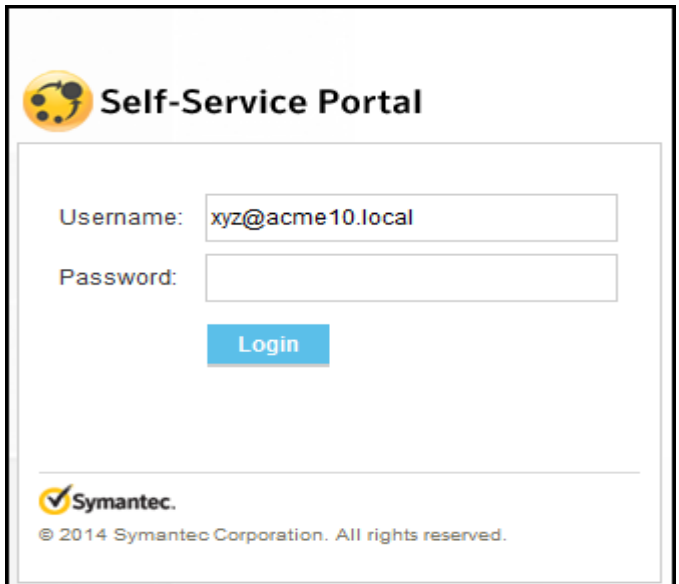


4.5.1 Quick Reference Guide

What can I do on the Self-Service Portal?

The Self-Service Portal allows your central information security team to distribute the remediation workflows directly to data owners and data custodians. You can use the portal for the following remediation tasks:

1. Remediate Data Loss Prevention (DLP) incidents.
2. Review entitlements on folders.
3. Confirm ownership of data.
4. Classify sensitive files as Record.



1 Install software

1. Install and configure Data Loss Prevention (DLP) version 12.5., if you intend to use DLP for remediating incidents. For instructions, see the DLP 12.5 Installation Guide.
2. Install and configure Symantec Enterprise Vault, version 10.4 or 11.0, if you intend to use Enterprise Vault to archive files marked as record. For details, see the Symantec Enterprise Vault™ documentation.
3. Install and configure Data Insight version 4.5.1.
4. Install the Portal server.

For instructions to install the Data Insight Management Server and the Portal server, see the Data Insight 4.5 Installation Guide.

The Self-Service Portal requires an Add-on license separate from Symantec Data Loss Prevention and Data Insight license. If your system is not licensed for the Portal, a prominent “License Required” message is displayed on relevant screens.

2 Configure DLP for use with the Self-Service Portal

1. Add policy groups, and configure policies and policy rules, so that incidents are generated when policy rules are violated.
2. Add file system targets and assign the appropriate policy groups to the targets.
3. Scan the file system targets to generate a list of incidents.
4. Configure Smart Response rules for your Network Discover file system incidents.
5. Create a Symantec Data Loss Prevention Enforce Server user with the appropriate role-based access control permissions for incident remediation.
6. Enable and configure the Response Rule Execution Service. Edit the *Manager.properties* file to change the value of `com.vontu.enforcewebservices.responserules.execution.service.schedule` to “ALWAYS”.

For more information, see the **Data Loss Prevention Administration Guide** and the DLP Data Insight Implementation Guide.

3 Configure settings on the Data Insight Management Console

1. Configure the communication between Data Insight Management Server and the DLP Enforce Server.
2. Configure the options to decide the look and feel of the SelfService Portal.
3. To use Symantec Enterprise Vault™ for the Records Classification workflow, ensure that Symantec Enterprise Vault™ is configured in Data Insight, and the device names in Enterprise Vault are mapped to those in Data Insight.

For more information on configuring DLP, Symantec Enterprise Vault™ and the SelfService Portal settings, see the Symantec Data Insight Administrator's Guide.

4 Create a workflow template

Create templates for each workflow type to suit your specific needs. Do the following:

1. In the Data Insight Management Console, click **Settings > Workflow Template > Add New Template**.
2. Select the type of workflow template—Entitlement Review, DLP Incident Remediation, Ownership Confirmation, or Records Classification.
3. On the **Add template** page, enter the name for the template, description, the details you want to show on the portal, and the frequency of email reminders that you want to send custodians.

You can customize the default workflow request email sent to custodians.

Notes:

In case of DLP Incident Remediation workflow templates, you must choose the Smart Response Rules that you want to present as remediation actions to the custodians. The Smart Response Rules are configured actions in DLP, such as delete or quarantine, for a given incident. Data Insight uses the DLP Response Rules Listing Service to fetch these rules from DLP.

Before you create a Records Classification workflow, create a mappings.csv file which maps the file classification policies to the retention category. Ensure that mappings.csv is saved in the data directory at %datadir%\conf\workflow\steps\ev\mappings.csv. A sample mappings.csv file is available for download on the **Workflow Template** page.

4. Click **Save**.

For details of each field on the **Add template** page, see the Symantec Data Insight Administrator's Guide.

5 Create a workflow request

Use a saved workflow template to create a workflow request for custodians. The custodians use the link provided in the workflow notification to log in to the SelfService Portal.

1. In the Data Insight Management Console, click **Settings > Workflow > Create Workflow**.
2. Select the type of workflow you want to create.
3. On the Workflow Information tab, enter the name, description, and start and end date for completing the workflow request.
Select the workflow template to be used for this workflow and the Self-Service Portal node on which you want to run the workflow.
4. On the Data Selection tab, select the paths for which you want to send the remediation requests.
Note: For DLP Incident Remediation workflows, you can select a data resource only if the share or folder contains sensitive files.
5. On the Resource-Custodian Selection tab, you can assign custodians on the selected paths. Custodians can either be imported from Data Insight, assigned using a CSV file or selected manually.
You can also explicitly assign or remove custodians on selected paths from this panel.
6. For Entitlement Review workflows, use the Exclusion List tab to exclude users or user groups from the scope of the review.
7. Click **Submit Workflow**.

For details of each field on the **Create Workflow** page, see the Symantec Data Insight Administrator's Guide.

6

Log in to the Self-Service Portal

After a workflow is submitted from the Data Insight Management Console, the custodians selected in the workflow receive an email notification with a link to the Self-Service Portal.

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**.
The branding on the Self-Service Portal depends on the look and feel configured in Data Insight.
3. When you log in to the portal, you are presented with a welcome message. On the message, click **OK** to continue with remediation actions on paths submitted for your attention.

The link received in the email notification is valid only till the workflow is completed or is cancelled. A workflow is said to be complete when an action is submitted for all paths assigned to the custodian or if the end date of the workflow lapses. Data Insight provides custodians a grace period of one day, during which the custodians do not receive email reminders, but they can still log in to the portal. Any actions that are already submitted will be completed during the grace period. After the grace period is complete, the workflow is marked as completed and custodians can no longer log in to the portal.

7

Take remediation actions on the Self-Service Portal

Once the custodians log in to the Self-Service Portal, they can view all paths that have been assigned to them for remediation. Depending on the type of workflow, they can take the following actions on the assigned paths:

DLP Incident Remediation Workflow

- Filter the list of files based on the severity of the incidents that the files have violated, the recency of the last access or modification date, and the DLP policy that the files violate. The filters available to the custodian depend on the options that are selected when configuring the workflow template.
- Perform a configured action on assigned paths. The available actions are DLP Smart Response rules configured in DLP. The custodian can select more than one file from the list and then choose the desired action.

Entitlement Review Workflow

- Filter the users to be reviewed based on their activity profiles and the assigned paths. For example, custodian might be interested in first reviewing the entitlements for the users who are inactive.
- Recommend whether to allow or revoke permission on a path to a specific user. You can configure custom actions in Data Insight to implement the recommendations.
- Decline the review request or delegate the path for review to another custodian.

Ownership Confirmation Workflow

- Confirm or deny ownership of assigned paths.

Records Classification Workflow

- Mark sensitive files as Records. The files marked as records are archived for a specified retention period using EnterpriseVault™, if automatic archiving is enabled at the time of creating the workflow.

8

View the status of submitted actions

Once custodians submit their actions on the portal, the actions are sent for execution to the DLP Response Rules Execution Service, in case of DLP Incident Remediation workflows, or to the Data Insight Management Server in case of Entitlement Review and Ownership Confirmation workflows.

To monitor the progress of the workflow, do the following:

1. On the Data Insight Management Console, click **Settings > Workflows**.
2. On the Workflow list page, click the workflow, or click the **Select Action** drop-down corresponding to a workflow and click View
3. The status for each path can be as follows:
 - **Pending** - Indicates that the custodian has not taken any action on the assigned paths.
 - **Success** - Indicates that the custodian has submitted an action from the Self-Service Portal and the action has been registered with the Data Insight Management Server.
In case of a DLP Incident Remediation workflow, the status "**Success**" indicates that Data Insight has sent the response rule request for execution to the DLP Response Rule Execution Service. You must ensure that the Response Rule Execution Service is enabled in DLP.
In case of a Records Classification workflow, if a file is marked as record by the custodian, and if automatic action is configured, Data Insight submits the response for action to Enterprise Vault. Once Enterprise Vault archives the file and applies the post-processing actions on the file, Data Insight displays the response from Enterprise Vault on the Management Console. In this case, "**Success**" indicates that the archive request is completed by Symantec Enterprise Vault™.
 - **Executing Action** - In case of a Records Classification workflow, this status indicates that a file is marked as record by the custodian, and the archive request is being processed by Symantec Enterprise Vault™.
 - **Failed** - Indicates that the action submitted by the portal user on the Self-Service Portal failed for some reason.
 - **Expired** - Indicates that the due date for completing the workflow has expired and the Portal users will not be able to take any action on the paths in that particular window.