflow enables custodians to verify that they indeed own the resources. Custodians can view the list of resources they own, and confirm or decline the ownership of these resources from the Self-Service Portal. See "Using the Self-Service Portal to confirm ownership of resources" on page 12.
Classify files for retention based on the policies that they violate	The Records Classification workflow enables custodians to mark as files that violate certain policies as a record. The policies may be defined in DLP or can be imported in to Data Insight using a `.csv` file. The files that are marked as Record are automatically processed for archiving, if automatic action is enabled when creating the workflow. The number of years for which a file is archived depends on the retention category applied to the file. See "Using the Self-Service Portal to classify sensitive data" on page 13.

Logging in to the Self-Service Portal

Custodians log in to the Self-Service Portal using the link in the email alert that they receive when a remediation workflow is submitted by a Data Insight or Data Loss Prevention administrator.

The link to the portal is valid only as long as paths in the workflow request are pending action by the custodians or until the end date specified in the workflow. Note that custodians cannot use the same link to log in to the portal after a workflow is complete, is cancelled for any reason, or if the custodian has taken action on all assigned paths.

In some cases, the Data Insight administrator or a Data Insight Workflow Administrator may log in as custodians to the portal on your behalf. You will receive a notification alerting you that a Data Insight administrator has logged in to a workflow that is assigned to you. You can disable further notifications for a particular workflow. However, you will continue to receive reminder notifications for other workflows that are assigned you.

To log in to the Self-Service Portal

1. Click the link contained in the email alert.

   The portal login page appears. The **Username** field is pre-populated with the your network username.

2. Enter your network password, and click **Login**.

3. When you log in to the portal, you may be presented with a welcome message if it is so configured for the workflow.

   On the message, click **OK** to continue with remediation actions on paths submitted for your attention.

Using the Self-Service Portal to review user entitlements

You can use the Self-Service Portal to review user access permissions to the paths that are assigned to you. On the **Entitlement Review** page of the portal, you can perform the following tasks:

- View a snapshot of the users whose permissions are assigned for your review.
- Review if the user has the creator owner permissions on a path.
  If the option to display the creator owner is selected in the workflow template, the **Creator Owner** column is displayed on the Portal UI with value as 'Yes' against user who is creator owner.

Note that if the Creator Owner is a group, no value is displayed in the **Creator Owner** column.

- Filter the users to be reviewed based on their activity profiles and the assigned paths. For example, you might be interested to first review the entitlements for the users who are inactive.
- Make recommendation to grant or revoke user permissions on the specified paths.
- Decline the review request or delegate the review work to another user.

To review user entitlements

1. Use the **Resources** drop-down to select the path for which you want to review the user permissions. From the drop-down list click the path for which you want to review user entitlements. All the review requests for the selected path are displayed on the panel.
2. Use the **Users by activity** filter to sort the users based on their activity profiles.

   You can further filter the users by selecting the group they belong to or by using their directory service attribute.
3. Do any of the following:
   - To review the permissions of individual users, click **Yes** to grant access to the path, and click **No** to revoke the user's access on the path
   - To review the permissions for multiple users, select the users based on the action you want to take. For example, select the users whose permissions you want to revoke on the selected path.
     Click either **Allow access** or **Revoke access** to grant or to decline the permissions to the selected group of users.

To decline or delegate entitlement review requests

1. Click the down-pointing arrow for the path filter. From the drop-down list select the paths using the check boxes.
2. Do any of the following:
   - Click **Decline** to reject the request to review permissions on the selected path.
   - Click **Delegate** to delegate the entitlement review task to another user.

After you submit the review request from the portal, the details are sent to the Data Insight Management Server. The Data Insight administrator can view the paths for which custodians have suggested changes to the permissions, and can perform the relevant changes. Alternatively, Data Insight can automatically trigger a

permission remediation action to distribute the actions to the proper authorities such as, directory server administrators.

To automatically initiate a permission remediation action, you must first configure the permission remediation settings. For more information, refer to *Veritas Data Insight Administrator's Guide*.

See "Logging in to the Self-Service Portal" on page 9.

Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents

You can use the Self-Service Portal to remediate incidents on the paths that are assigned to you. On the **DLP Incident Remediation** page of the portal, you can do following tasks:

- View a snapshot of the number of files that are assigned for your attention. The files are sorted according to the severity of incidents that are associated with them.
- Filter the list of files based on the severity of the incidents that the files have violated, the recency of the last access date, or the DLP policy that the files violate. The filters available to you depend on the options that are selected when configuring the workflow template.
  The different filters are applied together, and the list is filtered to show the data that matches the applied criteria.
- Perform a configured action on multiple files at one time. The available actions are DLP Smart Response rules configured in DLP. You can select more than one file from the list and then choose the desired action.

To remediate the files

1. Select the files that you want to remediate.

   You can choose to filter the list of files using the filter criteria at the top of the page. For example, you can prioritize the remediation of files that are associated with high severity incidents that violate a particular policy. Files that match the selected filter criteria are listed. Select the desired files from the list.

2. From the **Select Action** drop-down, select the action that you want to take on the selected files. For example, you may quarantine the files or mark the files for deletion. The listed actions are the Smart Response rules that are configured within DLP.

   For more information about Smart Response rules, see the *Symantec Data Loss Prevention Administration Guide*.

3. Click **Submit** to send the remediation request to the Data Insight Management Server for further action.

   On submission of the request, the actions that you select are sent to the Data Insight Management Server, which in turn requests the Response Rule Execution Service running on the DLP Enforce Server to execute the response rules. You can view the status of the workflow on the Data Insight Management Console.

Using the Self-Service Portal to confirm ownership of resources

You can use the Self-Service Portal to confirm or decline if you are the custodian of a particular path. On the **Ownership Confirmation** page of the portal, you can do following tasks:

- View all the paths for which you are requested to confirm your ownership.
- Select the paths you own and indicate your ownership.

To confirm ownership

1. Select the paths for which you have to confirm your ownership.
2. Click **Confirm** to accept ownership of the data resource for the purpose of remediation.

After you submit the confirmation request from the portal, the actions are sent to the Data Insight Management Server. The Data Insight administrator can view the paths for which custodians have declined ownership, and assign other custodians to the paths. For more information, refer to *Veritas Data Insight Administrator's Guide*.

See "Logging in to the Self-Service Portal" on page 9.

Using the Self-Service Portal to classify sensitive data

You can use the Self-Service Portal to classify files based on business value of their content. You can mark files with sensitive information as record. Files that are marked as record are submitted to Enterprise Vault, if it is configured in Data Insight, for further action.

On the **Records Classification** page of the portal, you can do following tasks:

- View a snapshot of the number of files that are assigned for your attention.
- Mark the assigned files as record or no record. .
- Filter the list of files based on the recency of the last access date or last modified date, or the policy that the files violate. The filters available to you depend on the options that are selected when configuring the workflow template.
  The different filters are applied together, and the list is filtered to show the data that matches the applied criteria.

To classify the files

1. Select the files that you want to remediate.
2. From the **Select Action** drop-down, select the action that you want to take on the selected files. For example, you may choose to archive the file. The listed actions indicate whether you want to mark the file as record or not. The name of the actions may vary depending on the name configured in the workflow.
3. Click **Submit** to send the remediation request to Enterprise Vault or the Data Insight Management Server for further action.

   The files that are marked as record are automatically archived using Enterprise Vault, if automatic action is enabled on these files. You can view the status of the workflow on the Data Insight Management Console.
4. Click **Delegate** to delegate the workflow to any other custodian.