Data Insight 4.5
Feature Briefing
Self-Service Portal

This document is about the new Self Service Portal feature introduced with Data Insight 4.5.

If you have any feedback or questions about this document please email them to **IIG-TFE@symantec.com** stating the document title.

This document is provided for informational purposes only. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Symantec.

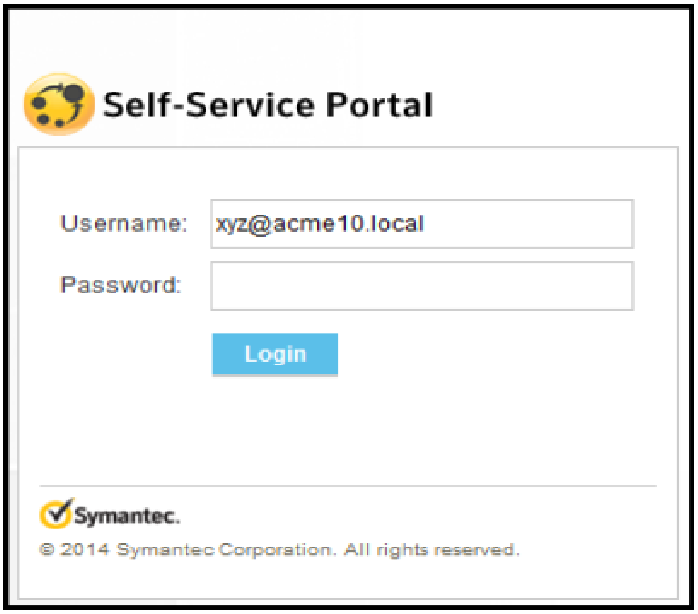
Feature Description

Data Insight 4.5 introduces a new feature called Remediation Workflows. These workflows provide an easy way to distribute remediation tasks to identified custodians and data owners to help identify any potential security or permissions issues that may reside on file shares and SharePoint within an organization.

Remediation Workflows include:

- Entitlement Review – This task requires custodians to review user permissions on folders. The custodian must then either confirm that assigned permissions are correct or suggest changes.
- DLP Incident Management – This workflow allows a custodian or data owner to view policy violations detected by DLP (Symantec Data Loss Prevention). Access to the DLP Enforce Console is not required by the custodian or the data owner when using Data Insight's Self-Service Portal. Please note that the DLP workflow is designed to be functional even if Data Insight is not monitoring the resource being managed by DLP. Data Insight will have the ability to import incidents from DLP to which the Administrator can assign data owners/custodians for the workflow.
- Ownership Confirmation – Confirm the ownership of resources (such as folders and files)

Data Insight 4.5 comes with a new web-based Self-Service Portal. The portal provides the ability for identified data owners/custodians to complete assigned tasks.


Self-Service Portal

Username: xyz@acme10.local

Password:

© 2014 Symantec Corporation. All rights reserved.

Business Value

Organizations that have large amounts of file storage may find it difficult to manage the responsibility of remediating data resources to data owners and custodians. Typically security and storage administrators must manually inform data owners about any identified issues with the resources that they own. It can also be a difficult task to track remediation actions on identified resources. As more data is added to an organization, the remediation process becomes more difficult to manage.

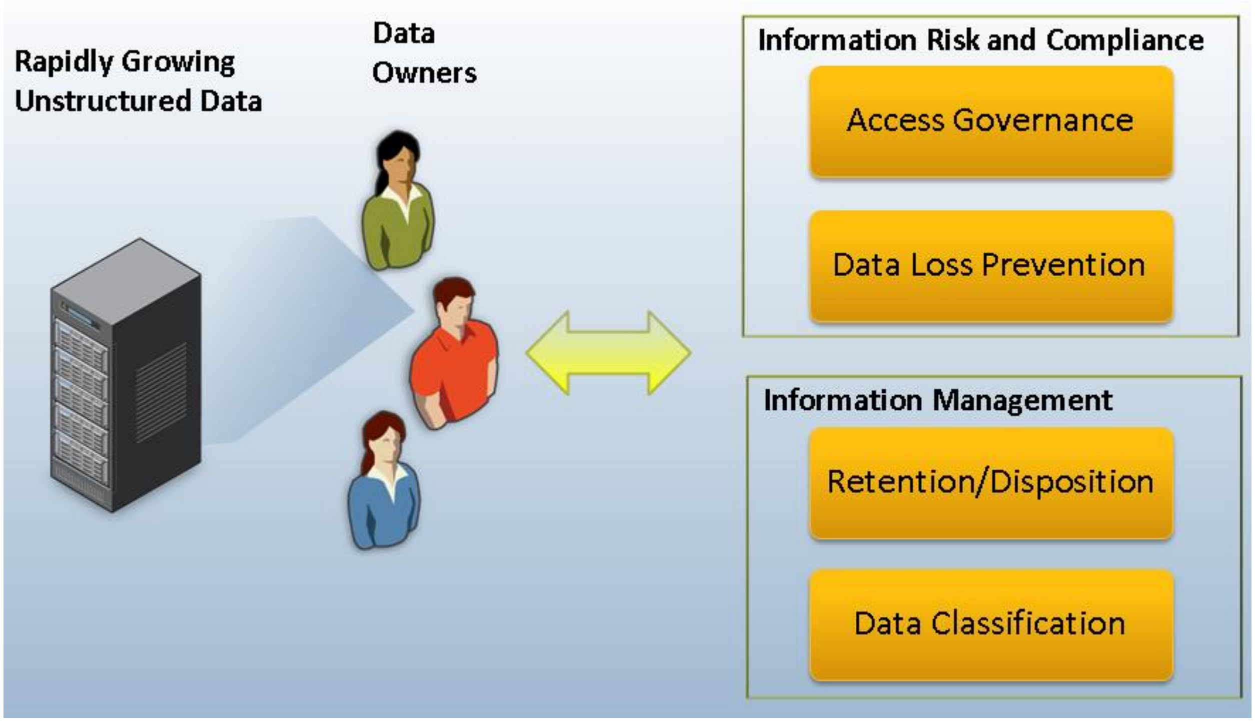


Figure 1 – Data Remediation Requirements

With the Self-Service Portal feature, remediation tasks can be created and tracked to ensure that custodians and data owners are complying with organizational security requirements. By having Data Insight manage remediation tasks, it will be easier for security and storage administrators to track to see if a task has been completed by identified data owners.

Underlying Principles

Architectural Overview

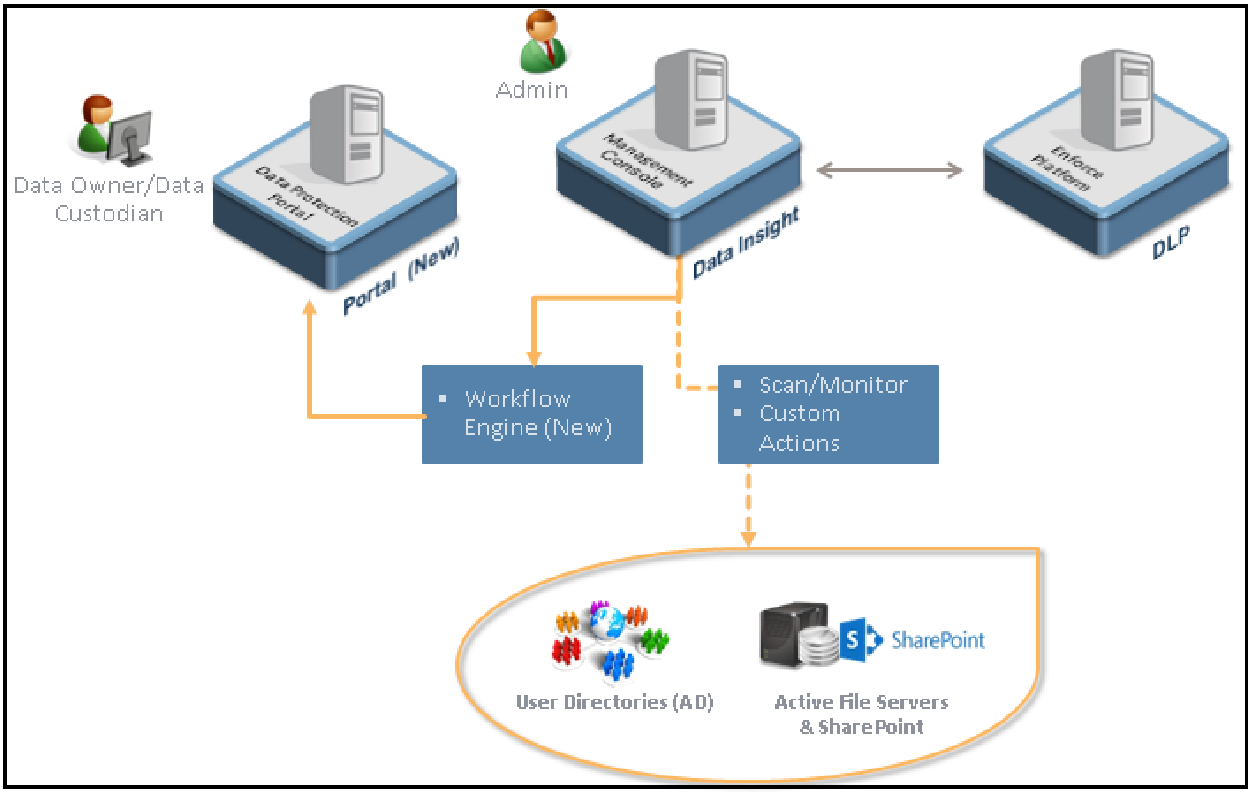


Figure 2 – Data Insight Architectural Overview

Remediation within Data Insight includes multiple components:

- **Data Insight Server** – The Data Insight server is at the heart of the remediation process and facilitates communications and data gathering between Symantec Data Loss Prevention (DLP), SharePoint and file shares, Active Directory, and the Self-Service Portal
- **DLP** – Symantec Data Loss Prevention has the ability to scan file systems and detect violations that may exist. The Data Insight server can gather a list of all violations for reporting and remediation purposes.
- **Self-Service Portal** – The Self-Service Portal, which is a component on the Data Insight Server, allows security and storage administrators to create remediation workflows and tasks and also has the ability to notify identified data custodians and owners of any tasks that need to be completed

- **Administrator** – The Data Insight administrator has the ability to generate remediation workflows and tasks
- **Data Owner/Data Custodian** – These users receive notifications that they have been assigned remediation tasks
- **Data Endpoints** – Data endpoints include file servers and SharePoint servers
- **User Directories** – Data Insight will synchronize a list of users from Active Directory to help identify data custodians and owners

The Remediation Workflow

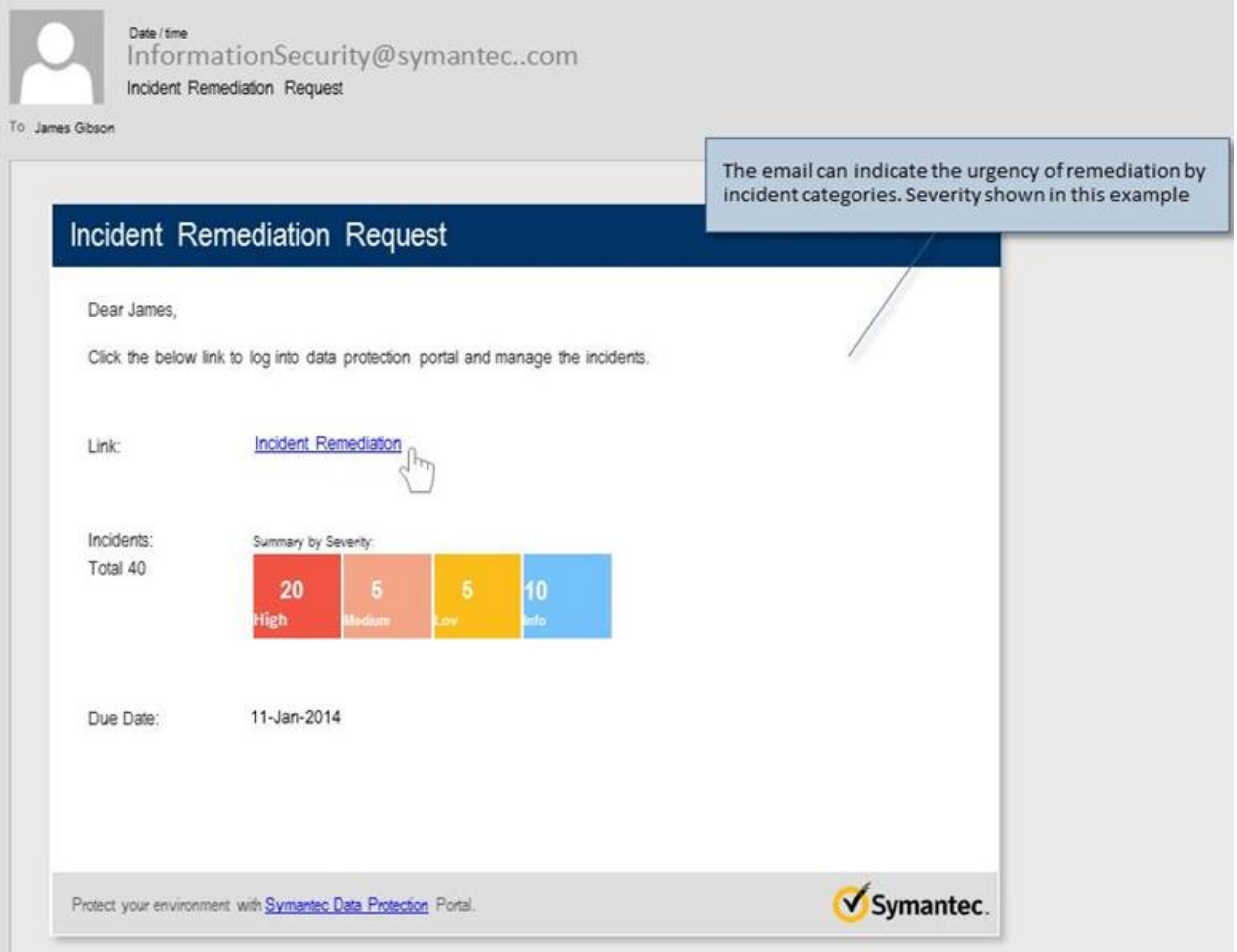
The process of creating a remediation workflow starts with the Data Insight administrator. The process contains the following steps:

- The administrator creates reports within Data Insight to find data that resides on file shares and SharePoint that requires remediation
- The administrator assigns data owners to the identified resources. Ownership can be assigned within the Data Insight Console or while creating the remediation workflow.
- The administrator creates a Workflow Template using the Self-Service Portal to fan-out incidents to identified data owners/custodians
- Lastly, the administrator creates a unique Workflow instance based on a Workflow Template. The administrator will also have the ability to track the progress of the workflow.

The data custodians/data owners then perform the following tasks once the Workflow has been created:

- The user receives emails on resources in question which describes actions to complete in the Workflow
- The user then requests actions on identified resources
- Lastly, the user verifies ownership, adjusts access controls (permissions), or remediates incidents identified in the Workflow

Figure 3 provide an example of an email that is generated from a Workflow Template and sent to the data custodian/owner. The email identifies the severity of incidents as well as the number of each. Included in the email is a link to begin the remediation process.



Date / time
InformationSecurity@symantec..com
Incident Remediation Request
To James Gibson

The email can indicate the urgency of remediation by incident categories. Severity shown in this example

Incident Remediation Request

Dear James,

Click the below link to log into data protection portal and manage the incidents.

Link: Incident Remediation

Incidents: Total 40

Summary by Severity:

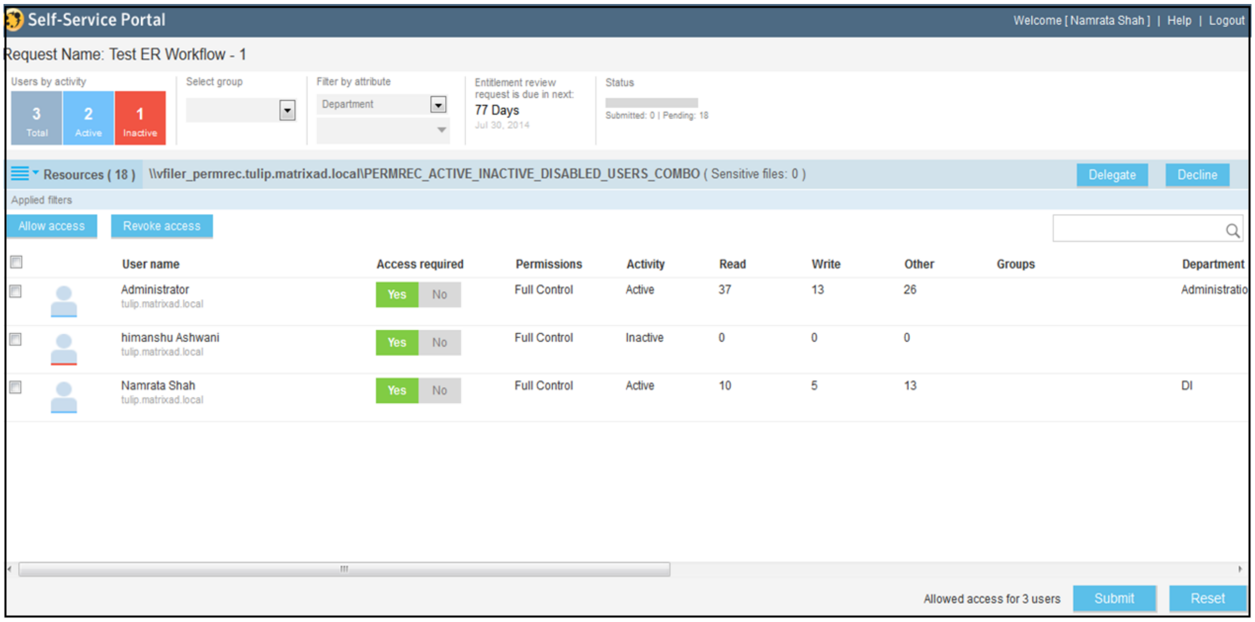
20	5	5	10
High	Medium	Low	Info

Due Date: 11-Jan-2014

Protect your environment with Symantec Data Protection Portal.

Figure 3 – Incident Remediation Request Email

Once logged into the Self-Service Portal, the user will be presented screens based upon the workflow template type (Entitlement Review, DLP Incident Management, or Ownership Confirmation). Figure 4 provides a sample screenshot of a data custodian/owner fulfilling a Workflow Task.



Request Name: Test ER Workflow - 1

Entitlement review request is due in next: 77 Days
Jul 30, 2014

Submitted: 0 | Pending: 18

\\vfiler_permrec.tulip.matrixad.local\PERMREC_ACTIVE_INACTIVE_DISABLED_USERS_COMBO (Sensitive files: 0)

User name	Access required	Permissions	Activity	Read	Write	Other	Groups	Department
Administrator tulip.matrixad.local	Yes No	Full Control	Active	37	13	26		Administratio
himanshu Ashwani tulip.matrixad.local	Yes No	Full Control	Inactive	0	0	0		
Namrata Shah tulip.matrixad.local	Yes No	Full Control	Active	10	5	13		DI

Allowed access for 3 users

Figure 4 – Entitlement Review

Prerequisites

Before the Data Insight administrator can submit a remediation workflow to the Self-Service Portal, the following configuration tasks must be completed:

- The Self-Service Portal is installed and registered with the Data Insight Management Server. The administrator can validate the installation by going to the **Settings -> Data Insight Servers** section in the Data Insight Console
- To create DLP Incident Remediation workflows, install DLP 12.5 on a Data Insight node (non-Management server) and ensure that DLP settings have been configured in the Data Insight Console on the Management server.
- Ensure that directory service domains have been configured in Data Insight
- Ensure that custodians are assigned to paths to resources configured in Data Insight. If paths do not have custodians assigned, the administrator can assign custodians at the time of creating the workflow request.

For more information on configuring and using Self-Service Portal and Remediation Workflows, refer to the *Data Insight 4.5 Administrator's Guide* and the *Self-Service Portal Quick Reference Guide*.

Licensing and support considerations

Licensing

In order to use Remediation Workflows and the Self-Service Portal, a separate license is required. The feature can be purchased on a per user or per terabyte basis.

Support Considerations

The Self-Service Portal feature has the following hardware and operating system requirements:

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2. The operating system must be 64-bit.
- 8GB RAM
- 4 CPUs (or cores)

About Symantec:

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at **www.symantec.com**.

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934