



# A Guide for Deploying and Administering the RSA Solution for Microsoft SharePoint

**RSA® SecurBook  
for Microsoft SharePoint®**



The Security Division of EMC

## **The RSA Solution for Microsoft SharePoint Team**

Susam Pal, Arun P Kumar, Satish Vohra, Vineet Mittal, Kartik Saxena, Rinmy Moideen, Vikas Madhusudan, Arjuna Rangathappa, Vrinda Keshav, Srinath Gaddam, Amanda VanVeen, Andrew Lickly, Bikram Barman, Dave Howell, Nirav Mehta.

### **Contact Information**

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: [www.rsa.com](http://www.rsa.com)

### **Trademarks**

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.

### **License agreement**

This software and the associated documentation are proprietary and confidential to RSA, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

### **Third-party licenses**

This product may include software developed by parties other than RSA.

### **Note on encryption technologies**

This documentation is about products or solutions that may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

### **Distribution**

Limit distribution of this document to trusted personnel.

# Contents

<i>About This Guide</i>	4
References	5
<i>Solution Objectives</i>	6
SharePoint Basics	6
Business Scenarios	9
High-Level Security Objectives	12
Functional Requirements	13
<i>Solution Architecture</i>	15
<i>Solution Deployment</i>	22
Enterprise Deployment	22
Supported Product Versions	23
Deployment Instructions	24
<i>Solution Administration</i>	32
Introducing Macers Corporation	32
Administering the RSA Solution for Microsoft SharePoint	36
<i>Troubleshooting</i>	62
Debugging RSA Secure View	62
Common Issues and Resolution	62

## About This Guide

This document provides guidance for planning, deploying, and administering the RSA Solution for Microsoft SharePoint. It is intended for the security or IT operations department of an organization that has acquired one or more components of the RSA Solution for Microsoft SharePoint.

The guide is divided into the following sections:

**Solution Objectives** - Introduces the SharePoint resource hierarchy essential to understanding the scope and functionality of the solution. It also describes the solution objectives based on common security-related requirements of organizations that use Microsoft SharePoint. These solution objectives are based on direct market research that RSA has conducted to understand such requirements.

**Solution Architecture** - Introduces the main components that make up the solution and the role of each component.

**Solution Deployment** - Focuses on the configuration and planning necessary to ensure that solution components integrate with each other (where applicable) and with SharePoint. It provides instructions (with screenshots where applicable) to ease and accelerate the deployment of the solution. This guide does not repeat instructions from other product documentation.

**Solution Administration** - Using a fictitious company provides step-by-step instructions for the administration and operation of the RSA Solution to deliver the visibility and control that a security department may need. Product screenshots are provided where appropriate.

**Troubleshooting** - Describes the known issues and workarounds. It also provides detail about the customer support and consulting services available from RSA to support the RSA solution at customer sites.

## References

<a href="#">Microsoft SharePoint Farm Installation</a>	<a href="http://technet.microsoft.com/en-us/library/cc262243.aspx">http://technet.microsoft.com/en-us/library/cc262243.aspx</a>
<a href="#">Microsoft AD RMS Product Documentation</a>	<a href="http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.aspx">http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.aspx</a>
<a href="#">RSA DLP Product Documentation</a>	<a href="https://knowledge.rsasecurity.com/docs/rsa_edp/dlp_70/Datacenter_7.0_Deployment.pdf">https://knowledge.rsasecurity.com/docs/rsa_edp/dlp_70/Datacenter_7.0_Deployment.pdf</a>
<a href="#">RSA Authentication Manager Product Documentation</a>	<a href="https://knowledge.rsasecurity.com/docs/rsa_securid/rsa_auth_mgr/61/authmgr_install_windows.pdf">https://knowledge.rsasecurity.com/docs/rsa_securid/rsa_auth_mgr/61/authmgr_install_windows.pdf</a>
<a href="#">RSA Access Manager Installation and Configuration Guide (server)</a>	<a href="https://knowledge.rsasecurity.com/docs/rsa_cleartrust/access_manager/install_config.pdf">https://knowledge.rsasecurity.com/docs/rsa_cleartrust/access_manager/install_config.pdf</a>
<a href="#">RSA Access Manager Agent Installation and Configuration Guide (agent)</a>	<a href="https://knowledge.rsasecurity.com/docs/rsa_cleartrust/agent/48/docs/WebServersInstallConfig.pdf">https://knowledge.rsasecurity.com/docs/rsa_cleartrust/agent/48/docs/WebServersInstallConfig.pdf</a>
<a href="#">RSA enVision Configuration Guide</a>	<a href="https://knowledge.rsasecurity.com/docs/rsa_env/envision/400/RSA%20enVision%204.0%20Configuration%20Guide.pdf">https://knowledge.rsasecurity.com/docs/rsa_env/envision/400/RSA%20enVision%204.0%20Configuration%20Guide.pdf</a>

## Solution Objectives

In this guide, the term ‘SharePoint’ refers to Windows SharePoint Services (WSS) 3.0 and applications that are supported by WSS, for example, Microsoft Office SharePoint Server 2007.

The use of SharePoint to manage collaboration has grown precipitously over the last few years in both large and small organizations. This widespread use of SharePoint for collaboration at both departmental and corporate levels is a testament to the usability of SharePoint. However, organizations find it difficult to gain the central visibility and control they need to ensure that unfettered collaboration and document sharing does not lead to loss of sensitive<sup>1</sup> data or unauthorized access.

This section includes the:

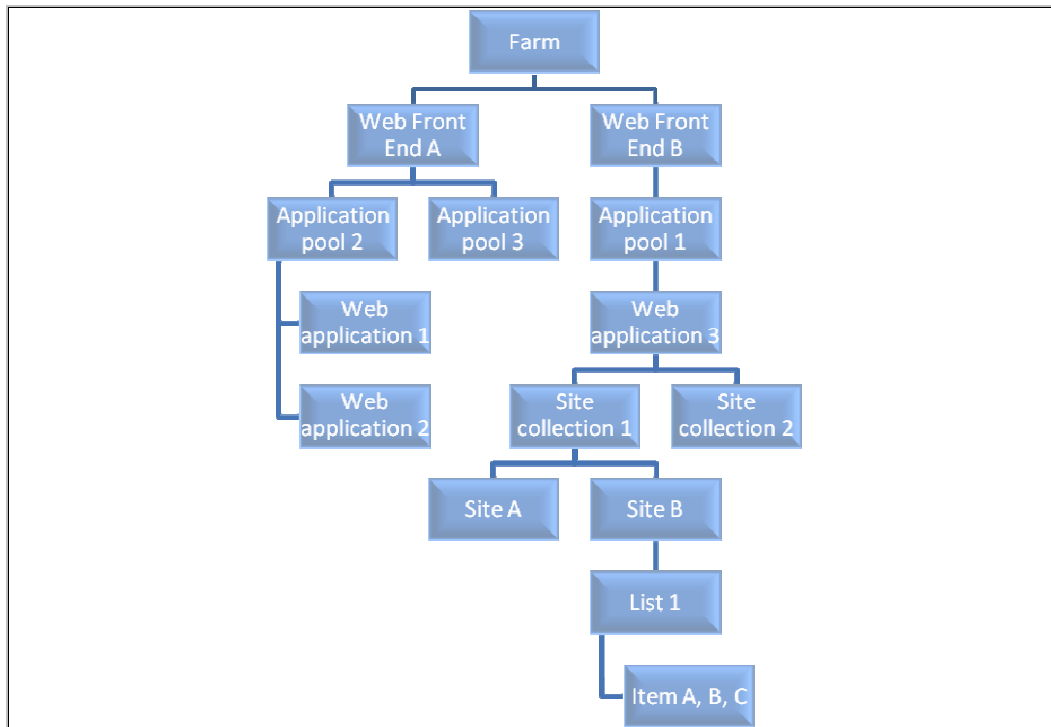
- SharePoint terminology and an illustration of the SharePoint resource hierarchy. These are essential to understanding the scope and functionality of the solution.
- Typical business scenarios that drive the need for security in SharePoint deployments.
- Security activities that information security departments may undertake to ensure that the use of SharePoint is in compliance with internal and external security policies.

## SharePoint Basics

This section describes the SharePoint terminology and the major components that make up the SharePoint architecture. The SharePoint resource hierarchy is described in [Figure 1](#).

---

<sup>1</sup> In this document, ‘sensitive information’ or ‘sensitive data’ means data whose confidentiality, integrity or availability must be protected or else it would have significant negative impact to the organization responsible for managing that data.



**Figure 1: SharePoint Resource Hierarchy**

## Farm

The collection of servers, services and databases that make up the SharePoint implementation. A SharePoint farm is a collection of one or more SharePoint servers and one or more SQL servers that come together to provide a set of basic SharePoint services bound together by a single Configuration Database.

## Servers

The following servers are part of a farm:

**Web Front End Servers.** These servers respond to web requests from SharePoint users. Depending on the expected load, generally one to eight servers are used at this layer of the topology.

**Application Servers.** These servers (for example, Index Server, Query Server, Excel Calculation Services and Forms Services) may be used to add specific services to the SharePoint environment.

**SQL Server.** This server is used as the backend database for SharePoint. SQL Server is the repository for almost everything in SharePoint.



## Application Pools

These pools are hosted and managed by Internet Information Services (IIS) on a Windows Server. IIS application pools typically provide process isolation between content, in part for security reasons. For example, if one site is exploited, process isolation makes it harder for an attacker to inject code into the server to attack other sites.

## Web Applications

These are IIS web sites created and used by SharePoint. Each web application is represented by a different web site in IIS. A unique domain name is assigned to each web application to help prevent cross-site scripting attacks. There are two kinds of web applications:

- Central Admin Web Application. This web application enables central administration of SharePoint (can be disabled when not in use).
- Content Web Applications. These provide access to SharePoint content.

## Databases

Each site collection in SharePoint can exist only in one content database. It cannot be split over multiple content databases. SharePoint has these types of databases:

- Configuration database
- Administration database
- Shared Service Provider database(s)
- Search database(s)
- Content databases

## User Directory

This is an LDAPv3-compliant directory that stores user profile information. Although the user directory is not part of the SharePoint resource hierarchy, it is important to note that all users within SharePoint are either users in Microsoft Active Directory (AD) or another supported LDAP directory.

## Site Collections

- Site collections are hosted in a web application. Each site collection is a set of web sites that has the same owner and shares administration settings.
- Each site collection contains a top-level web site and can contain one or more sub-sites. A site collection has a shared navigation structure.





- Site collections bridge logical architecture and information architecture. They satisfy requirements for URL design and create logical divisions of content. A site collection manages itself and its sub-sites.

## Sites

Sites span from the highly structured top-level site to the unstructured ad hoc collaboration team sites. Sites can contain sub-sites. For example, a Finance site could contain three Accounting sites. A site does not have all the features of a site collection. It is largely focused on looking after itself but not the sub-sites.

## Lists

Almost everything in Microsoft Office SharePoint Server 2007 is stored in a list. An example of a list is a SharePoint Document Library which is used to store documents. Windows SharePoint Services 3.0 lists provides a core set of functionality including content management (create, read, update, delete), check-in/checkout, versioning, security, workflow, storage management, presentation management, the ability to perform advanced list customization, and column configuration.

## Items

Items can be documents, calendar items, contacts, customers, images and custom list items. An item in SharePoint uses a list as a storage container.

## Business Scenarios

The business scenarios discussed in this section are not exhaustive and are only meant to provide useful context for understanding the requirements for the solution. The scenarios are organized under the following themes:

**Visibility.** These scenarios involve activities that utilize discovery, monitoring, and the reporting capabilities of the solution. These activities address questions such as, Where does sensitive information exist? Who has access? Are the servers hosting SharePoint vulnerable to attack?

**Control.** These scenarios involve activities that often result from gaining visibility and involve activities that modify the current state of security to bring it in line with the intended policy. These scenarios utilize the solution to address questions such as, How can access to sensitive information be restricted to authorized persons?

The following figure describes the business scenarios and how they map to the high-level security objectives and functional requirements that are described later in this section.

The main entity responsible for supporting the following scenarios and requirements is typically the information security department of an organization that has a relatively wide distribution of SharePoint sites across the network (for example, several departments with one or more site collections for each department).

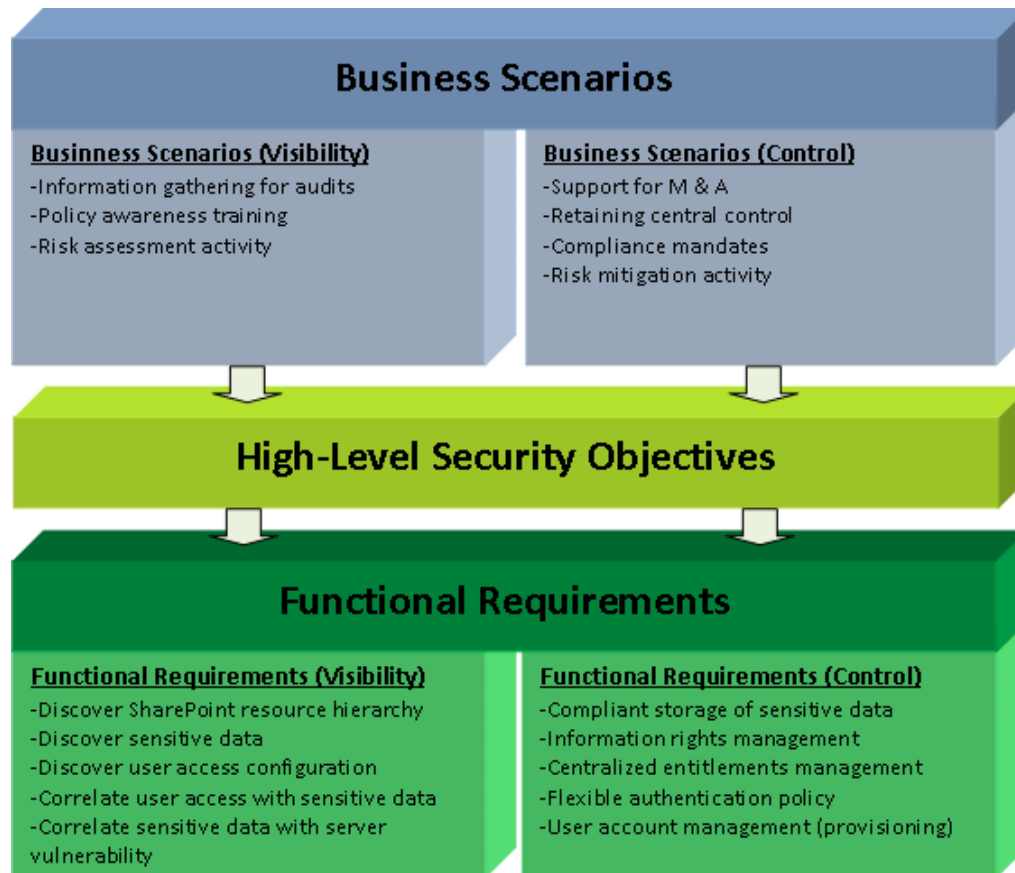


Figure 2: Business Scenarios Mapped to Functional Requirements

## Business Scenarios for Visibility

### Information Gathering for Audits

Organizations may have internal or external (for example, regulatory) audit requirements that mandate a review of configuration and any activity that is related to access of sensitive resources. In order to satisfy this requirement, sensitive information must be identified wherever it resides in the infrastructure, and it must be correlated with users who have access to it.



## **Policy Awareness Training**

Training and awareness is an important aspect of organizational security. There is often a requirement to train employees on how to store and handle sensitive information. By understanding exactly who accesses sensitive information and what they do with it (for example, downloading, editing, deleting), the organization can better track the effectiveness of its training activities.

## **Risk Assessment Activity**

Risk assessment often requires time-consuming manual detection of sensitive resources and interviewing resource owners to determine the intended and actual policy enforcement for these resources. By identifying sensitive information and the user groups that can access it, risk analysts can quickly prioritize the sites where they must perform a more costly, in-depth, risk analysis.

## **Business Scenarios for Control**

### **Support for Mergers & Acquisitions**

When organizations undergo large changes to infrastructure and the addition or removal of user accounts (for example, in mergers and acquisition scenarios), they typically require a scalable and structured way to ensure that all users are provisioned correctly to the applications and user directories of the company. During this transition, security administrators need a way to restrict any access to sensitive data by new employees until the correct roles can be established for new users.

### **Retaining Central Control**

Administrators within an organizational department typically have control over their department's SharePoint deployments. In certain cases, where it is likely that SharePoint sites contain intellectual property or confidential corporate information, the corporate security department may want to control what users can access the data and under what conditions the data is allowed to leave those SharePoint sites.

### **Compliance Mandates**

Many organizations are mandated to abide by compliance regulations that specifically address the issue of protecting sensitive information. These organizations must be able to effectively enforce controls, in addition to reporting on them.

### **Risk Mitigation Activity**

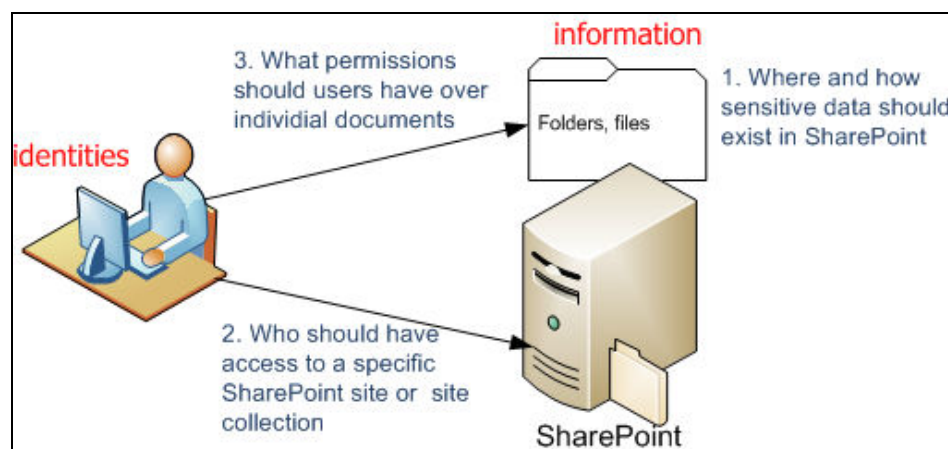
Risk analysis often requires a process for prioritizing control of resources that are of high value to the company and are at a high potential for loss. Risk mitigation may involve protecting sensitive resources by using a data security policy to enforce the compliant storage of sensitive information, and may also involve the enforcement of proper access to these resources.

## High-Level Security Objectives

The business scenarios described in the previous section result in the following security objectives across a SharePoint farm:

1. Where and what type of sensitive data can exist in SharePoint? (For example, financial statements should never exist on any SharePoint site in the DMZ.)
2. Which users should have access to specific SharePoint sites based on their organizational roles? (For example, only Executive Management should access SharePoint sites hosting financial statements.)
3. On a given SharePoint site, who should have access to specific sensitive SharePoint objects and what type of permissions should they have? (For example, on the HR site, HR Managers should be able to modify files related to employee benefit information, but they should not be able to save the data to their desktop.)

The following figure shows the security objectives described above as elements of a SharePoint security policy.



**Figure 3: Elements of a SharePoint Security Policy**

Another critical component of the governance of the above policies is the need for a complete view of security events across the entire SharePoint environment. (For example, Where is new sensitive data being created in the environment? Is sensitive information on servers that are vulnerable to attack?) Visibility into these activities can provide useful insight into how to prioritize security enforcement. For example, from a security perspective, it is crucial knowledge that sensitive data resides on the same set of unpatched servers where multiple failed logon attempts have been recorded.

## Functional Requirements

The business scenarios and high-level security objectives typically result in the following detailed functional requirements. The RSA Solution for Microsoft SharePoint is primarily targeted to meet these requirements.

### Functional Requirements for Visibility

#### Discover SharePoint Resource Hierarchy

In order to identify areas on which to focus security efforts, the security administrators have to survey the SharePoint environment. They typically have to navigate deployed site collections one at a time. This process can be tedious and may be impractical when an environment consists of a large number of site collections and sites. It would be helpful to have a single security console that allows navigation of the SharePoint hierarchy for a given farm and then allow probing into security aspects of selected branches of the hierarchy.

#### Discover Sensitive Data

It is not easy to identify the specific SharePoint sites and resources within those sites (for example, documents) that contain sensitive data. This is especially troublesome if users do not erase the data and the data persists in SharePoint after a project is completed. Such proliferation of data across a widely dispersed SharePoint deployment makes it difficult to know how much or exactly where sensitive data exists.

#### Correlate User Access with Sensitive Data

It is difficult to determine which users and user groups have access to:

- SharePoint sites that contain sensitive data
- Resources (files and folders) within those sites that contain the sensitive data

#### Correlate Sensitive Data with Server Vulnerability

Sensitive information may have been created on or moved to hosts with security vulnerabilities. This elevates the overall risk posed to confidentiality of information. It is difficult for security administrators to investigate whether hosts that contain sensitive information also have security vulnerabilities. Some examples of security vulnerabilities include unpatched OS/applications and the lack of malware protection. A security administrator may also want to correlate the presence of sensitive data on a host with the number of failed logon attempts. This detects abnormalities that may be indicative of a security attack.



## **Functional Requirements for Control**

### **Compliant Storage of Sensitive Data**

Security administrators need to ensure that sensitive data is stored in compliance with the customer security policy. Some examples of policy objectives that may be implemented are:

- Some types of sensitive data must not exist on certain SharePoint sites at all
- Some types of data must always be encrypted when stored on SharePoint
- Some types of data must be moved if found in places where they are not allowed to be stored

### **Information Rights Management**

Organizations need to centrally exert control over what can be done with information within SharePoint even after it leaves SharePoint, for example, restricting users from copying files to their desktops or printing documents. This type of enforcement is critical to preventing the leakage of sensitive data. Microsoft Active Directory Rights Management Services (RMS) provides these capabilities and it would be even more effective if RMS protection can be automatically triggered based on sensitivity of content.

### **Centralized Access and Entitlements Management**

Security administrators sometimes need to ensure that user access to a few high-sensitivity SharePoint sites and resources is controlled at a granular level from a central security console with the ability to override the control of a departmental SharePoint administrator. Such central control should be used sparingly (for sensitive corporate content) because information owners and SharePoint administrators within individual departments of an organization are often best suited to make decisions about who should access the content that they manage.

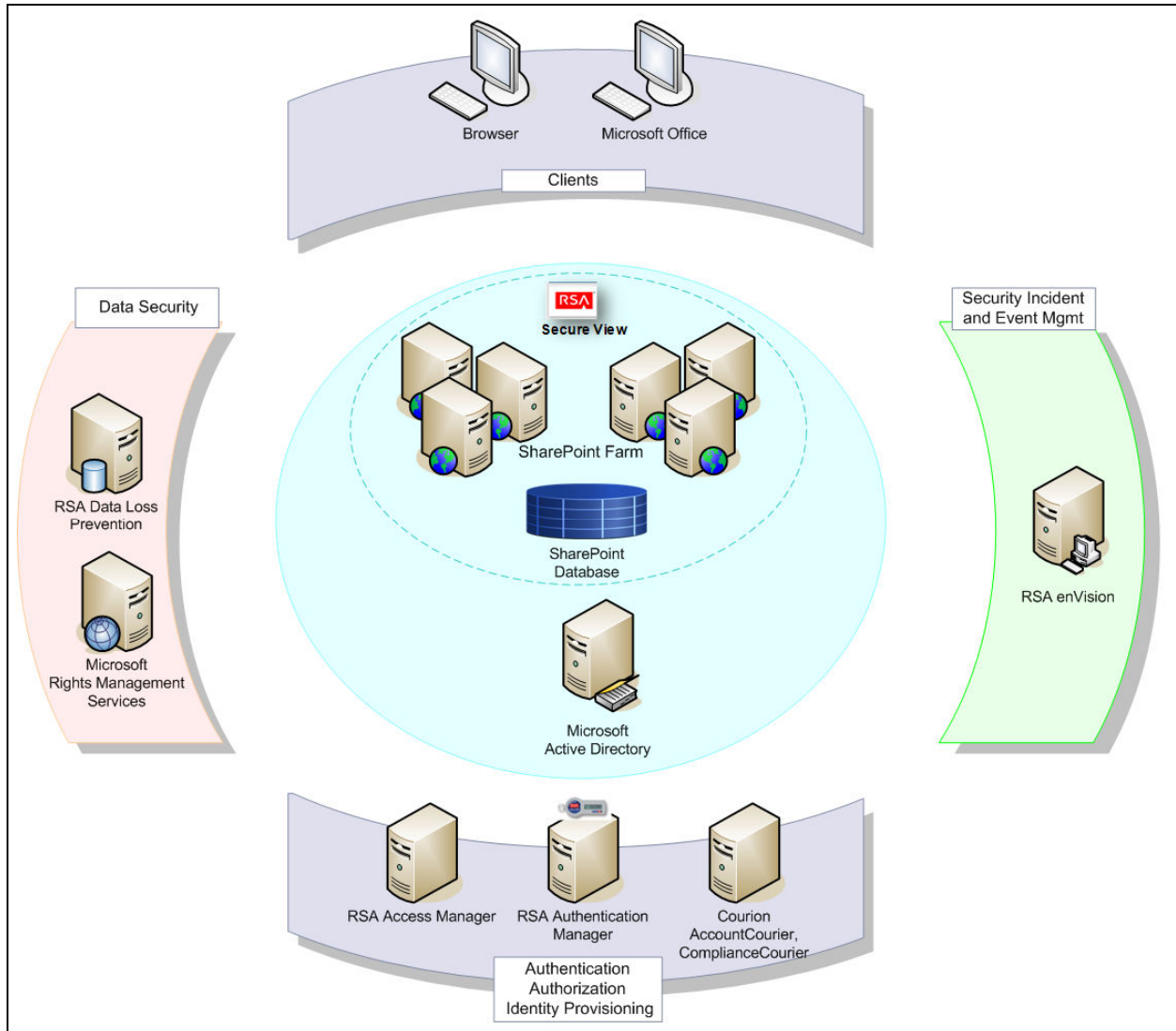
### **Flexible Authentication Policy**

There is a need to enforce authentication policies based on the sensitivity of resources being accessed (for example, requiring two-factor authentication for access to all draft company financial statements that have not been released yet).

### **User Account Management (Provisioning)**

In organizations with a large number of employees, it is difficult to ensure that SharePoint privileges are granted, modified, or revoked as users join the organization, transition to new roles or leave the organization. There is a need to systematically link SharePoint account management to the HR system and processes that manage the addition, movement, and termination of personnel.

## Solution Architecture



**Figure 4: Solution Architecture**

The RSA Solution for Microsoft SharePoint includes:

- A content-aware protection approach spanning identities and information.
- Central visualization and control of SharePoint security.
- Enterprise-grade RSA and partner products that can be extended to secure other applications in an organization.



- A modular architecture that enables an organization to deploy one or more product components. Every component delivers value on its own, but the combination of products delivers a solution greater than that sum of its parts.

The solution supports a full cycle of activities including the following:

- Discover the current state (where the sensitive data is and who has access to it)
- Set/Adjust/Enforce desired data security and user access policy
- Monitor and report on security-relevant events

## Architectural Goals and Components

This section describes the architectural goals met by various products in the solution.

### Discovery

#### RSA Secure View

RSA Secure View for Microsoft SharePoint (referred to as simply RSA Secure View in this document) enables security administrators to centrally view the entire SharePoint hierarchy for a single SharePoint farm. It enables administrators to select specific branches of the hierarchy and view whether sensitive information was identified by the RSA Data Loss Prevention Datacenter product (RSA DLP). Also, it has the ability to show user access policies defined in SharePoint on those resources.

#### RSA Data Loss Prevention suite

The products in the RSA Data Loss Prevention (DLP) Suite accurately identify and locate sensitive information within large enterprise networks, whether it is stored on computers or file shares, or is being transmitted to external networks, or is being copied, saved, printed, or otherwise used inappropriately. Using centralized policy administration and a distributed and highly scalable detection technology, the DLP products identify regulated or confidential data in the largest of networks and, if necessary, take immediate action on it. The RSA DLP Datacenter product scans and identifies sensitive information within SharePoint.

### Remediation

The following options are available for remediation of security non-compliance:

#### RSA Secure View:

Often, remediating security issues involves a workflow in which a security administrator detects the issue and the application or infrastructure administrator executes the necessary changes after necessary





consultation. To facilitate such a workflow, RSA Secure View offers the ability to export reports that show who can access sensitive information. Security administrators can then use the reports to initiate conversations with the information owners and ensure compliance with the security policy.

### **RSA Data Loss Prevention:**

Once it identifies sensitive information, the RSA Data Loss Prevention Datacenter product can automatically apply the following remediation policies if appropriately configured.

- Invoke Microsoft Rights Management Services directly to apply specified protection templates
- Move a document to a secure location if it is found in a place where it should not be stored

### **Microsoft Active Directory Rights Management Services (AD RMS):**

Organizations can create reliable information protection solutions using AD RMS. AD RMS allows enforcement of policies such as who can open, modify, print, forward and/or take other actions with the information. Organizations can create custom usage policy templates such as "confidential - read only" that can be applied directly to the information. With AD RMS, organizations can create persistent protection policies such as locking the usage rights within the document itself, that control how information is used even after it has been opened by the intended recipients. The RSA Data Loss Prevention Suite makes RMS protection more efficient by automatically invoking AD RMS protection templates once it identifies sensitive documents.

### **RSA Access Manager:**

RSA Access Manager is designed to enable organizations to manage large numbers of users while enforcing a centralized security policy that ensures compliance, protects enterprise resources from unauthorized access, and makes it easier for legitimate users to do their jobs. Along with other web applications, RSA Access Manager can centrally manage access to SharePoint sites. You can use this central control to override local control, but do this selectively for sites that hold highly sensitive corporate information. It is more appropriate for the information owners at the departmental or business unit level, rather than the security administrators, to determine who should have access to information. RSA Access Manager offers the following authentication and authorization capabilities.

#### *Authentication:*

Use RSA Access Manager to define different graded authentication mechanisms or multifactor authentication mechanisms based on the sensitivity of the documents. Instead of requiring a blanket authentication type for the entire site, define an authentication policy for individual documents based on the sensitivity of documents. Specifically, RSA Access Manager can invoke RSA SecurID two-factor authentication for select high-sensitivity SharePoint sites. RSA Authentication Manager is the RSA product that is required to implement RSA SecurID authentication.



### *Authorization:*

RSA Access Manager authorization policies enable organizations to define access rules at the user or group level. Administrators can define, apply and audit the access rules centrally.

### **Microsoft SharePoint native capability**

At a departmental or site collection level, SharePoint administrative consoles provide sufficient access control capabilities. RSA Secure View provides the visibility to determine where sensitive information exists and who has access to it. Using this information, departmental or business unit administrators can adjust user access policies directly in SharePoint.

The limited operating scope for the administrator of SharePoint may not effectively address policies applicable to the entire organization. For this reason, use central access management products in addition to SharePoint to control access policies.

### **Courion AccountCourier and CompliantCourier**

With the help of the Courion AccountCourier, security administrators can meaningfully weave the human resources processes and systems to user account management in several systems, including Microsoft SharePoint and Active Directory, by providing the necessary workflow management capability. The Courion ComplianceCourier product can be used by security departments to perform periodic attestation and audits of user accounts configured in SharePoint.

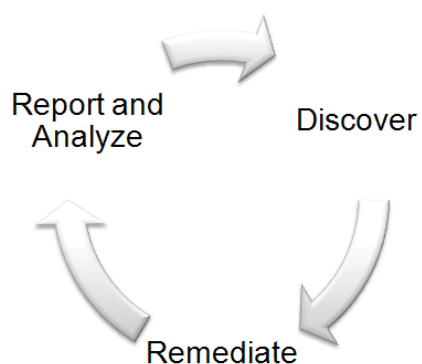
## **Reporting and Analysis**

### **RSA enVision:**

RSA enVision collects logs from various device types and enables administrators to obtain reports on security-relevant events. RSA enVision monitors events related to the discovery of sensitive information from RSA DLP. It also collects information from third-party systems that scan enterprise networks for vulnerabilities in systems and applications and has visibility into security-relevant events such as logon failures on a given server. RSA enVision administrators can reveal high risk areas in the enterprise by correlating servers that have sensitive information with servers that have vulnerabilities. This visibility helps prioritize security efforts.

### **Continuous Refinement**

Security for SharePoint is a continuous and cyclical process. Conduct discovery periodically based on the content growth rate in the organization. Launch remediation steps in response to the discovery of compliance gaps. This maintains compliance with internal and external policies. Conduct reporting and analysis regularly to monitor the compliance of the overall environment.



**Figure 5 Security: Continuous Refinement**

### Functional Summary

The following table describes the products used to implement the RSA Solution for Microsoft SharePoint and their function in the solution.

Product	Function
RSA Secure View for Microsoft SharePoint	A new tool developed by RSA for navigation of the Microsoft SharePoint resource hierarchy, discovery of user access policy in SharePoint and correlation with the RSA Data Loss Prevention data scan results to provide central visibility into the security of the Microsoft SharePoint deployment.
RSA Data Loss Prevention Datacenter	Discovery of sensitive information and enforcement of data security using direct interface with Microsoft SharePoint and Microsoft Active Directory Rights Management Services.
RSA Access Manager	Central access management for select Microsoft SharePoint sites.
RSA Authentication Manager	RSA SecurID two-factor authentication for select Microsoft SharePoint high-sensitivity sites.
RSA enVision	Reporting on where sensitive information is found and correlation with server vulnerability to help prioritize SharePoint security activities.
Courion AccountCourier and Courion Compliance Courier	Central provisioning system for provisioning, de-provisioning and attestation of user accounts in Microsoft SharePoint.

**Table 1: Products and Functional Mapping**

The following diagram shows the functional view of the SharePoint solution.

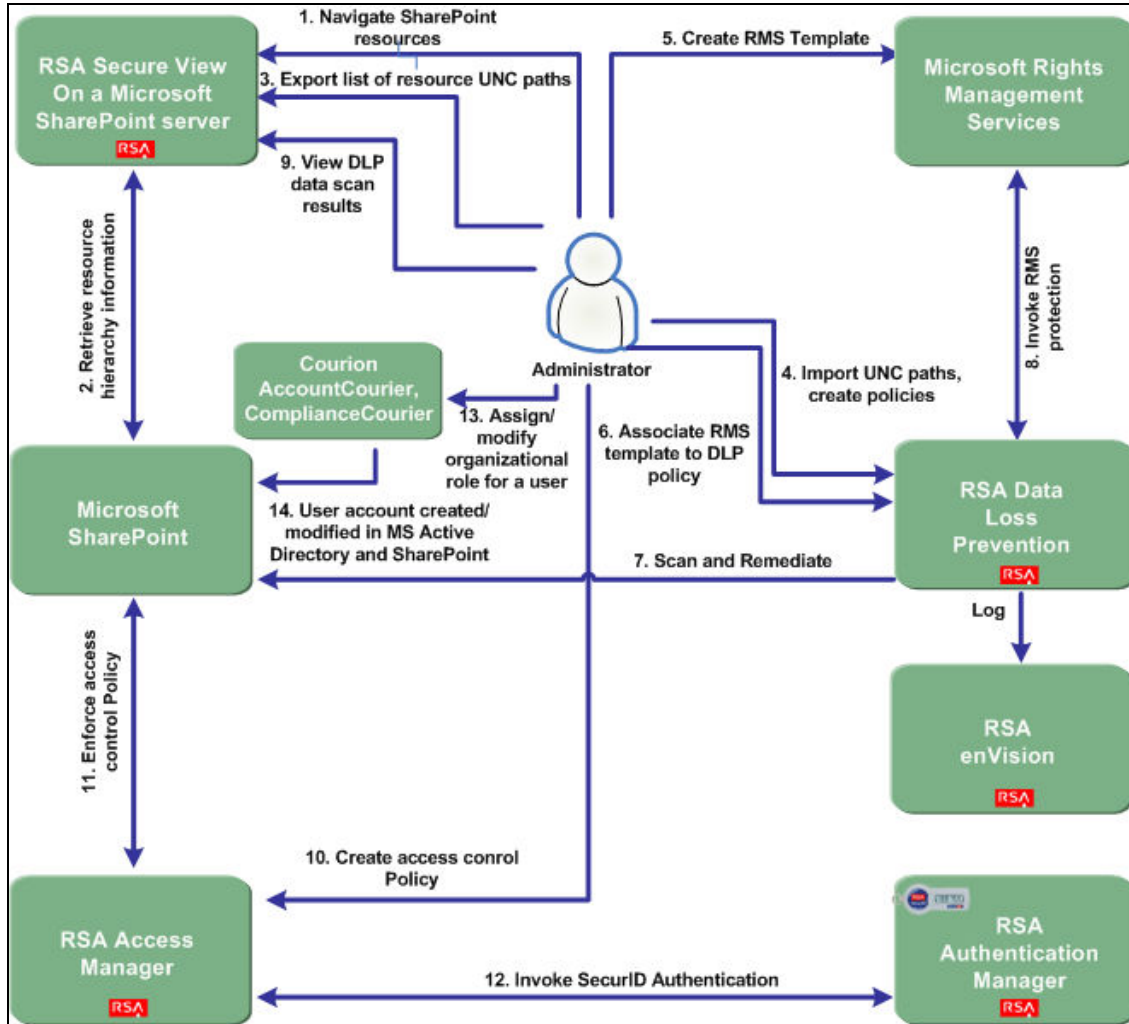


Figure 6: Functional Flow

The following list describes the steps in the previous figure.

1. The administrator logs on to RSA Secure View to navigate the various web applications, site collections, sites, and resources within a SharePoint farm.
2. RSA Secure View retrieves information using a local SharePoint interface and presents information about the entire farm in tree structure.
3. The administrator selects a few sites, folders or documents and uses the RSA Secure View option to export these resource names as UNC paths in the CSV format for ease of importing into RSA DLP.

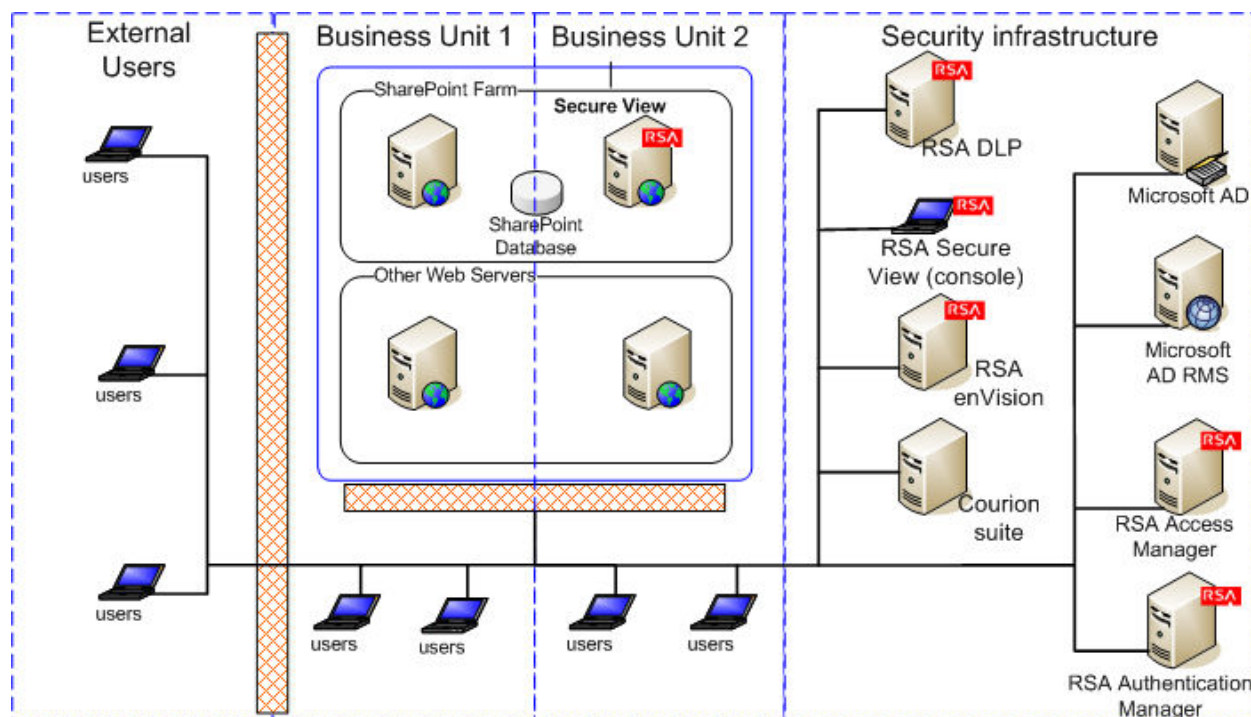


4. The administrator uses the RSA DLP Enterprise Manager console to import the UNC paths and creates the RSA DLP data scan policies.
5. The administrator configures Microsoft RMS protection templates that are used to protect specific types of sensitive content (for example, a protection template for personally identifiable information).
6. The administrator uses the RSA DLP Enterprise Manager to associate the AD RMS protection templates with select RSA DLP policies so that AD RMS protection can be applied automatically to content that RSA DLP finds sensitive (for example, RSA DLP policy 'Annual Report' could be associated with AD RMS protection template 'Financial Content').
7. The administrator schedules the scan. RSA DLP runs the scan, records the data scan results, and invokes any automated remediation that was configured.
8. If the RSA DLP policies require AD RMS protection, RSA DLP invokes AD RMS, AD RMS then applies the appropriate protection templates on the documents.
9. The administrator views the data scan results from RSA DLP directly in RSA Secure View.
10. Based on the sensitivity of the documents, one of the remediation options is that the administrator can deploy the RSA Access Manager agent on a few SharePoint servers and configure the appropriate authentication and authorization policies for selected SharePoint sites using the RSA Access Manager administrative console.
11. From this point on, all user access to the sites protected by RSA Access Manager has to conform to the configured authentication and authorization policies.
12. Optionally, the administrator configures multifactor authentication, such as RSA SecurID, for important documents such as confidential financial statements.
13. An administrator uses Courion AccountCourier to grant a user access to a specific organizational role (for example, new recruit) or to revoke/change a role (for example, employment termination or change in departments).
14. If SharePoint is configured as one of the applications that is affected by the change in the above step, CourionAccountCourier will either grant or modify SharePoint access accordingly. Further, an administrator can use Courion ComplianceCourier to periodically review and perform attestation of user accounts.
15. RSA enVision collects logs from RSA DLP related to where sensitive information was found and allows correlation with other information RSA envision, such as server vulnerability.

# Solution Deployment

## Enterprise Deployment

The following figure depicts the recommended deployment for an enterprise.



**Figure 7: Recommended Deployment**

The deployment of various components of the solution may vary based on the enterprise need. The model presented here suggests that all security applications are managed by security administrators. In some organizations, there may be a hierarchy of security administrators. For example, enterprise policies for data loss prevention and compliance monitoring may be defined at the highest levels and protection mechanisms, such as access control and rights management, may be managed by another tier of security or IT administrators.

Implement the proper network segmentation and trust zones with the help of firewalls to ensure that only the allowed protocols and trusted clients can access SharePoint.

## Supported Product Versions

The following table shows the products that are involved in the RSA Solution for SharePoint along with the version numbers.

Component Name	Release Version	Remarks
Microsoft Sharepoint	Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007	
RSA Secure View for Microsoft Sharepoint	1.0	.Net application that is to be installed on any one SharePoint server in the farm
RSA Data Loss Prevention Data Center	7.0	
RSA Access Manager	6.0.4	
RSA Authentication Manager	6.1 and 7.1	
Microsoft Active Directory	Windows 2003 and Windows 2008	
RSA enVision	4.0	Appliance
Microsoft Active Directory Rights Management System (AD RMS)	2008	
Microsoft Windows	Windows 2003 Server and Windows 2008 Server	Recommended Operating System for the entire stack is Windows 2003
Courion AccountCourier and Courion ComplianceCourier	7.70 or higher	

**Table 2 Product Versions**

## Deployment Instructions

The following deployment instructions are based on the sample environment assumed for the Macers Corp. fictional case study described in the Solution Administration section. Assume that a SharePoint farm has been created to reflect the scenario described below.

For installation of SharePoint farm please refer to related [Microsoft documentation](#).

Server	Purpose
SHAREPOINT-A.MACERS.ORG	Microsoft SharePoint Web Front End A (Windows SharePoint Services 3.0 and MOSS 2007)
SHAREPOINT-B.MACERS.ORG	Microsoft SharePoint Web Front End B, SQL Server Database (Windows SharePoint Services 3.0 and MOSS 2007)
DOMAIN-CONTROL.MACERS.ORG	Microsoft Active Directory 2003

**Table 3: SharePoint Farm Deployment**

### Deploying RSA Secure View

The RSA Secure View should be installed on any one of the servers in the SharePoint farm. For the scenario described in this document, the tool is to be setup on SHAREPOINT-A.MACERS.ORG. Transfer binaries of RSA Secure View using ftp or other means to this machine. You need to have administrative rights to the local machine or to the MS Windows domain Macers.org in order to execute the following steps.

#### Following are installation steps for the tool:

1. Run the install program “RSA Secure View.msi.”
2. Click “Next” on the dialog box
3. Select the website where RSA Secure View must be installed. You can install on any SharerPoint server, but it is recommended that you install it on the same server that hosts the SharePoint Central Administration Console. Click “Next.”

*Note: Microsoft recommends the following security measures to protect the Central Administration Console. RSA Secure View would inherit these security benefits if deployed on the same server.*

- a. Restrict access to the Central Administration site to appropriate users only.





- b. If you are enabling the Central Administration site for remote administration, secure the Central Administration site by using Secure Sockets Layer (SSL).
- c. Administrators who run deployment operations must be members of the local administrators group on the server that hosts the Central Administration site.

In the “Virtual directory” field accept the default directory or enter a new virtual directory name. This will create a virtual directory inside the website selected in the previous step.

4. Click “Next”.
5. In the “Confirm Installation” dialog box, click “Next.”
6. Once the installation is complete, click “Close.”

*Note:* For more details, review the *readme.txt* available for RSA Secure View.

### **Testing the Deployment of RSA Secure View**

Access the following URL in the browser <http://sharepoint-A.macers.org/rsa-Secure View>, login as Farm Administrator (MACERS\administrator) and you should see the home page with the SharePoint farm hierarchy on the left.

### **RSA Secure View Deployment Details**

RSA Secure View is accessed through browser by an administrator using the http/https protocol. The type of communication protocol depends on the configuration at server. RSA Secure View retrieves information from a SharePoint farm using the WSS 3.0 APIs. The information returned by the WSS API is limited by the permission level of the user credentials that the administrator uses to log in to RSA Secure View. All SharePoint components in the farm upload their configuration details in the SharePoint configuration data store which allows WSS API to return information about the entire farm to RSA Secure View.

RSA Secure View also queries the RSA DLP data store to fetch data scan results and other configuration information from RSA DLP. RSA Secure View uses an encrypted channel to connect to the RSA DLP datastore and Integrated Windows Authentication ensures secure logon to the datastore using the credentials entered by the administrator to logon to RSA Secure View.

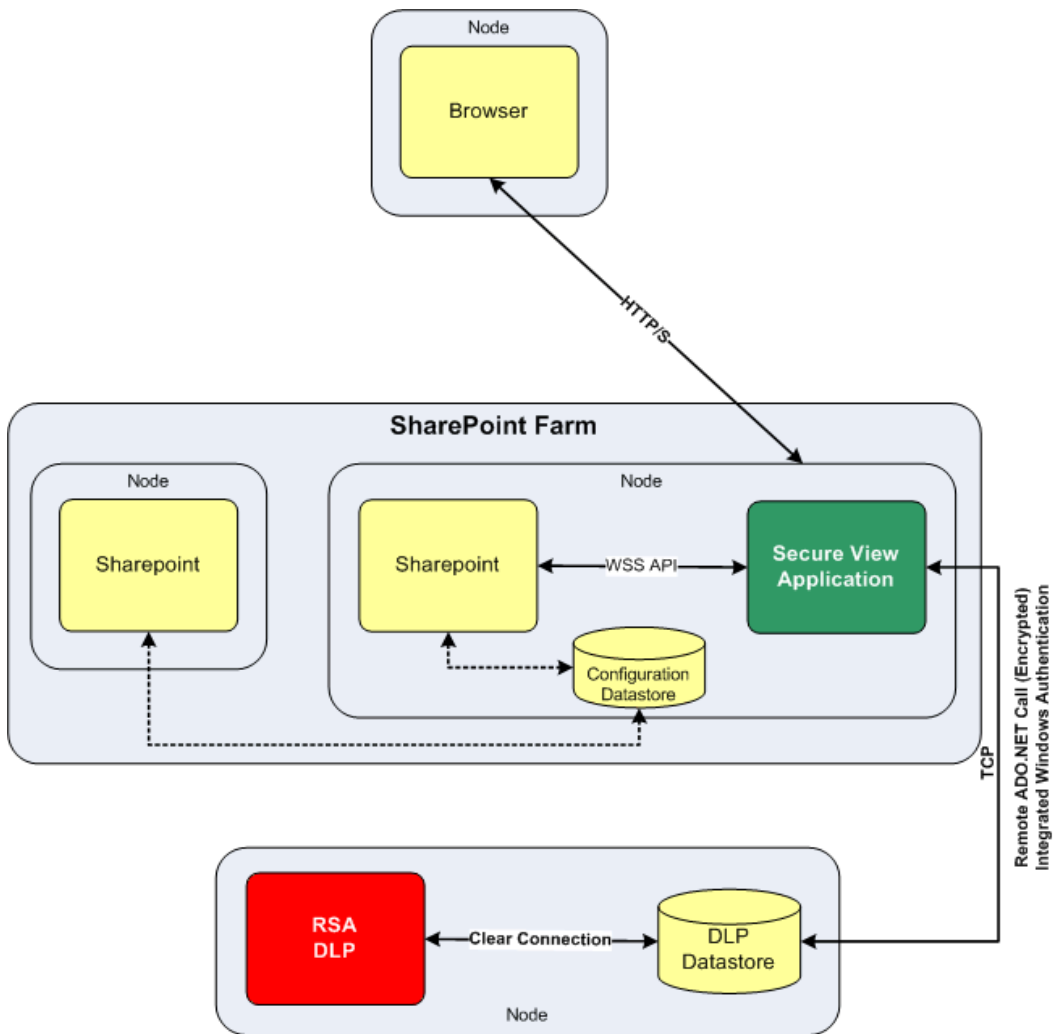


Figure 8: RSA Secure View Deployment Details

## Deploying RSA Data Loss Prevention (DLP)

Follow the installation instructions in the [RSA DLP product documentation](#) to install RSA DLP Datacenter.

As a result, RSA DLP is deployed on one system as described below.

Machine	Purpose
DLP-7.MACERS.ORG	RSA Data Loss Prevention Datacenter : Enterprise Co-ordinator and Enterprise Manager for data scanning and loss prevention

**Table 4: RSA DLP Deployment**

## Deploying Microsoft Active Directory Rights Management Service (AD RMS)

Follow the installation instructions in the related [Microsoft product documentation](#) for installing AD RMS.

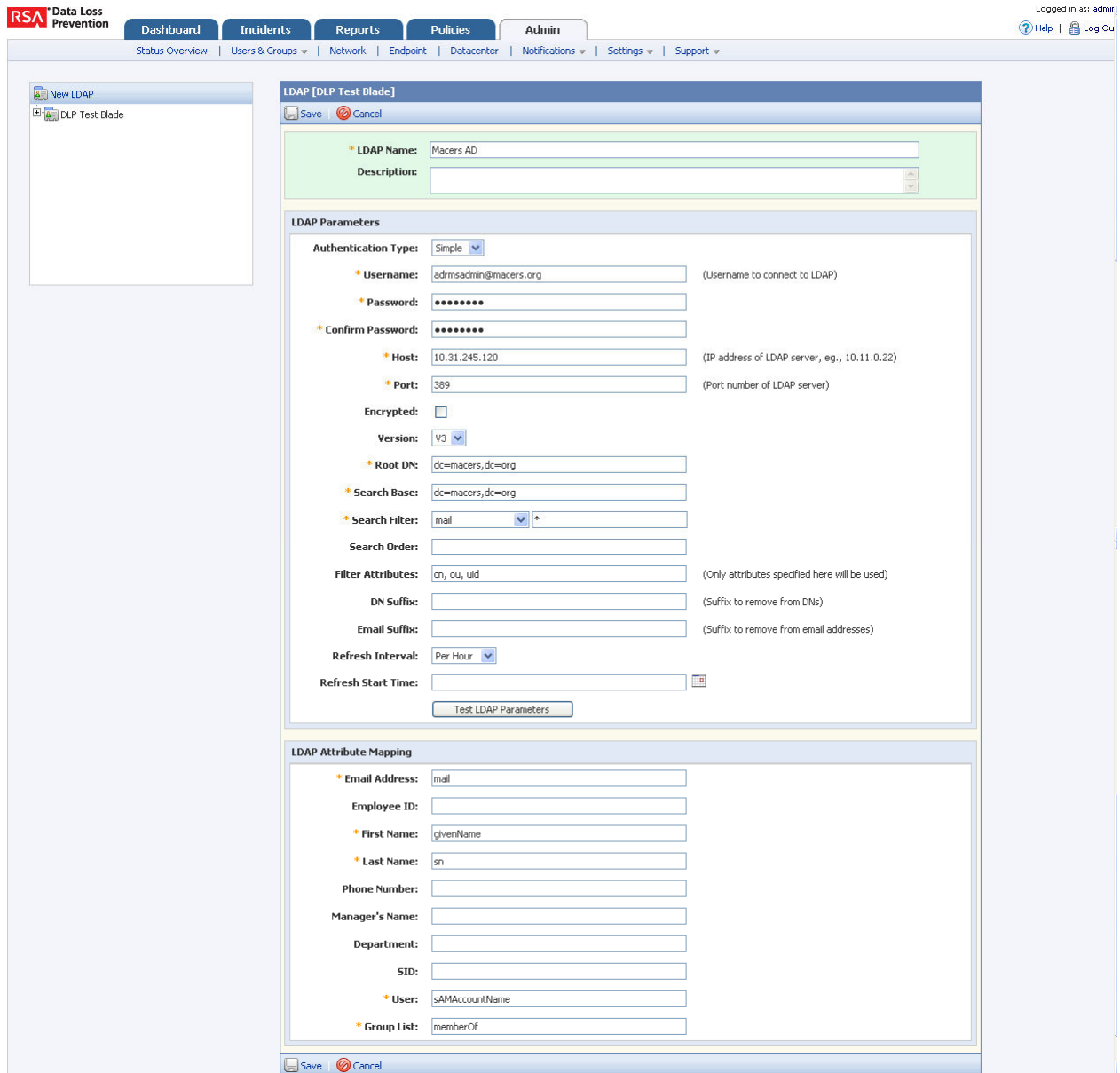
As a result, RMS is deployed on one system as described below.

Machine	Purpose
RMS.MACERS.ORG	Microsoft AD RMS for information rights management

**Table 5: RMS Deployment**

Following additional steps are required to ensure that RSA DLP can invoke AD RMS for protecting sensitive content.

1. Configure details of Active Directory within the RSA DLP Enterprise Manager console.



The screenshot shows the RSA Data Loss Prevention (DLP) configuration interface. At the top, there is a navigation bar with tabs for Dashboard, Incidents, Reports, Policies, and Admin. The Admin tab is selected. Below the navigation bar, there is a breadcrumb trail: Status Overview > Users & Groups > Network > Endpoint > Datacenter > Notifications > Settings > Support. The main content area is titled "LDAP [DLP Test Blade]" and contains a "Save" button and a "Cancel" button. The configuration is divided into three sections: 1. \*\*LDAP Name and Description\*\*: "LDAP Name" is set to "Macers AD" and "Description" is empty. 2. \*\*LDAP Parameters\*\*: This section includes fields for "Authentication Type" (Simple), "Username" (admsadmin@macers.org), "Password" (masked), "Confirm Password" (masked), "Host" (10.31.245.120), "Port" (389), "Encrypted" (checkbox), "Version" (v3), "Root DN" (dc=macers,dc=org), "Search Base" (dc=macers,dc=org), "Search Filter" (mail), "Search Order" (empty), "Filter Attributes" (cn, ou, uid), "DN Suffix" (empty), "Email Suffix" (empty), "Refresh Interval" (Per Hour), and "Refresh Start Time" (empty). A "Test LDAP Parameters" button is located at the bottom of this section. 3. \*\*LDAP Attribute Mapping\*\*: This section maps LDAP attributes to system fields: "Email Address" (mail), "Employee ID" (empty), "First Name" (givenName), "Last Name" (sn), "Phone Number" (empty), "Manager's Name" (empty), "Department" (empty), "SID" (empty), "User" (sAMAccountName), and "Group List" (memberOf). At the bottom of the form, there are "Save" and "Cancel" buttons.

Figure 9: RSA DLP Configuration Screen for Active Directory

2. Configure details of the AD RMS server in the RSA DLP Enterprise Manager console.

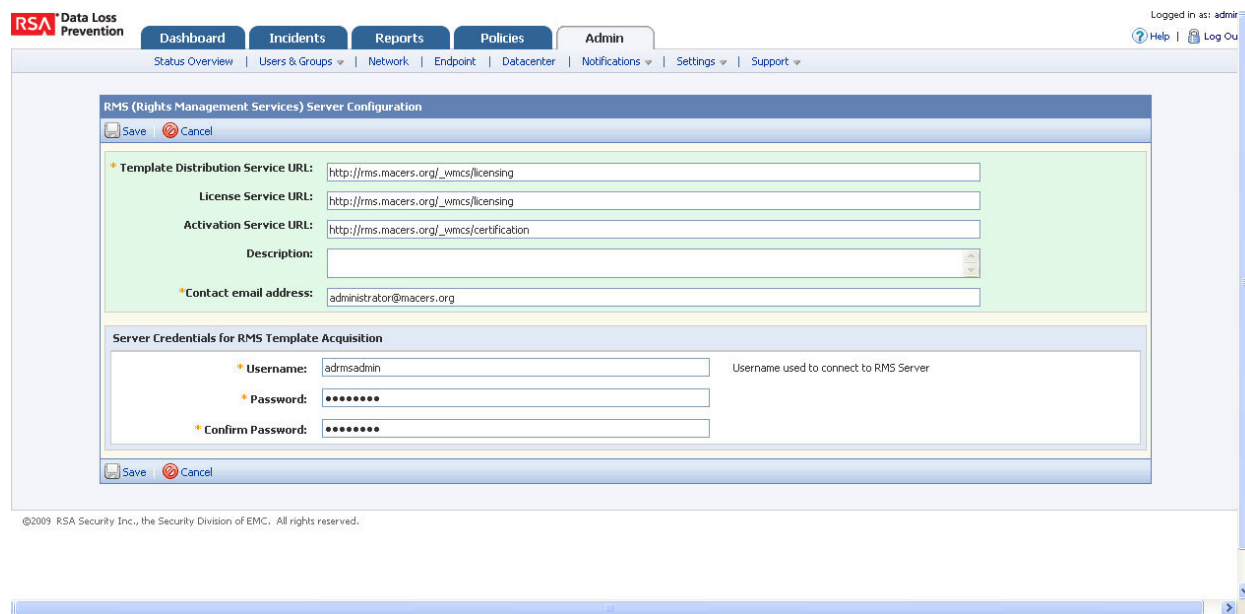


Figure 10: RSA DLP Configuration Screen for AD RMS

For detailed instructions, refer the [RSA DLP product documentation](#) (Section – Configuring Rights Management Services) and the [Information Rights Management](#) in the administration section of this document.

### Deploying RSA Authentication Manager

RSA Authentication Manager enhances native Windows security with strong, two-factor authentication based on RSA SecurID tokens.

Follow the installation instructions in the [RSA Authentication Manager product documentation](#) for your platform.

After successful installation, RSA Authentication Manager 6.1 would be deployed on one system as described below.

Machine	Purpose
AM-6.MACERS.ORG	RSA Authentication Manager 6.1 for 2-factor authentication

Table 6: RSA Authentication Manager Deployment

## Deploying RSA Access Manager

RSA Access Manager provides centralized access management for web applications in an enterprise. The RSA Access Manager agent is to be deployed on the Microsoft IIS web server instances that host the SharePoint sites for which access must be centrally controlled.

Follow the instructions for installign the RSA Access Manager [server](#) and [agent](#) in the RSA Access Manager product documentation.

As a result of the installation, RSA Access Manager would be deployed on one system as described below.

Machine	Purpose
AXM.MACERS.ORG	RSA Access Manager 6.0.4

**Table 7: RSA Access Manager Deployment**

To enable RSA Access Manager to invoke RSA SecurID authentication, please refer the “RSA SecurID Authentication” section in the RSA Access Manager [Installation and Configuration Guide](#).

For detailed instructions on configuring RSA Access Manager, please refer [Centralized Access Management](#) in the administration section of this document.

## Deploying RSA enVision

RSA enVision is a feature-rich security information event management application. It collects and analyzes log information automatically from network, security, application, operating and storage environments.

Follow the installation instructions in the RSA enVision [configuration guide](#).

Upon installation, RSA enVision 4.0 would be deployed on one system as described below.

Machine	Purpose
ENV.MACERS.ORG	RSA enVision 4.0 for monitoring and reporting on security-relevant events

**Table 8: Solutions enVision System Details**

### Configuring RSA DLP to log events to RSA enVision

1. Log on to RSA DLP Enterprise Manager. Click the “Admin” Tab on the top bar. Next click the “SIEM Configuration” under the settings tab which is just below the top bar.



2. Enter RSA enVision IP address in the SIEM configuration and save the settings.
3. Ensure all the RSA envision services are started in the envision system. Log on to RSA enVision and check the Event Viewer for messages from the newly recognized RSA DLP device.

### **Configuration for SharePoint servers Windows logs and enVision**

1. Log on to the RSA enVision administration console and click the System Configuration tab.
2. Select “Services”, then ‘Device Services’ and finally “Windows Service”.
3. Inside “Windows Service” click “Manage Windows Services”.
4. Click “Add” (bottom bar). Next, a window would open to configure the new Windows device to send its logs to RSA enVision. Configure the IP addresses of the SharePoint servers and the type of logs (System/Application/Security) and click “Apply”.
5. The RSA enVision Windows service would automatically restart after this step and RSA enVision would be ready to read logs from the new device.

### **Configuration of VAM**

Please refer the online help available in the RSA enVision administration console for configuring Vulnerability Asset Management (VAM) to ensure that RSA enVision is able to capture vulnerability data on the servers that SharePoint.

### **Deploying Courion AccountCourier and ComplianceCourier**

Please refer the following Courion product documents – ‘Installing the Enterprise Provisioning Suite’ and ‘Creating Workflows with the Enterprise Provisioning Suite Administration Manager’.

## Solution Administration

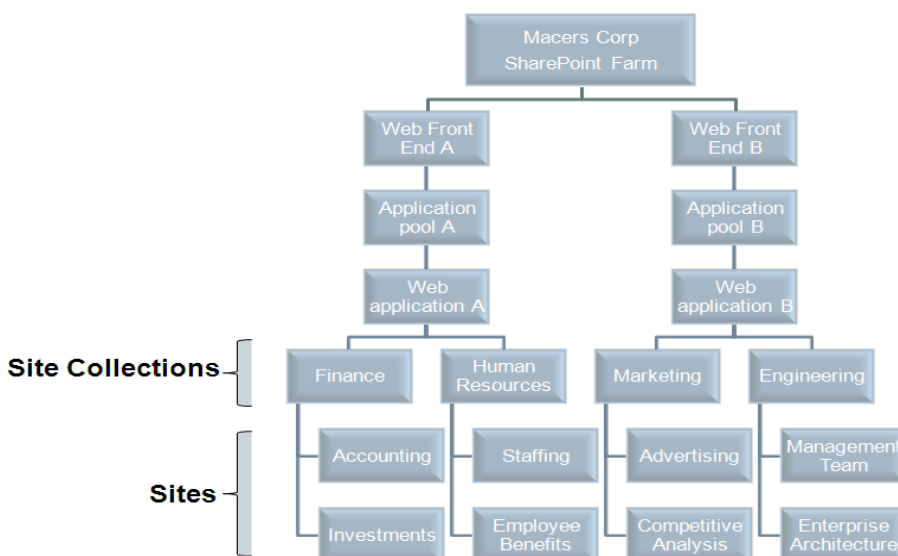
Having deployed one or more of the component products, an administrator can use the RSA Solution for Microsoft SharePoint to support the set of business scenarios and fulfill the related functional requirements described in the *Solution Objectives* section (summarized in [Figure 2](#)).

### Introducing Macers Corporation

To illustrate the operation of the solution clearly, the product-related workflows are described within the context of a fictional company, *Macers Corporation*. The example of Macers Corp. is intended to be generic and the scenarios painted in this section should resonate with many organizations.

#### SharePoint Resource Hierarchy

Macers Corporation uses Microsoft Office SharePoint Server 2007.



**Figure 11: SharePoint Hierarchy for Macers Corporation**

At Macers Corporation:

SharePoint site collections are used for four major departments: Finance, Human Resources, Marketing and Engineering.

- Each site collection contains other sites used for specific teams and functional objectives.



- The sites contain a variety of shared resources in the form of Microsoft Office documents as well as other common types of data.
- Microsoft Active Directory (AD) is the primary user directory. User groups in Active Directory map directly to functional groups with the same name, for example, Finance department maps directly to the Active Directory group Finance.

The following tables summarize the Macers Corporation SharePoint site hierarchy. They show the site collections and sites, a representation of folders and files within some sites, and the Active Directory users and user groups.

Site Collections				
Sites	Finance	Human Resources	Marketing	Engineering
	Accounting	Staffing	Advertising	Management Team
	Investments	Employee Benefits	Competitive Analysis	Enterprise Architecture

**Table 9: Macers Site Collections and Sites**

Site: Accounting	Site: Staffing	Site: Employee Benefits	Management Team
<u>Folder:</u> Financial Statements <u>Files:</u> Q1Draft.xls, Receivables.xls	<u>Folder:</u> 2009 <u>Files:</u> OpenReqs.doc, Q3Action.xls, CommunicationGuide.ppt	<u>Folder:</u> Medical <u>Files:</u> BulkEnrollment.xls	<u>Folder:</u> Q3Plan <u>Files:</u> CommunicationGuide.ppt
<u>Folder:</u> Budget <u>Files:</u> Budget09.xls, MngmtReview.ppt, BulkEnrollment.xls	<u>Folder:</u> Payroll <u>Files:</u> March09Payroll.xls, AnnualReview.doc	<u>Folder:</u> Employee Discounts <u>Files:</u> VendorList.xls	<u>Folder:</u> OrgChart <u>Files:</u> Q109.ppt

**Table 10: Example Folders and Files**



Active Directory User Group	Active Directory Users
Finance	User1, User2
Human Resources	User3, User4
Marketing Management	User5, User6
Engineering Management	User7, User8
Executive Management	UserA, UserB
SharePoint Administrators	AdminA, AdminB

**Table 11: Users and User Groups**

## Macers Corporation Security Scenarios

At Macers Corporation, the use of SharePoint originated at the departmental level with document sharing and collaboration as primary drivers. Over the last two years, the use of SharePoint for sharing information across departments has spread rapidly, creating scenarios that call for central oversight and governance of security of information within SharePoint. Some of these scenarios are described below.

- It is common practice for departmental SharePoint administrators to grant access to various sites to everyone in the corporate Active Directory. While this eases collaboration, it increases the probability that sensitive information becomes accessible to unauthorized persons within the company. Manual audits of access control configuration are not feasible given the large number of sites. A technology solution that flags non-compliant sites is required.
- The Human Resources team shares information regarding employee headcount plans with managers of other departments such as Engineering and Marketing. While such information sharing is necessary, wider distribution of such sensitive information has resulted in a recent incident in which a print copy of draft head count reduction plans was left unattended. This led to low morale and affected productivity of the organization. Security training programs have not been very effective in preventing such confidentiality breaches. A technology solution is required to complement the training program.
- Macers Corporation has to comply with regulations related to protection of personally identifiable information. It is imperative that users in the Human Resources group are the only ones that can access personally identifiable information of employees.



- Macers Corporation is a publicly traded company with its stock traded actively on a major stock exchange. In the past, lack of sufficient control over access to pre-release quarterly financial statements has resulted in an inadvertent data leak that adversely affected the Macers stock. In addition to loss of stock value, Macers was subjected to regulatory action as a result of this data leak. Strict access control over these documents is required.
- Macers has seen rapid staff growth (new hires, acquisitions) over the last few years and very recently, rapid staff reduction on account of the volatile global economy. Such change is expected to continue. It is increasingly difficult to ensure that employees are granted access to the correct Active Directory user groups and that their group memberships are modified or terminated as employees change roles or leaves the company. This could result in incorrect privileges in SharePoint because SharePoint access is linked to Active Directory group membership. An efficient process and tools are required to manage this situation.

The information security and compliance department of Macers Corporation under direction from the Chief Security Officer and Chief Information Officer has carefully assessed the situation and has chosen the RSA Solution for Microsoft SharePoint to mitigate the risks outlined above. The RSA Solution for Microsoft SharePoint will be used to remediate policy violations with the following actions:

- Ensure that SharePoint is configured as follows.
  - Only the Human Resources user group in Active Directory can access the Staffing site.
  - Only the Engineering user group in Active Directory can access the Management Team site
  - Only the Marketing user group in Active Directory can access the Marketing site collection
- Apply Microsoft Rights Management Services protection to content related to the headcount action planned in Q3 2009. By applying this protection, no one will be able to print or download such content (e.g. Q3Action.xls, CommunicationGuide.ppt) except the Human Resources user group in Active Directory.
- If content that contains personally identifiable information is found anywhere, it should be moved to its appropriate location. For example, content that contains personally identifiable information (e.g. BulkEnrollment.xls) for the purpose of medical insurance enrollment should only exist in the Employee Benefits site.
- Centralize access management for the Accounting site within RSA Access Manager so that the site can only be accessed by the Finance and Executive Management user groups in Active Directory after RSA SecurID 2-factor authentication.
- Ensure that the user's SharePoint privileges change appropriately when the user changes his or her role in the organization.

The rest of this section describes in detail how the RSA Solution for Microsoft SharePoint is used by the Macers information security department to achieve the above objectives.

## Administering the RSA Solution for Microsoft SharePoint

This section describes how a central security administrator within the Macers Corporation administers the RSA Solution for Microsoft SharePoint to achieve the functional requirements described in the Solution Objectives section and the specific scenarios described earlier in this section. A step-by-step workflow is described along with screenshots to demonstrate how each objective is achieved.

### Discover the SharePoint Resource Hierarchy

#### Products Required: RSA Secure View

1. Run RSA Secure View to discover and display the resource hierarchy of the SharePoint farm.
3. Expand a few sites to view the sites within and the resources within the sites as desired. Avoid using the ‘Expand All’ option as it can take a long time to fetch the results from SharePoint. Also, such an exhaustive display of all resources is rarely useful or meaningful. Instead, security administrators are likely to investigate a few interesting branches of the resource tree at a time.

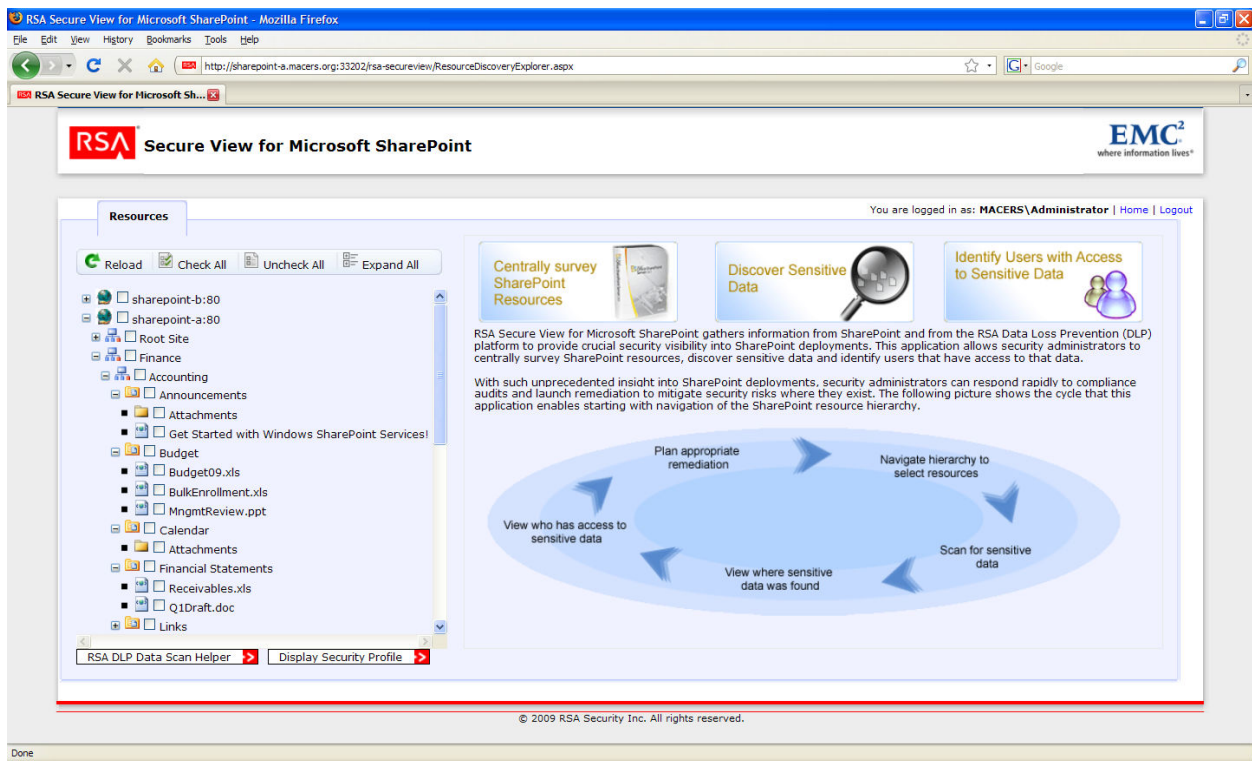


Figure 12: SharePoint Farm Hierarchy View

## Discover Sensitive Data

### Products Required: RSA Secure View, RSA Data Loss Prevention

1. Using RSA Secure View, navigate the resource hierarchy for the SharePoint farm.
2. Select the sites you want to scan for sensitive information and click the **RSA DLP Data Scan Helper** option in RSA Secure View. The results indicate whether DLP is configured to scan the selected resources and also the resource identifiers in the UNC format expected by RSA Data Loss Prevention product. Click on **Export** to export the UNC information as a CSV file using RSA Secure View.

*Note: Only resource identifiers for resources that have not been configured for scanning in RSA DLP will be exported by RSA Secure View as would be expected.*

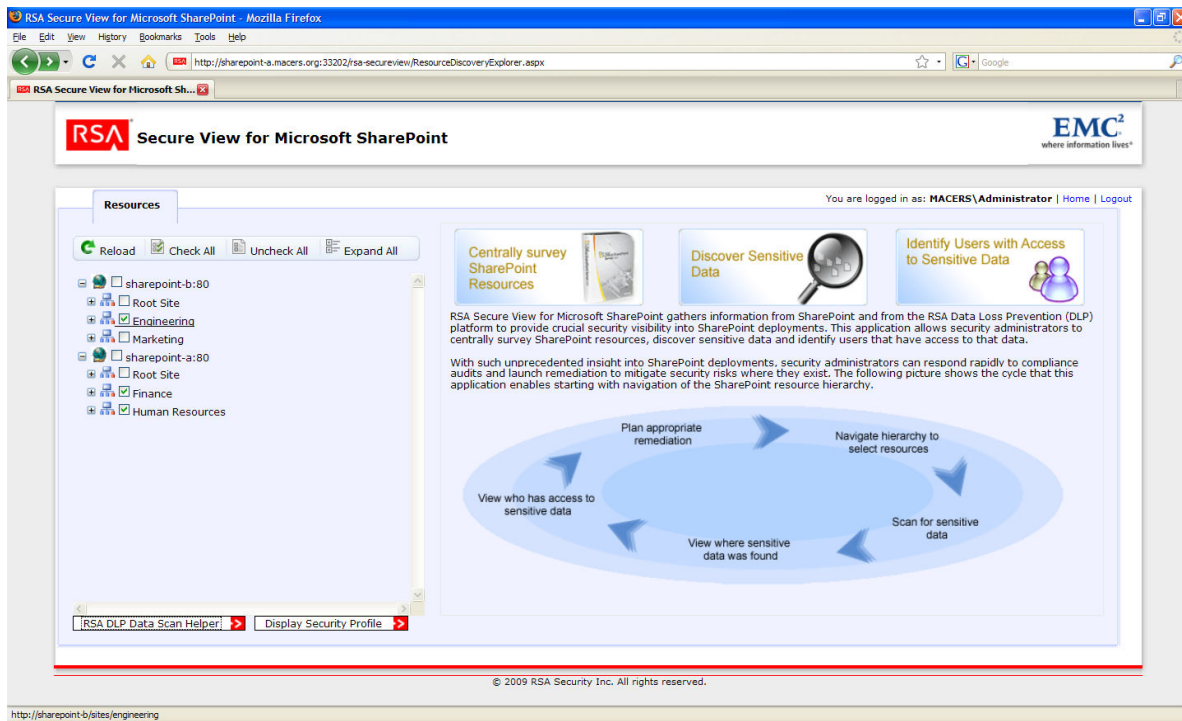


Figure 13: Sites Selected for Scan

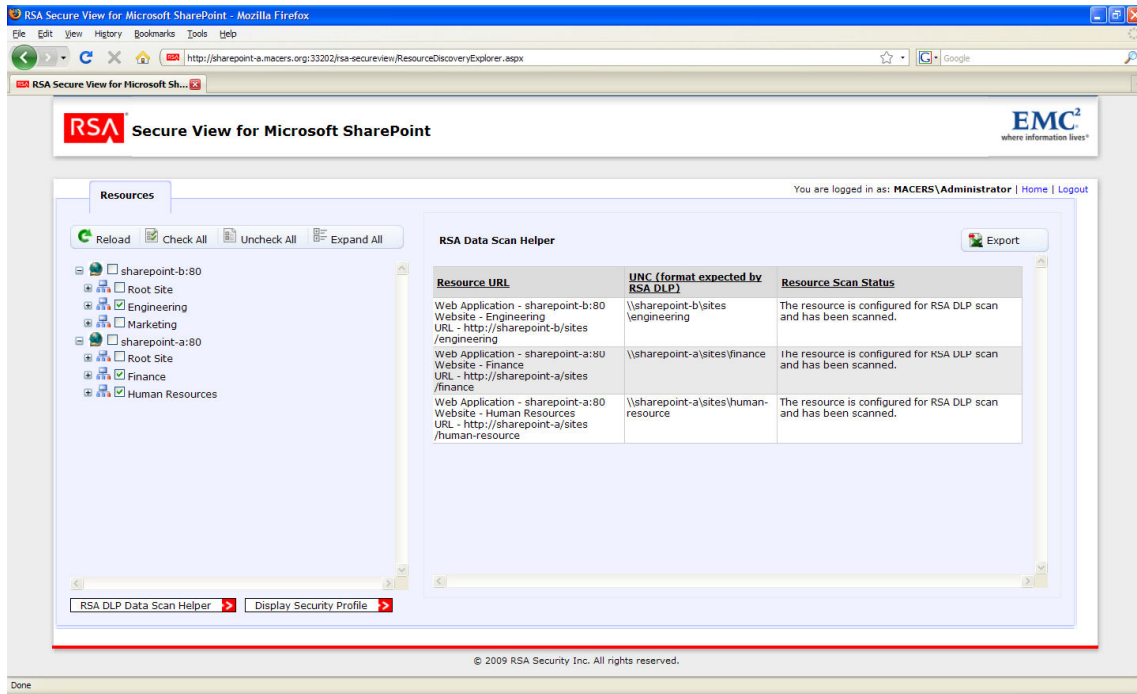


Figure 14: DLP Configuration Status and UNC Paths

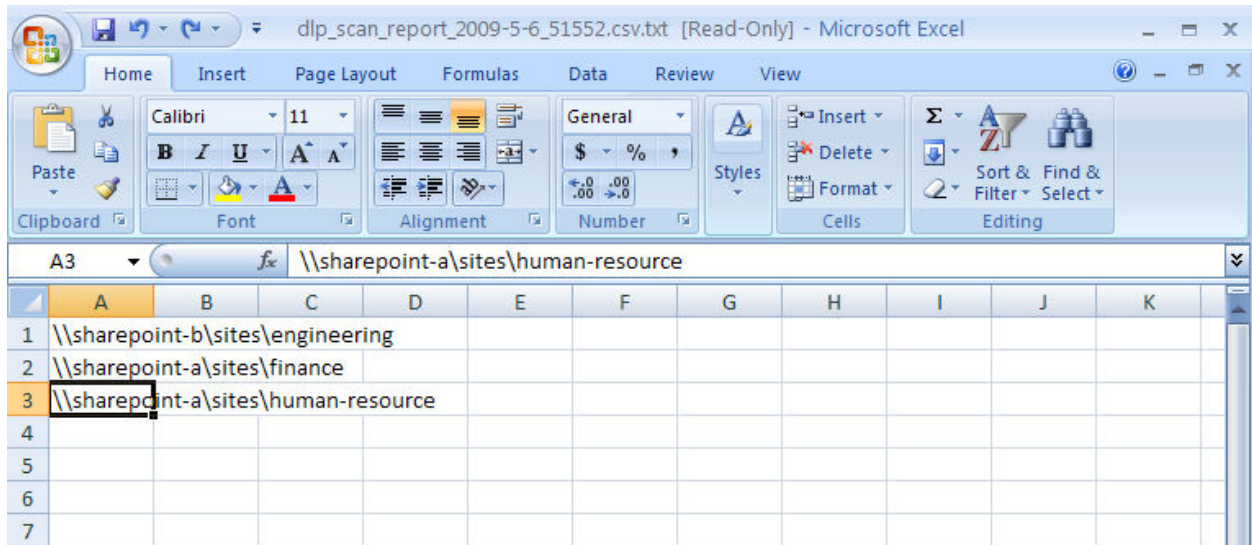


Figure 15: Exported UNC paths in CSV format

3. Configure RSA Data Loss Prevention product to scan for sensitive content.

- a. Import resource UNC information from CSV file generated by RSA Secure View into the RSA Data Loss Prevention product. This feature can be found on the grid group configuration page within Enterprise Manager.

*Note: RSA DLP must be configured to scan the SharePoint instances as file shares (configure a Grid Group instead of Repository Group) in order for the resource import from CSV file to work.*

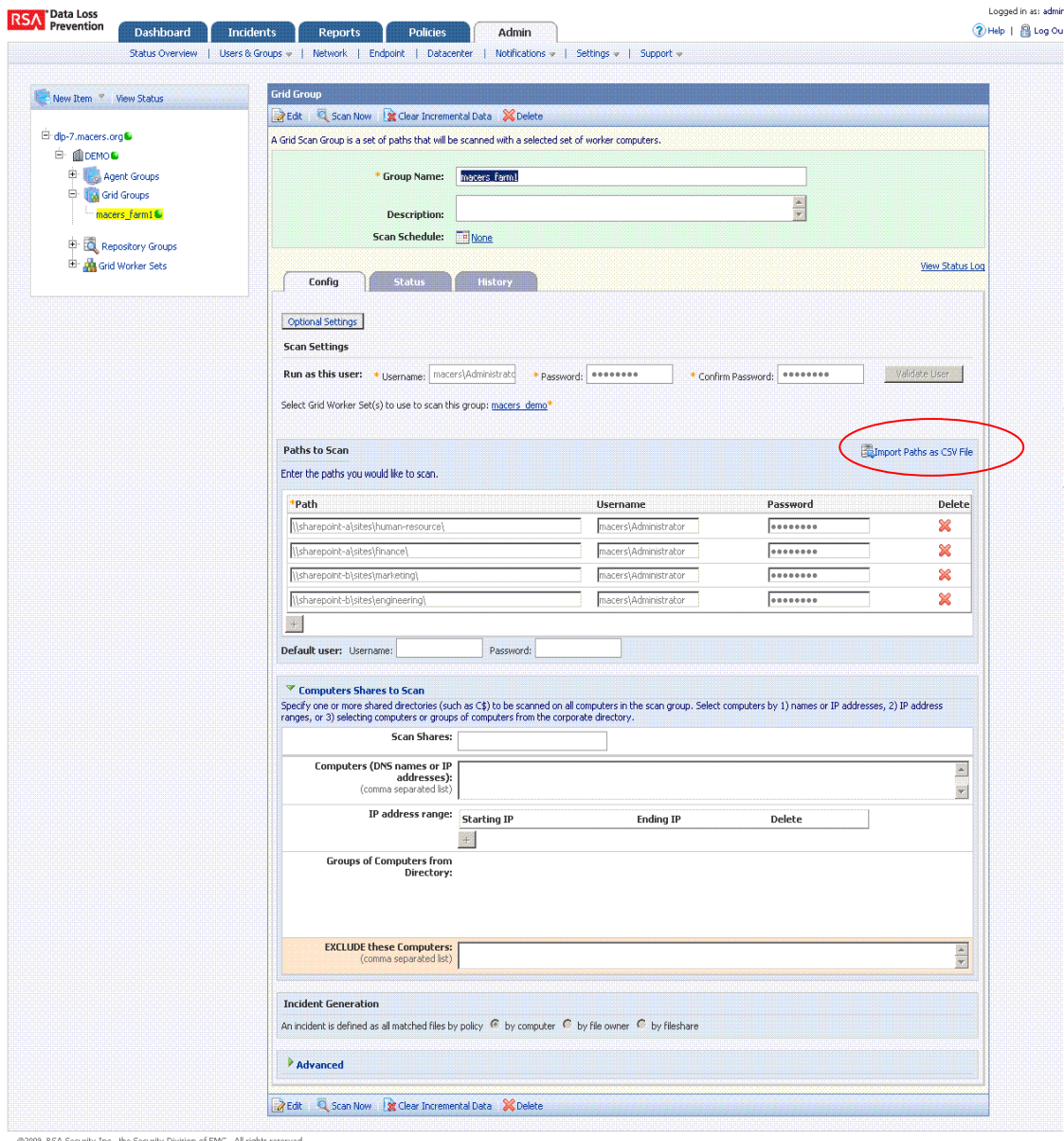


Figure 16: Imported UNC paths in DLP Enterprise Manager

- b. Select (or create new) RSA DLP Content Blades and RSA DLP Policies using the RSA DLP Enterprise Manager interface to protect personally identifiable information, company internal information, such as head count reduction plans, and draft financial statements.
  - i. Start a new policy.
  - ii. Select or create a content blade for the target data class or type (e.g. select *US Social Security Number* content blade for the Personally Identifiable Information policy, a custom blade for financial statements called *Draft Financial Statements*, and a custom blade for head count reduction plans called *Company Internal*).

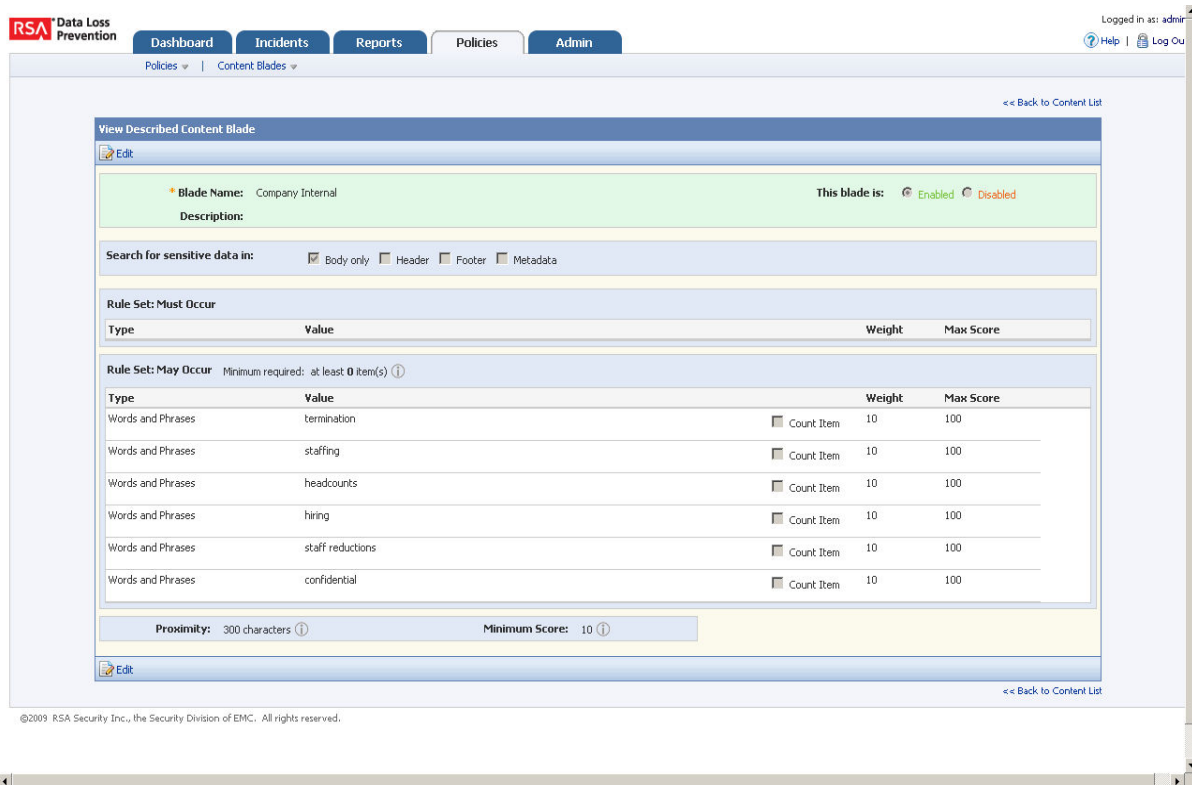


Figure 17: *Company Internal* policy in RSA DLP using *Company Internal* content blade



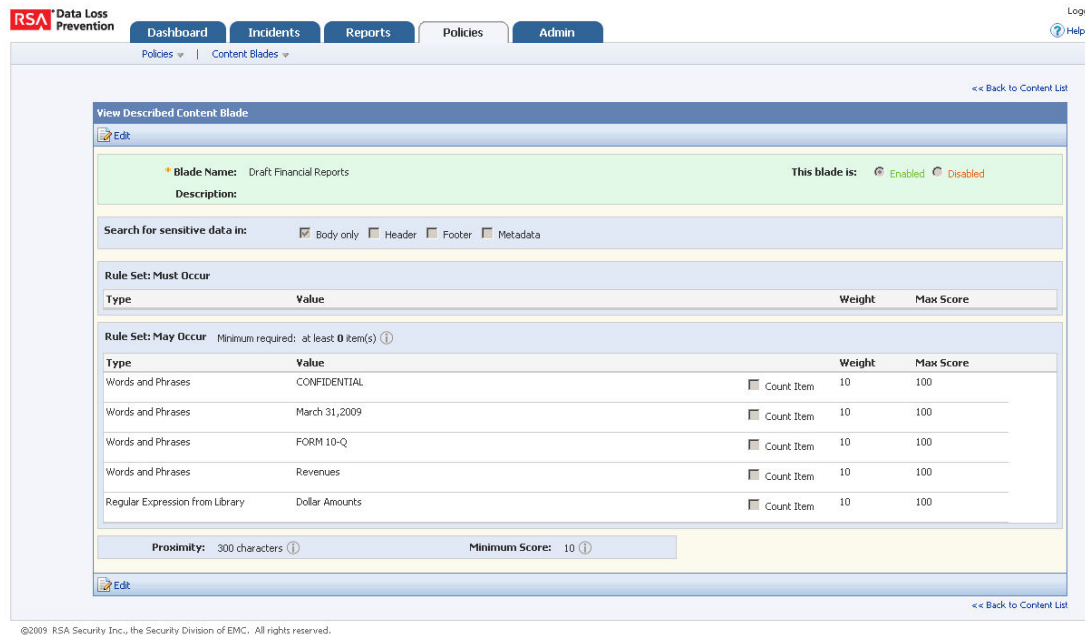


Figure 18: *Draft Financial Reports* Policy in RSA DLP using *Draft Financial Reports* Content Blade

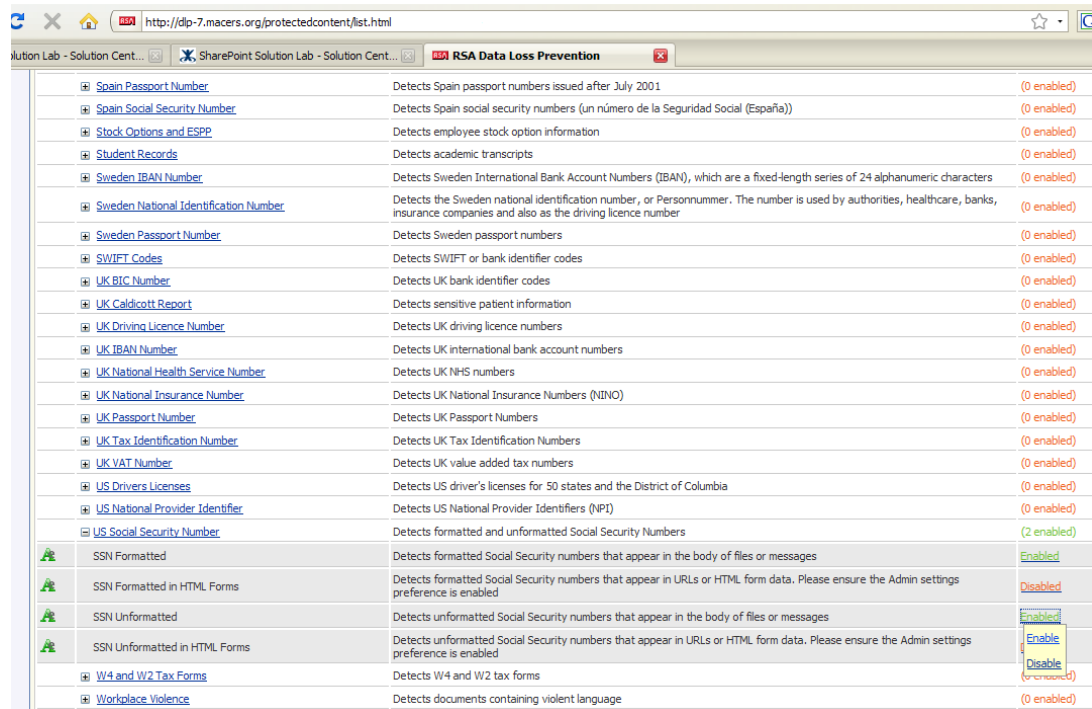


Figure 19: *Personally Identifiable Information* policy in DLP using *US Social Security Number* content blade.

- Run a RSA DLP scan on the target sites. Upon completion of the scan, a list of SharePoint resources that match the configured scan is collected by RSA DLP and reported as Incidents within RSA DLP. These results can subsequently be seen within the RSA Secure View console.

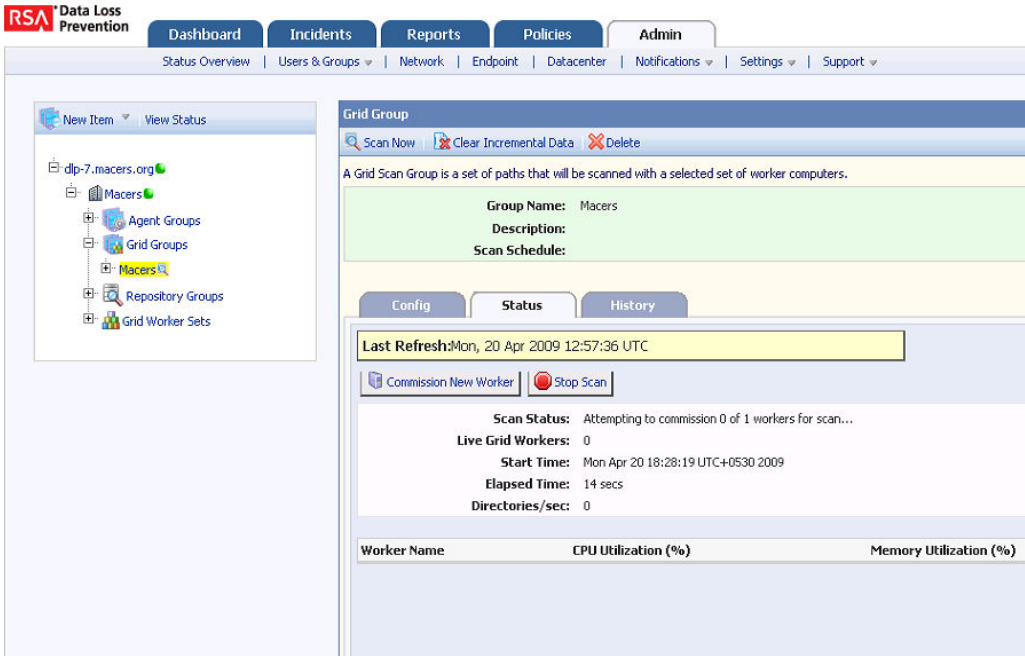


Figure 20: Start of DLP Scan

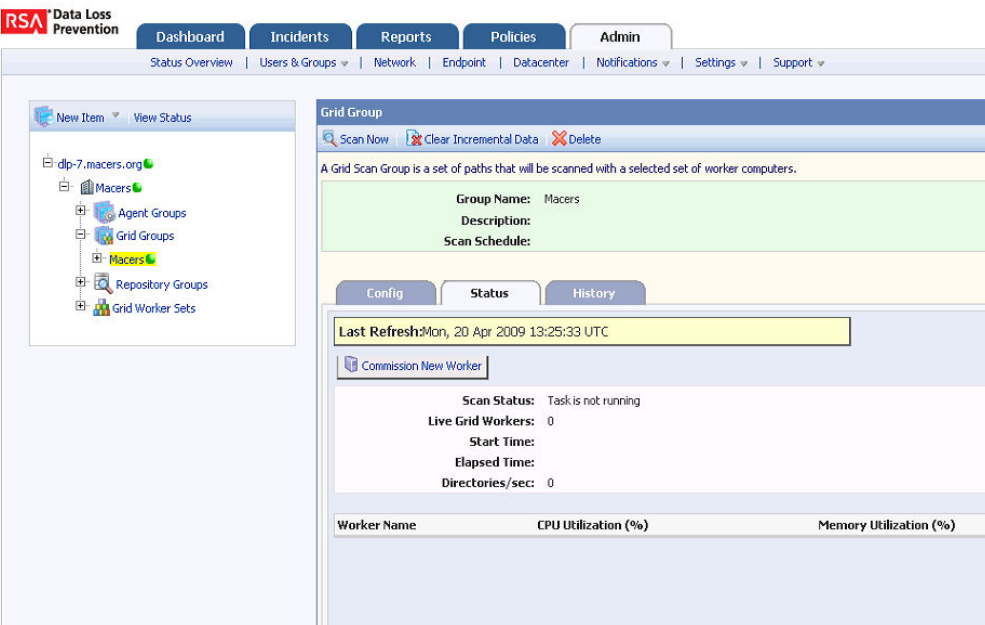


Figure 21: End of DLP scan

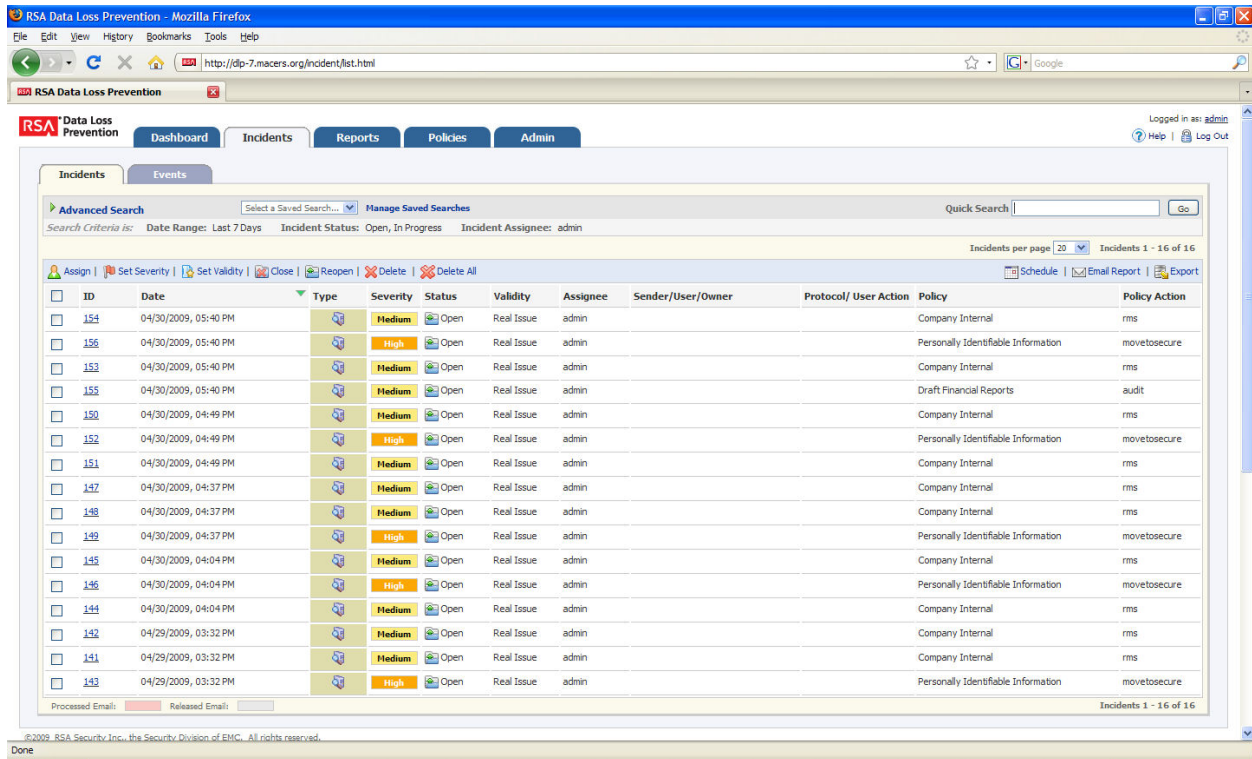
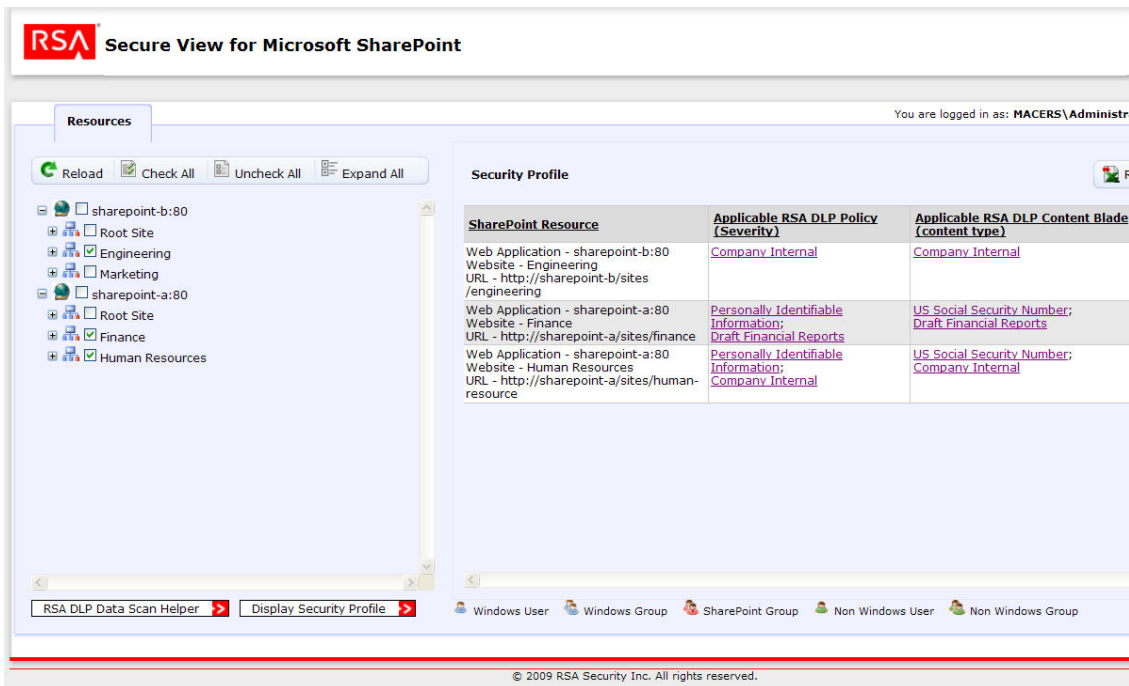


Figure 22: Incidents from the DLP Scan

- After the RSA DLP scan has been completed, open RSA Secure View and select the site collections, sites, or folders for which to view the RSA DLP data scan results, and click **Display Security Profile**. Select the option to view the RSA DLP data scan results for selected resources. In the resulting table, clicking on the policy and content blade matches on selected folders will cause Secure View to identify the sensitive information that exists deeper within the SharePoint hierarchy. Using this capability, a security administrator can rapidly identify the high level branches in the hierarchy as well as resources deep in the hierarchy that have sensitive data.



**Resources**

Reload Check All Uncheck All Expand All

sharepoint-b:80  
 Root Site  
 Engineering  
 Marketing  
 sharepoint-a:80  
 Root Site  
 Finance  
 Human Resources

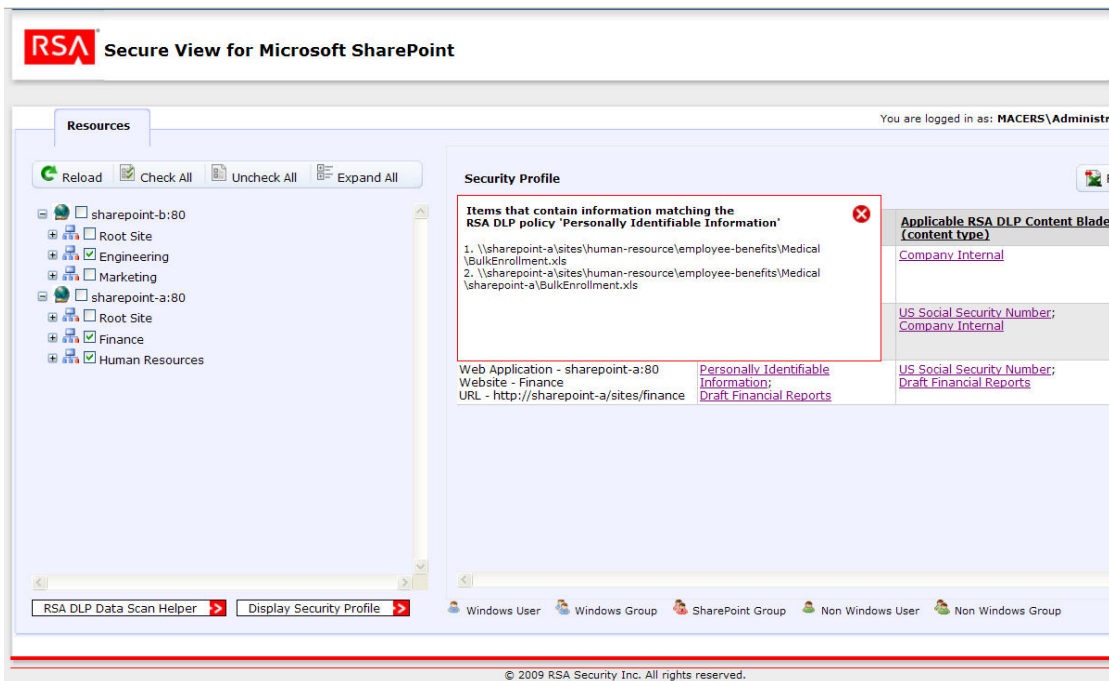
**Security Profile**

SharePoint Resource	Applicable RSA DLP Policy (Severity)	Applicable RSA DLP Content Blade (content type)
Web Application - sharepoint-b:80 Website - Engineering URL - http://sharepoint-b/sites/engineering	Company Internal	Company Internal
Web Application - sharepoint-a:80 Website - Finance URL - http://sharepoint-a/sites/finance	Personally Identifiable Information; Draft Financial Reports	US Social Security Number; Draft Financial Reports
Web Application - sharepoint-a:80 Website - Human Resources URL - http://sharepoint-a/sites/human-resource	Personally Identifiable Information; Company Internal	US Social Security Number; Company Internal

RSA DLP Data Scan Helper Display Security Profile

Windows User Windows Group SharePoint Group Non Windows User Non Windows Group

© 2009 RSA Security Inc. All rights reserved.



**Resources**

Reload Check All Uncheck All Expand All

sharepoint-b:80  
 Root Site  
 Engineering  
 Marketing  
 sharepoint-a:80  
 Root Site  
 Finance  
 Human Resources

**Security Profile**

**Items that contain information matching the RSA DLP policy 'Personally Identifiable Information'**

- \\sharepoint-a/sites/human-resource/employee-benefits/Medical/BulkEnrollment.xls
- \\sharepoint-a/sites/human-resource/employee-benefits/Medical/\\sharepoint-a/BulkEnrollment.xls

Web Application - sharepoint-a:80  
 Website - Finance  
 URL - http://sharepoint-a/sites/finance

Personally Identifiable Information;  
 Draft Financial Reports

US Social Security Number;  
 Draft Financial Reports

Applicable RSA DLP Content Blade (content type)  
 Company Internal

US Social Security Number;  
 Company Internal

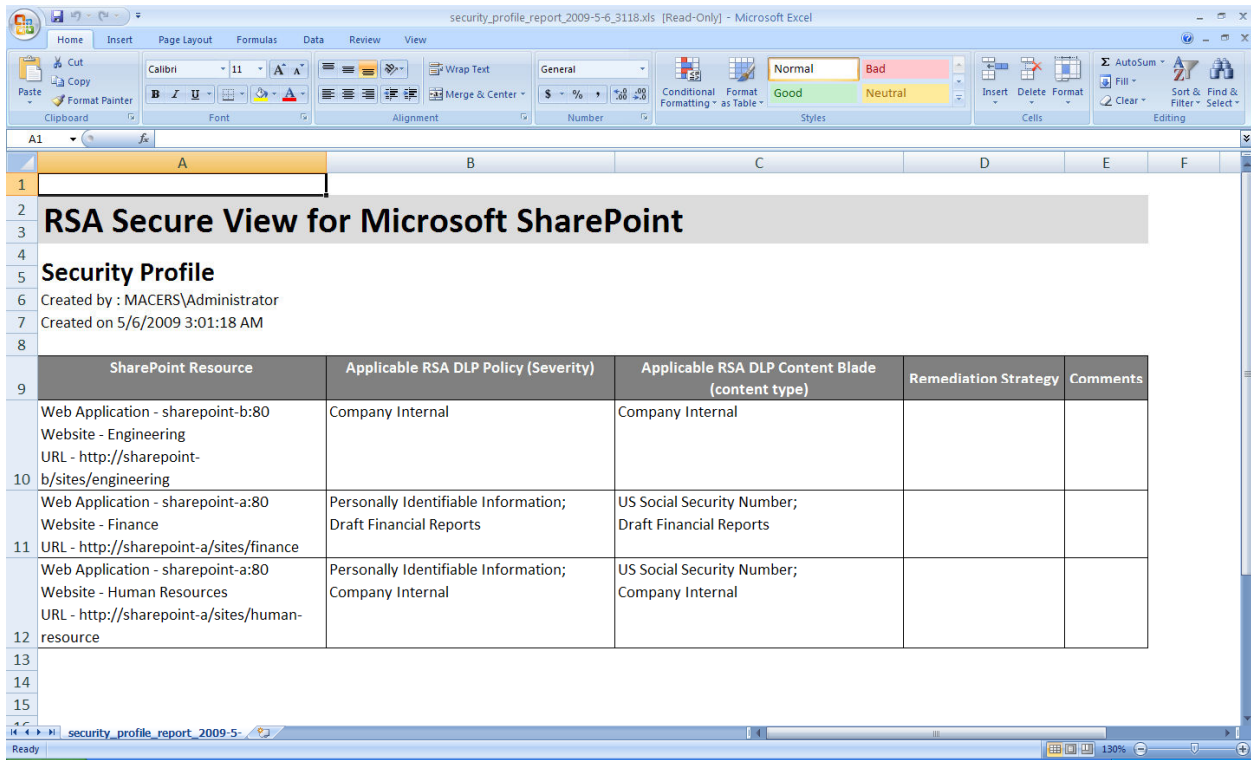
RSA DLP Data Scan Helper Display Security Profile

Windows User Windows Group SharePoint Group Non Windows User Non Windows Group

© 2009 RSA Security Inc. All rights reserved.

Figure 23: Data scan results for few sites and a view of deeply nested sensitive information

- Click on “Report” in the Secure View window to export the resulting RSA DLP scan results in the Microsoft Excel format, showing the sites, resources, and matched RSA DLP policies and content blades. Such a report can be used by the security department to initiate security-relevant conversations with business units that own the information and manage the individual SharePoint sites.



SharePoint Resource	Applicable RSA DLP Policy (Severity)	Applicable RSA DLP Content Blade (content type)	Remediation Strategy	Comments
Web Application - sharepoint-b:80 Website - Engineering URL - http://sharepoint-b/sites/engineering	Company Internal	Company Internal		
Web Application - sharepoint-a:80 Website - Finance URL - http://sharepoint-a/sites/finance	Personally Identifiable Information; Draft Financial Reports	US Social Security Number; Draft Financial Reports		
Web Application - sharepoint-a:80 Website - Human Resources URL - http://sharepoint-a/sites/human-resource	Personally Identifiable Information; Company Internal	US Social Security Number; Company Internal		

Figure 24: Data Scan Result Exported to Excel

## Correlate User Access with Data Sensitivity

### Products Required: RSA Secure View

1. Use RSA Secure View to view the SharePoint hierarchy.
2. Select the sites for which you want to view user access configuration in SharePoint. *To narrow the discovery to only those sites with sensitive data, refer to the “Discover Sensitive Data” workflow in this section.*
3. Click **Display Security Profile**, and select the options to view both, which users have access to selected sites and which resources have sensitive data. The result is a table that shows the Active Directory users and user groups that have been provisioned to the selected SharePoint resources. This correlated information can also be captured in a report by clicking on the **Report** button.

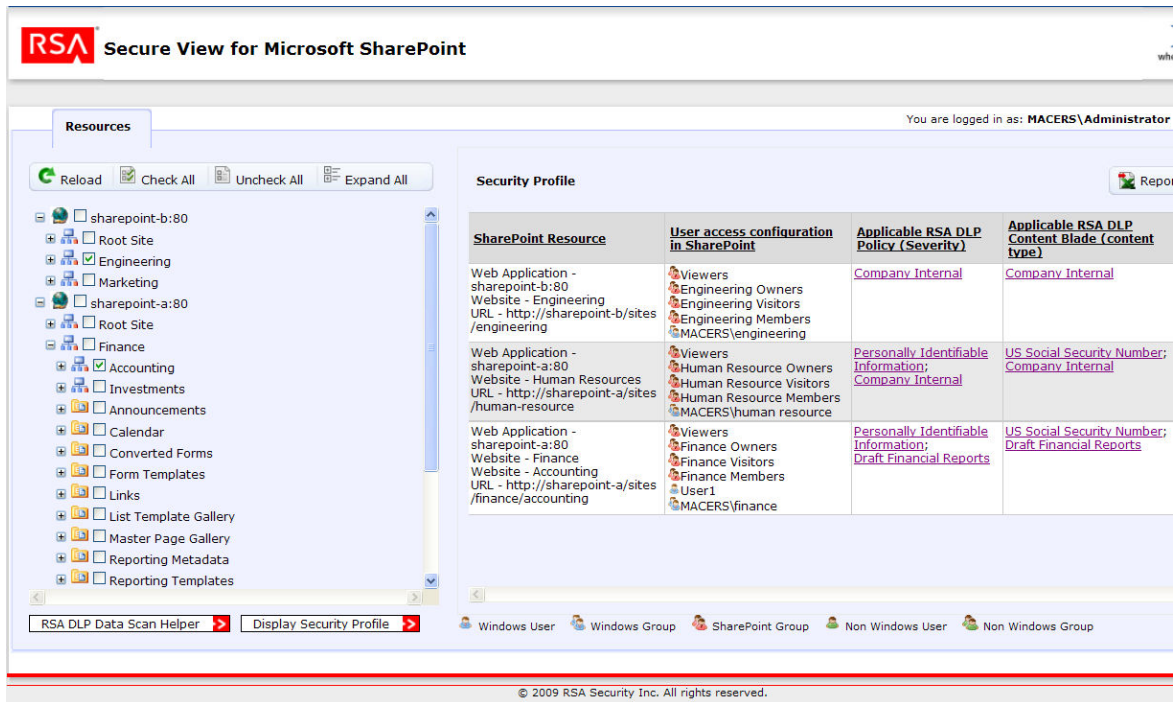


Figure 25: Correlated View

## Correlate Sensitive Data with Server Vulnerability

### Products Required: RSA Data Loss Prevention, RSA enVision

RSA enVision provides central visibility into RSA DLP incidents related to sensitive data discovery and into vulnerability of servers that host SharePoint. By correlating the two, security administrators can prioritize their security efforts.

### Sensitive Data Alert

A 'Sensitive Data' alert can be triggered when RSA DLP identifies sensitive documents and records them in the RSA DLP database. If configured, RSA DLP sends these incidents in the form of events to RSA enVision. RSA enVision can be configured to generate alerts for different content blades defined in RSA DLP such as "PCI", "PII" etc.

1. Log on to the RSA enVision administrative console.
2. Click the *'Alerts'* tab on enVision top bar. Next select *'Alert Configuration'*, then *'Correlated Alerts'* and finally *'Manage Correlation Rules'*. This would populate the various correlation rules in enVision.
3. Click *'Add'* tab at the bottom of the *'Manage Correlation Rules'* screen.
4. Next configure correlated alert at the *'Manage Correlation Rules - Add/Modify Rule'* screen with the following
  - a. MessageID - Sensitive\_Data\_Alert (spaces are not allowed in alert names)
  - b. Class - Security.NIC Security Correlated Class
  - c. Alert level - 4
  - d. Event Category - Content.Object

Message text, Description, Action options can also be configured accordingly. For example Message text can be configured as "This alert is triggered when sensitive data is found by RSA DLP after scanning the various servers present in the SharePoint farm".

5. Next click *'Add Circuit'* tab at the bottom which would open the *'Add/Modify Circuit Definition'* screen. The *'Circuit label'* can be configured as desired. Next click *'Add Statement'* at the bottom of this screen to open *'Add/Modify Statement'* screen. *'Statement label'* can be set to provide a label to the statement. Under the option of *'Device Selection'* select *'Select devices by Device Class/Type'* and click *'Add'*. Select *'Security.DLP'* as the *'Device Class/Type'*.



6. Click *'Set Filter'* tab at the bottom which would open the screen *'Set Statement Filter'*. Next click *'Add Filter'* at the bottom of the current screen. Set the following options when configuring the filter.
  - a. Variable - CONTENT
  - b. Comparison – IN
  - c. Criteria - ‘Personally Identifiable Information’
7. The above filter could be also configured for other content blades such as PCI , HIPPA etc.
8. Click *'Apply'* at each screen to reach *'Add Modify Rule'* screen. Click *'Apply'* the final time to save the newly created correlated rule.
9. After the rule has been created it can be seen listed at the *'Manage Correlation Rules'* screen.

Rule Name	Created	Last Modified	Enabled	Priority	Category	Expression	View	Alert	Incident	Msg	URL
Personal Identifiable Information	2009-05-14 10:00:00	2009-05-14 10:00:00	True	1	Content	Content IN 'Personally Identifiable Information'	Content	Alert	Incident	Msg	URL
...	...	...	...	...	...	...	...	...	...	...	...

**Figure 26: Sensitive Data Alerts**

### Sensitive Data Alert View

A **view** defines the devices, messages, correlated alerts and user-defined criteria, within a single site, for which enVision issues alerts.

1. Click ‘Alerts’ tab in the administrative console. Next click ‘Alert configuration’ and then finally click ‘Manage Views’.
2. Let the view name be ‘Sensitive Data Alert View’.
3. In the next screen select various devices or correlation classes for which the alert is defined. Select the correlation class to be ‘NIC Security Correlated Class’ and devices to be the SharePoint servers.
4. Click ‘Next’ to move to the screen named, ‘Customize Alert Configuration’. Select the Attribute drop down to be ‘Device/Type’ and criteria to be ‘NIC Security Correlated Alerts’ so that the filter is ‘WHERE Type IN 'NIC Security Correlated Alerts'. Then click ‘Apply’ and this would list the various correlation rules which match the search criteria. Select ‘Sensitive Data Alert’ to assign this correlation rule to the view and click ‘OK’.



5. The next screen would list the ‘Sensitive Data Alert’ with the ‘Threshold’ option defined as ‘No threshold’. There is no threshold which is necessary for this alert; leave the option as it is.
6. Click Finish and the view would automatically restart.
7. The view created here can be browsed by the administrator at ‘Alert History’ to see the ‘Sensitive Data Alert’.

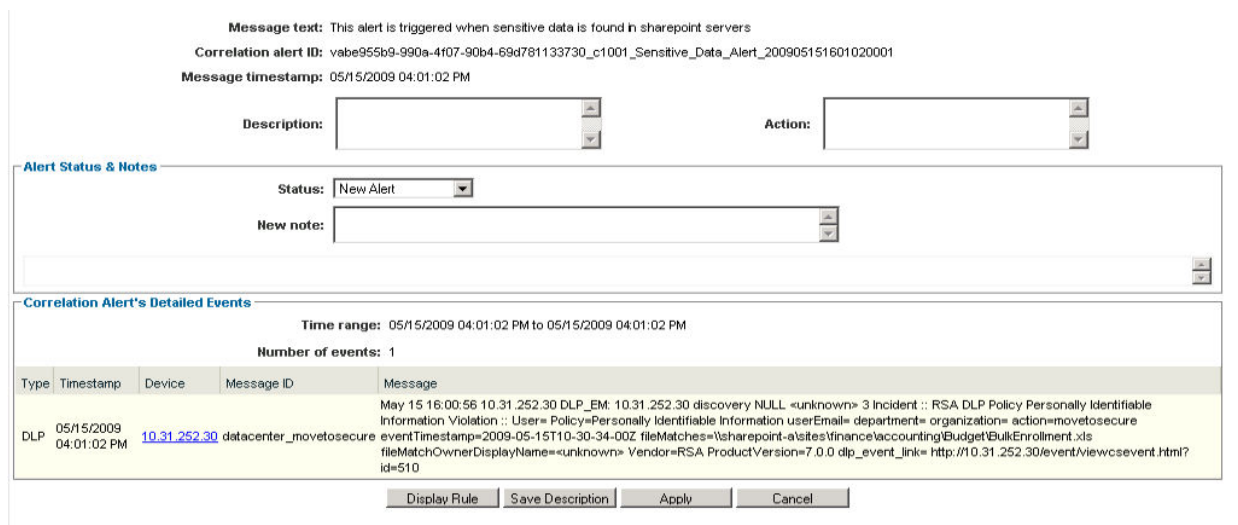


Figure 27: RSA enVision Sensitive Alert Data View

### ‘Most Vulnerable Assets in SharePoint Farm’ Report

Through its Vulnerability and Asset Management (VAM) module, RSA enVision captures vulnerability data about IT applications and systems. Once an administrator identifies the servers that have sensitive data based on results from RSA DLP, RSA Secure View or RSA enVision, the administrator can generate an RSA enVision report that shows SharePoint servers ordered by number of vulnerabilities. The instructions for generating such a report are as follows.

1. Logon to the administrative console of RSA enVision and click ‘Reports’ at the top menu bar. This would populate a drop down on the left hand side, consisting of broad categories of report templates. Next click ‘VAM’, then ‘**Most Vulnerable Assets by Count**’ report.
2. Next click ‘Copy’ tab inside ‘Edit Report’ option.
3. Next you would see the screen ‘Name the Report’. Name the report ‘**Most Vulnerable Assets in SharePoint Farm**’ and modify the description as desired.
4. Click ‘Next’ to go to the next screen named ‘Select Fields’. Select ‘Asset’ as the table and the following fields:
  - i. Scope

- ii. IPAddress
  - iii. Vulnerabilities
  - iv. LastScanned
  - v. LastModified
  - vi. LastPatched
5. Click 'Next' to reach the screen named 'Select Sort Oder'. Specify the sort order of the various fields accordingly.
  6. Click 'Next' to reach the screen named 'Specify Report Selection Creteria'. Leave the 'SQL where clause' unchanged.
  7. Click 'Next' to reach the screen named 'Customize Column Headings'. Various column headings can be modified accordingly.
  8. Click 'Next' to reach the screen named 'Customize Column Order'. The column order can be changed according to the view desired.
  9. Click 'Next' to reach the screen named "Select Additional Report Options' and click 'Apply'.

Generated by RSA enVision					
<b>Report title: Most Vulnerable Assets in SharePoint Farm</b>					
Description: This report lists the assets in order of the number of vulnerabilities associated with an asset in the SharePoint Farm					
Time range: <i>Fri May 15 18:06:15 GMT+05:30 2009 to Fri May 15 18:06:15 GMT+05:30 2009</i>					
Displaying results 1 of 1					
Scope	IPAddress	Vulnerabilities	LastScanned	LastModified	LastPatched
default	10.31.252.128	1869	2009-05-05 19:43:52.0	2009-05-05 19:41:57.0	1970-01-01 05:30:00.0

**Figure 28: Servers with Vulnerability Report**

**‘Failed Logons on SharePoint Farm’ Report**

Multiple failed logon attempts on a server could be indicative of a malicious attempt to logon to a server without authorization. An administrator can use RSA enVision to report whether servers in the SharePoint farm that have sensitive information have had multiple failed logon attempts as part of a periodic risk analysis exercise. Such a report can be generated as follows.

1. Login to administrative console of envision, click 'Reports' at the top menu bar. This would populate a drop down on the left hand side, consisting of broad categories of the report templates. Next click 'Host', then 'Windows' and finally 'Logon/Logoff'.
2. Inside 'Logon/Logoff', click 'Windows - Failed Logons' report. Next click 'Copy' tab inside 'Edit Report' option.



3. Next you would see the screen 'Name the Report'. Name the report 'Failed Logons on SharePoint Farm' and modify the description as desired.
4. Click 'Next' to go to the next screen named 'Select Fields'. Select 'Windows Accounting' as the table and the following fields:
  - a. Date/Time
  - b. UserName
  - c. Workstation
  - d. Reason
  - e. LogonType
  - f. DomainName
5. Click 'Next' to reach the screen named 'Select Sort Oder'. Specify the sort order of the various fields accordingly.
6. Click 'Next' to reach the screen named 'Specify Report Selection Creteria'. Modify the 'SQL where clause' by inserting a logical 'AND' to the existing selection criteria as shown below:
  - a. *AND ((Workstation = 'SHAREPOINT-A') OR (Workstation = 'SHAREPOINT-B'))*. This operator ensures that the report template displays events occurring only on SharePoint servers in the configured farm, ie 'SHAREPOINT-A' and 'SHAREPOINT-B'.
7. Click 'Next' to reach the screen named 'Customize Column Headings'. Various column headings can be modified accordingly.
8. Click 'Next' to reach the screen named 'Customize Column Order'. The column order can be changed according to the view desired.
9. Click 'Next' to reach the screen named "Select Additional Report Options' and click 'Apply'.

Generated by RSA enVision

**Report title: Failed Logons on SharePoint Farm**

Description: This report shows a list of all failed logon events including failure reason, user name, domain name and workstation on SharePoint Servers.

Time range: *Fri May 15 15:21:05 GMT+05:30 2009 to Fri May 15 16:21:05 GMT+05:30 2009*

Displaying results 12 of 12

Date/Time	User Name	Domain Name	Workstation	Logon Type	Reason
2009-05-15 16:12:58.0	administrator	MACERS	SHAREPOINT-B	10	Unknown user name or bad password
2009-05-15 16:12:58.0	administrator	MACERS	SHAREPOINT-B	10	Unknown user name or bad password
2009-05-15 16:12:58.0	administrator	MACERS	SHAREPOINT-B	10	Unknown user name or bad password
2009-05-15 16:12:58.0	siteuser-b	MACERS	SHAREPOINT-B	10	Unknown user name or bad password
2009-05-15 16:12:58.0	siteuser-b	MACERS	SHAREPOINT-B	10	Unknown user name or bad password
2009-05-15 16:12:58.0	siteuser-b	MACERS	SHAREPOINT-B	10	Unknown user name or bad password
2009-05-15 16:11:22.0	administrator	MACERS	SHAREPOINT-A	10	Unknown user name or bad password
2009-05-15 16:11:22.0	administrator	MACERS	SHAREPOINT-A	10	Unknown user name or bad password
2009-05-15 16:11:22.0	administrator	MACERS	SHAREPOINT-A	10	Unknown user name or bad password
2009-05-15 16:11:22.0	siteuser-a	MACERS	SHAREPOINT-A	10	Unknown user name or bad password
2009-05-15 16:11:22.0	siteuser-a	MACERS	SHAREPOINT-A	10	Unknown user name or bad password
2009-05-15 16:11:22.0	siteuser-a	MACERS	SHAREPOINT-A	10	Unknown user name or bad password

**Figure 29: Multiple Login Failure Report**

### ‘Sensitive Data On SharePoint Farm By Policy’ Report

The following steps describe to create the “*Sensitive Data On SharePoint Farm By Policy*”. This report would give the administrator the intelligence about the sensitive data on the SharePoint farm that was found to match a specific RSA DLP policy.

1. Login to administrative console of envision, click ‘Reports’ at the top menu bar. This would populate a drop down on the left hand side, consisting of broad categories of the report templates. Next click ‘Security’ and then finally ‘DLP’.
2. Inside ‘DLP’ click ‘Create New Report’.
3. Give ‘Name’ as ‘**Sensitive Data On SharePoint Farm By Policy**’. Also provide a suitable ‘Title’, ‘Description’ too.
4. Click ‘Next’ to go to the next screen named ‘Select Fields’. Select ‘DLP’ as the table and the following fields:
  - a. Date/Time
  - b. Product
  - c. PolicyName
  - d. DeviceAddress
  - e. Message

- f. MessageID
  - g. EventTime
  - h. EventCategoryName
  - i. EventCategory
  - j. Directory
  - k. DeviceHostName
  - l. Action
5. Click 'Next' to reach the screen named 'Select Sort Oder'. Specify the sort order of the various fields accordingly.
  6. Click 'Next' to reach the screen named 'Specify Report Selection Creteria'. Specify the filter to be PolicyName = 'Personally Identifiable Information'. Filter can be applied for other policy names as well, for eg HIPPA, PCI as desirable.
  7. Click 'Next' to reach the screen named 'Customize Column Headings'. Various column headings can be modified accordingly. In the provided screenshot column named 'Directory' was replaced with 'Sensitive Data File'. Similar substitutions can be done for the remaining column headings as well.
  8. Click 'Next' to reach the screen named 'Customize Column Order'. The column order can be changed according to the view desired.
  9. Click 'Next' to reach the screen named "Select Additional Report Options" and click 'Apply'.

## Compliant Storage of Sensitive Data

### Products Required: RSA Secure View, RSA Data Loss Prevention

1. Use RSA Secure View to discover the SharePoint resource hierarchy and to discover where sensitive information resides.

The screenshot shows the RSA Secure View interface for Microsoft SharePoint. On the left is a 'Resources' tree view showing a hierarchy of sites and folders. The main area displays a 'Security Profile' report. A red-bordered popup window titled 'Items that contain information matching the RSA DLP policy 'Personally Identifiable Information'' is overlaid on the report, listing a file path: '1. \\sharepoint-a\sites\finance\accounting\Budget\BulkEnrollment.xls'. The report table below has columns for 'SharePoint Resource', 'User access configuration in SharePoint', 'Applicable RSA DLP Policy (Severity)', and 'Applicable RSA DLP Content Blade (content type)'. The report shows two entries with violations.

SharePoint Resource	User access configuration in SharePoint	Applicable RSA DLP Policy (Severity)	Applicable RSA DLP Content Blade (content type)
Website - Finance Website - Accounting URL - http://sharepoint-a/sites/finance/accounting	Finance Owners Finance Visitors Finance Members User1 MACERS\finance	Personally Identifiable Information (Severity : High)	Company Internal
Web Application - sharepoint-a:80 Website - Human Resources URL - http://sharepoint-a/sites/human-resource	Viewers Human Resource Owners Human Resource Visitors Human Resource Members MACERS\human resource	Personally Identifiable Information (Severity : High)	Company Internal

This screenshot shows a more detailed view of the security profile report. The 'Resources' tree on the left is expanded to show the file 'BulkEnrollment.xls' under the 'Budget' folder. The 'Security Profile' table highlights this file with a red background, showing the specific user access configuration and the violation details.

SharePoint Resource	User access configuration in SharePoint	Applicable RSA DLP Policy (Severity)	Applicable RSA DLP Content Blade (content type)
Web Application - sharepoint-a:80 Website - Finance Website - Accounting List - Budget File - BulkEnrollment.xls URL - http://sharepoint-a/sites/finance/accounting/Budget/BulkEnrollment.xls	Viewers Finance Owners Finance Visitors Finance Members User1 MACERS\finance	*Personally Identifiable Information (Severity : High) [DLP Event ID : 491]	*US Social Security Number

Figure 30: Discovered sensitive data with violation and Secure View report generation

- Use RSA Data Loss Prevention to move the BulkEnrollment.xls file from the Accounting site to the Employee Benefits site. Clicking on the Event ID displayed in RSA Secure View launches the RSA DLP Enterprise Manager console in context and displays the details of the incident.

## Information Rights Management

### Products Required: RSA Secure View, RSA Data Loss Prevention, Microsoft Rights Management Services

- Use RSA Secure View to discover the SharePoint resource hierarchy, discover where sensitive information resides, and who has access to the information.

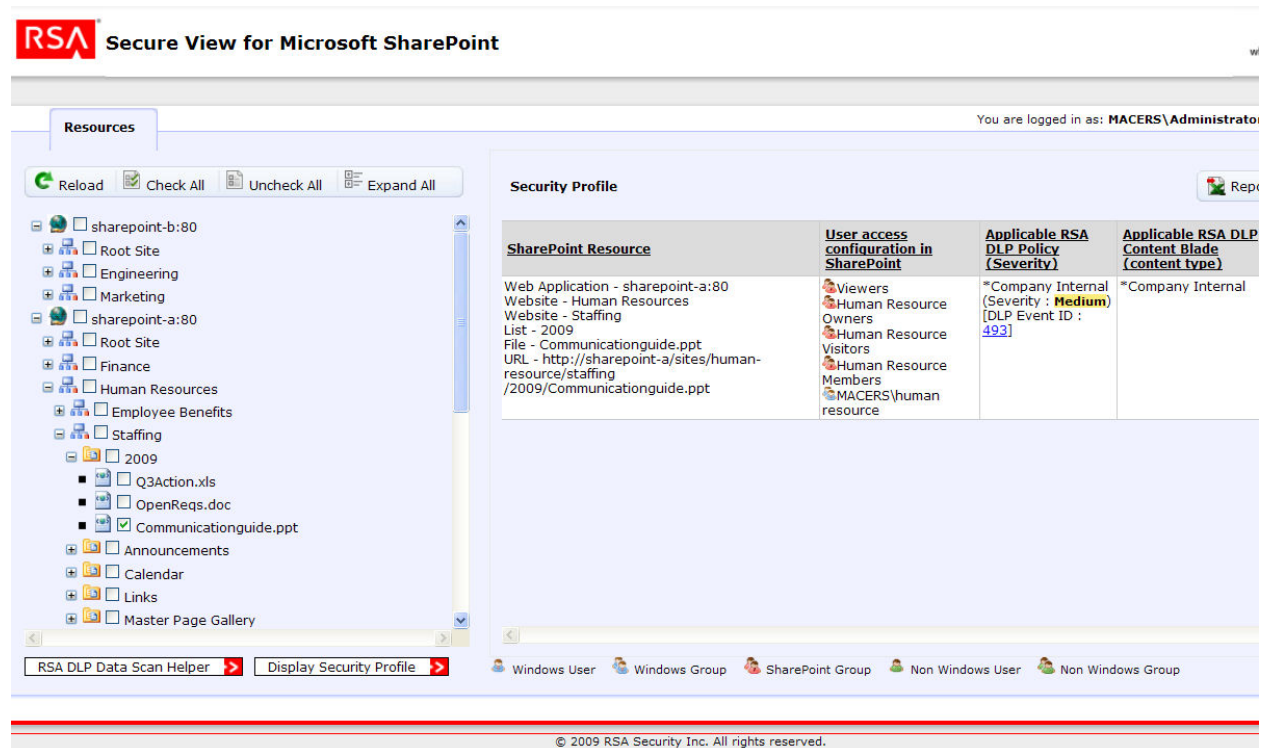


Figure 31: RSA Secure View Correlated View

2. Launch AD RMS and configure a rights management policy called *Company Internal* that allows only the AD groups **Human Resources** and **Engineering Management** to access the content. This ensures that if mistakes are made in the access control configuration within SharePoint, the data is accessible only to authorized individuals. Also, configure AD RMS to restrict printing or downloading of Company Internal content by anyone.

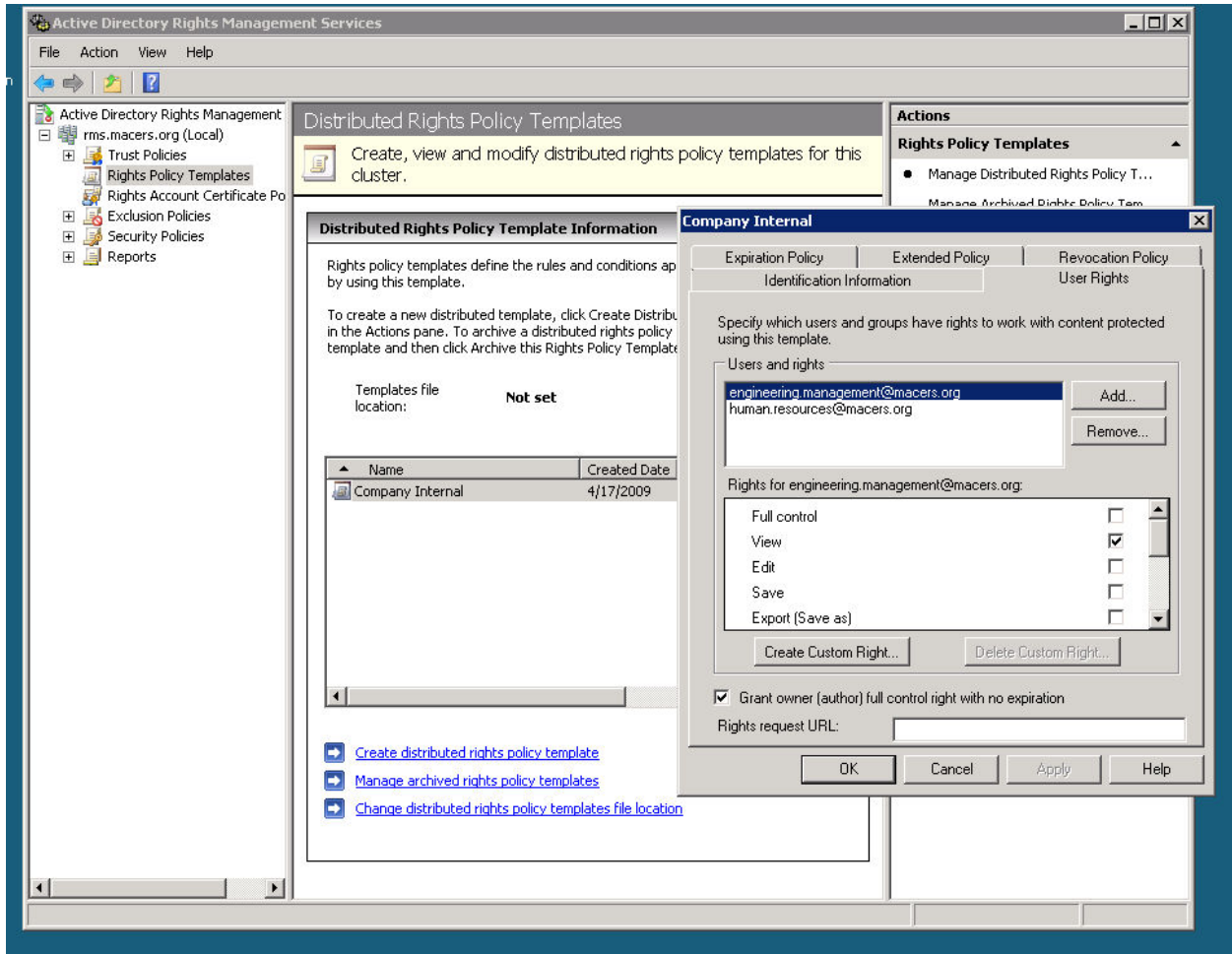


Figure 32: AD RMS



- Associate the RSA DLP Company Internal policy to the Company Internal protection template in AD RMS using the RSA DLP Enterprise Manager console as shown below.

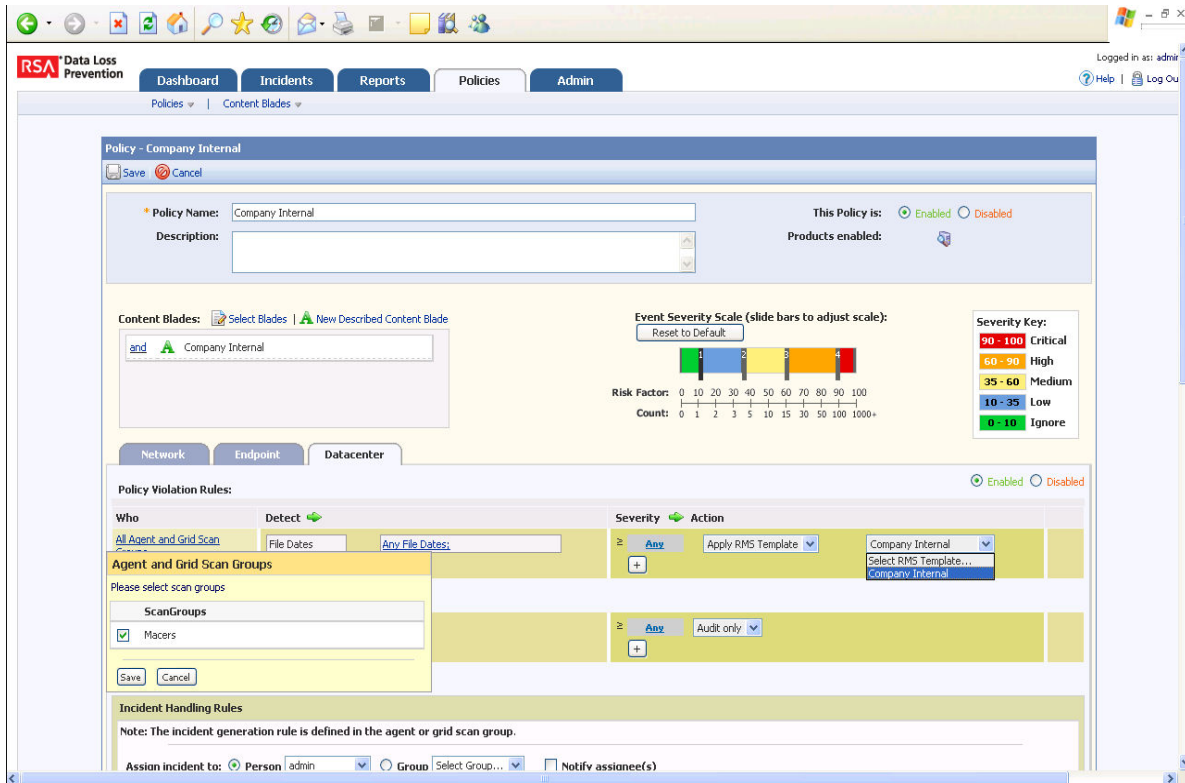


Figure 33: RSA DLP Policy Linked to AD RMS Template

## Centralized Access Management and Strong Authentication

### Products Required: RSA Secure View, RSA Access Manager, RSA SecurID

1. Using RSA Secure View, navigate the SharePoint farm. Please refer to the “Discover user access to sensitive data” workflow in this section to view which users currently have access to sites that have sensitive information.
2. Install the RSA Access Manager agent on the IIS web server instance that hosts the Finance site collection.
3. Add the Finance sites to RSA Access Manager as resources to be protected.
4. Configure roles in RSA Access Manager that map to the appropriate AD groups. For example, the role ‘Finance’ is associated with the AD group Finance and the role ‘Executive Management’ with the AD group ‘Executive Management’.
5. In RSA Access Manager, configure the role-based access policies for selected sites that have sensitive information. Macers Corporation will deploy Access Manager to protect the web server hosting the Finance site.
  - a. Select the URL corresponding to the Finance site in Access Manager.
  - b. Grant access to this URL to the RSA Access Manager roles Finance and Executive Management. Further, require SecurID authentication to the Financial Statements site.

## User Account Management

### Products Required: Courion AccountCourier, Courion ComplianceCourier

The following screenshots describe how Courion AccountCourier and ComplianceCourier products can be used to perform user account management for SharePoint along with other enterprise applications. The example provided below is not related to the Macers Corporation scenarios described throughout this guide but the concepts can be easily related to Macers.

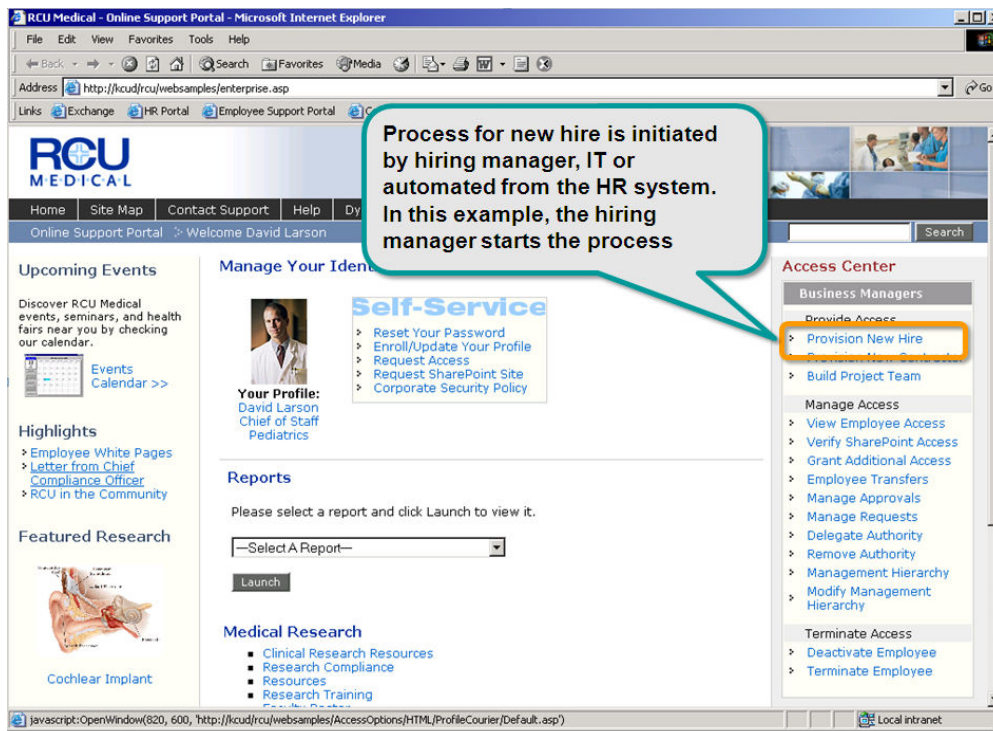


Figure 34: Courion AccountCourier - Begin User Provisioning Process

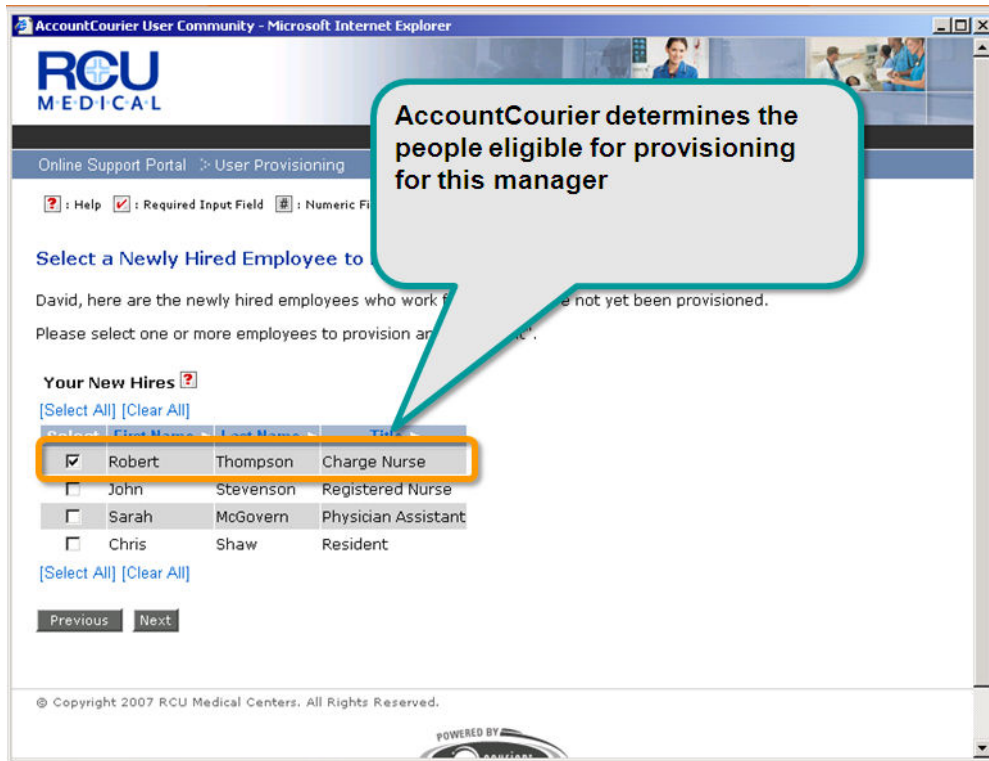


Figure 35: Courion AccountCourier – Select Users

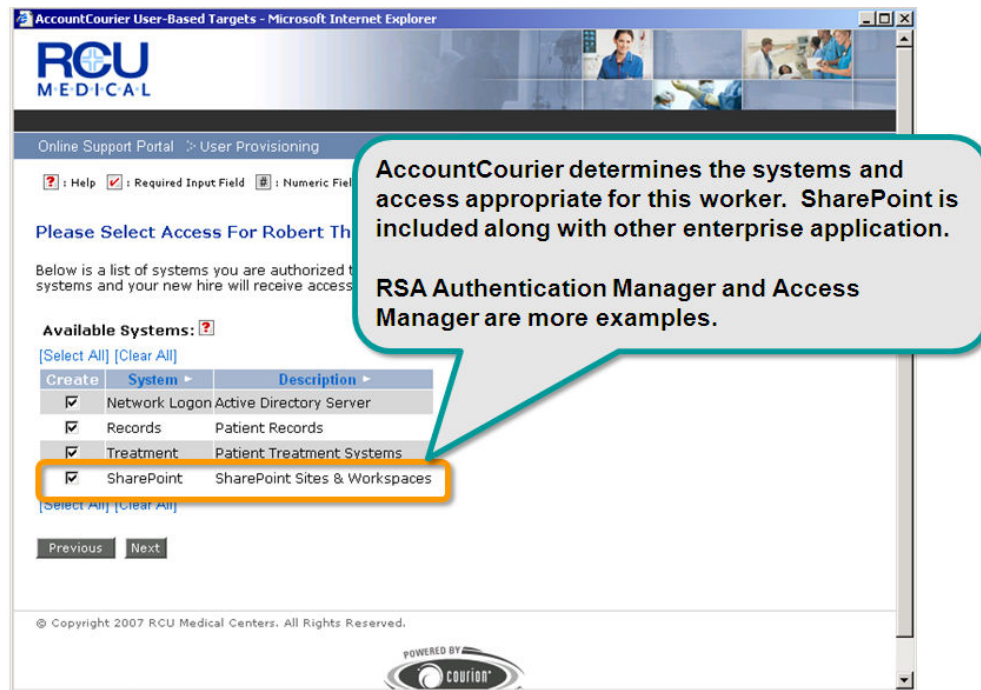


Figure 36: Courion AccountCourier – Select Target Applications

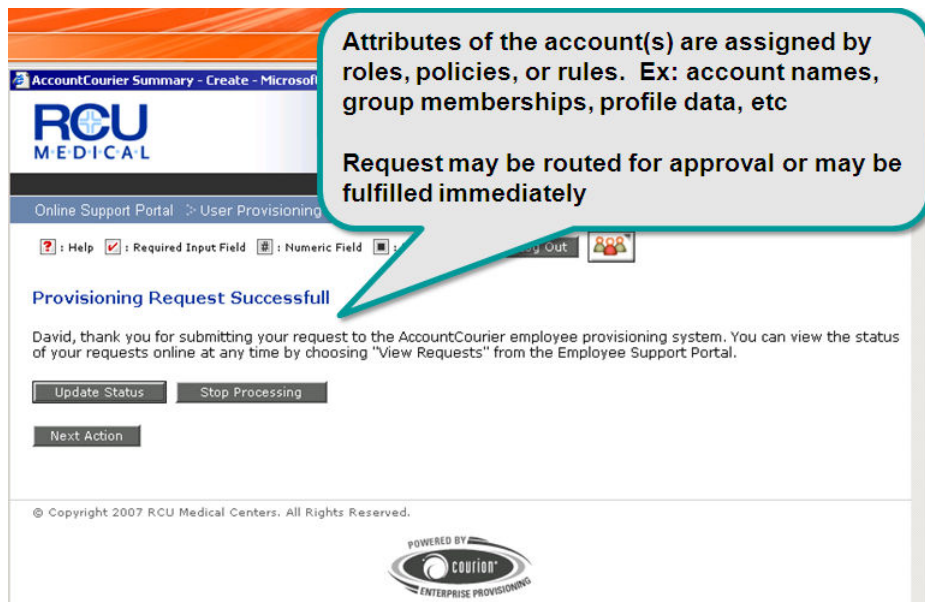


Figure 37: Courion AccountCourier – Routing for Approval

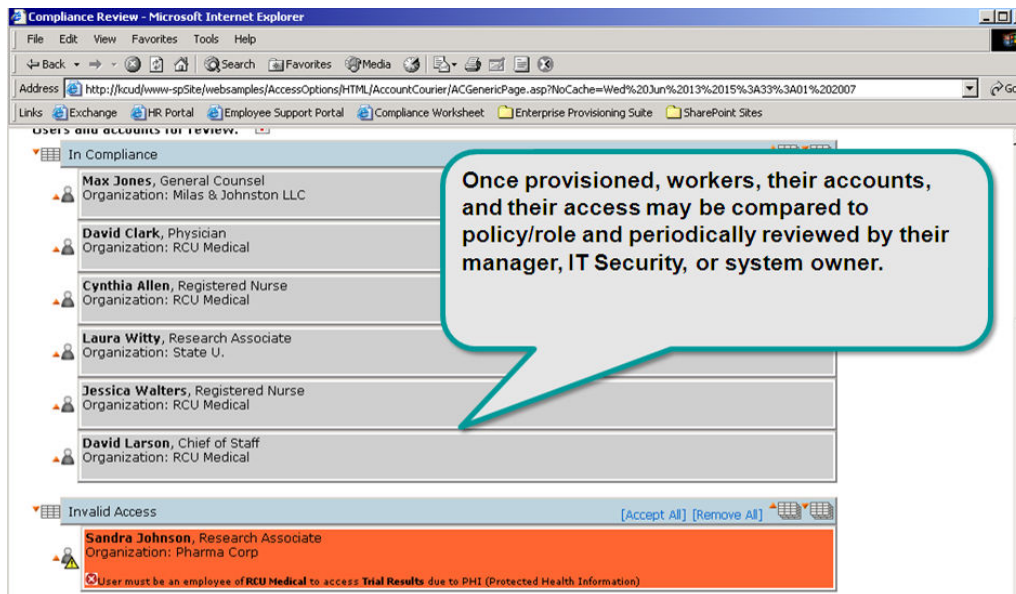


Figure 38: Courion ComplianceCourier – Attestation

## Troubleshooting

### Debugging RSA Secure View

In case of malfunctioning of RSA Secure View, the first step should be to enable logging for the tool. Debug logs can be enabled by editing the 'bin/log4net.xml' file in the installation directory. Details are provided in the 'Configuring logging' section of readme.txt file. The cause of the RSA Secure View errors is specified as an exception in the log file. If RSA Secure View is unable to connect to the RSA DLP database, an error message is displayed in the tool. The exact cause of the failure in connection can be obtained from the log file.

### Common Issues and Resolution

1. If the user session times out and a user tries to export a report from RSA Secure View, an error page is displayed. The user should visit the Home page of RSA Secure View or go back and refresh which creates a new session.
2. If the RSA DLP connection fails with the following error logged in the log file: Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON', the error is most likely due to double hop issue. IIS server would not pass on the user's credentials to a remote database unless constrained delegation has been configured. Details on 'constrained delegation' is provided in the following Microsoft article: <http://msdn.microsoft.com/en-us/library/ms998355.aspx>.