

## Whitepaper: Manage Access Control for Network Resources with Securitay's Security Policy Manager

### Introduction

The past several years has seen an increase in the amount of attention paid to security management in large and heavily regulated organizations. The drivers may be any of the following:

- Regulatory compliance
- Business and competitive pressures to better protect sensitive intellectual property and business-related data
- Greater concern for data security given the increasing threat levels

Security management can take many forms, but this paper focuses on endpoint access controls for resources that are otherwise widely available and visible. Securitay has deep experience in creating, documenting, and evangelizing core components of the Windows security infrastructure. Relative to the goals of enterprise security management we have identified the following weaknesses in the Windows platform:

1. Built largely on decentralized Windows NT technologies, centralized management of security is one of the weakest aspects of the Windows-based infrastructure.
2. The decentralized management experience for network resources such as File Shares, Printers, SharePoint, and Active Directory itself is a challenge for all but the most expert of administrators.
3. Active Directory provides a good identity and authentication service for the Windows-based infrastructure, but fails to provide direct control or visibility of user network access levels.

For those that are not Active Directory experts, the third point requires more explanation. Active Directory provides a rich infrastructure for managing aspects of identity including user attributes and a rich group infrastructure with capabilities for hierarchies and subordination. On the network resource side, all Microsoft server products have the capability to grant permissions, usually through an Access Control List (ACL) or functionally similar mechanism, to users through group membership. What is missing, however, is linkage between the groups and the network resources which use them to grant permissions. It is this linkage between identity and permissions that should be the foundation of security management in a large organization. It is also this linkage that forms the basis for any audit activity – either internal or external – in an organization.

The previous description of weaknesses in the Windows platform is not meant as a criticism relative to other platforms. Other operating systems provide arguably less capability for centralized management than Windows - but that does not mean that room for improvement does not exist. Securitay believes that there is substantial room for improvement and has developed an application, **Security Policy Manager**, that attempts to correct the deficiencies listed above.

Security Policy Manager was built to satisfy the following set of high-level requirements:

1. Report on the access privileges for a particular user

2. Show all of the users with access to a network resource
3. Centralize the administration of security permissions
4. Simplify permissions management for a group of resources containing data with the same classification
5. Provide the ability to delegate permission management from IT to the business unit
6. Simplify the interface for security permission management
7. Provide manage-anywhere capability using a web interface
8. Provide a change management database for permission and security policy changes
9. Make it possible to manage other aspects of endpoint security, such as encryption, through the same interface used to manage access controls
10. Easily extended to support additional resource types
11. Easy to deploy
12. Enable self-service access requests
13. Provide Policy Decision Point (PDP) interfaces for LOB applications

The remainder of this whitepaper describes how Security Policy Manager satisfies these high-level requirements.

### **Report on the Access Privileges for a Particular User**

Technical people familiar with Active Directory and the problems of access control often lament that it is not possible to right-click on a user object in Active Directory and select **Show Resources**. The idea is that it would be great if Active Directory had a role in access management as well as identity management. While it is true that this would be a great feature, Windows currently does not offer this capability.

Security's Security Policy Manager fills this gap by providing an interface that provides network resource access control information simply and reliably. Thirty minutes after beginning the installation of Security Policy Manager, it is possible to generate reports that specify exactly what file share, SharePoint, Printer, database and other network resources a user has access to and at what level.

Security Policy Manager provides reports down to the user level for each and every resource by performing full group expansion of single and multi-level nested Active Directory groups. Generating this same level of information using the native Windows UI could take hours to generate a report for a single user – long enough that the report may not even be accurate by the time it is completed as policy and Active Directory changes. With Security Policy Manager the same process takes seconds. Furthermore, the information that the report is based upon is never stale. Security Policy Manager can be configured to refresh access information from the source resources on whatever time interval is appropriate for your organization and requirements.

The screenshot shows the Security Policy Manager web application in Internet Explorer. The browser address bar shows the URL: `http://smfp-spm/SPM/SecurityPolicyManager/UserDetails.aspx?User=Corp\PaulP`. The page title is "Security Policy Manager" and the navigation menu includes "Policies", "Resources", "Reports", and "Administration".

The main content area displays the "Resources Accessible to the following user" report for user "PaulP" from domain "Corp". A checkbox labeled "View with resource specific access" is present. Below the user information is a table listing resources and their access privileges.

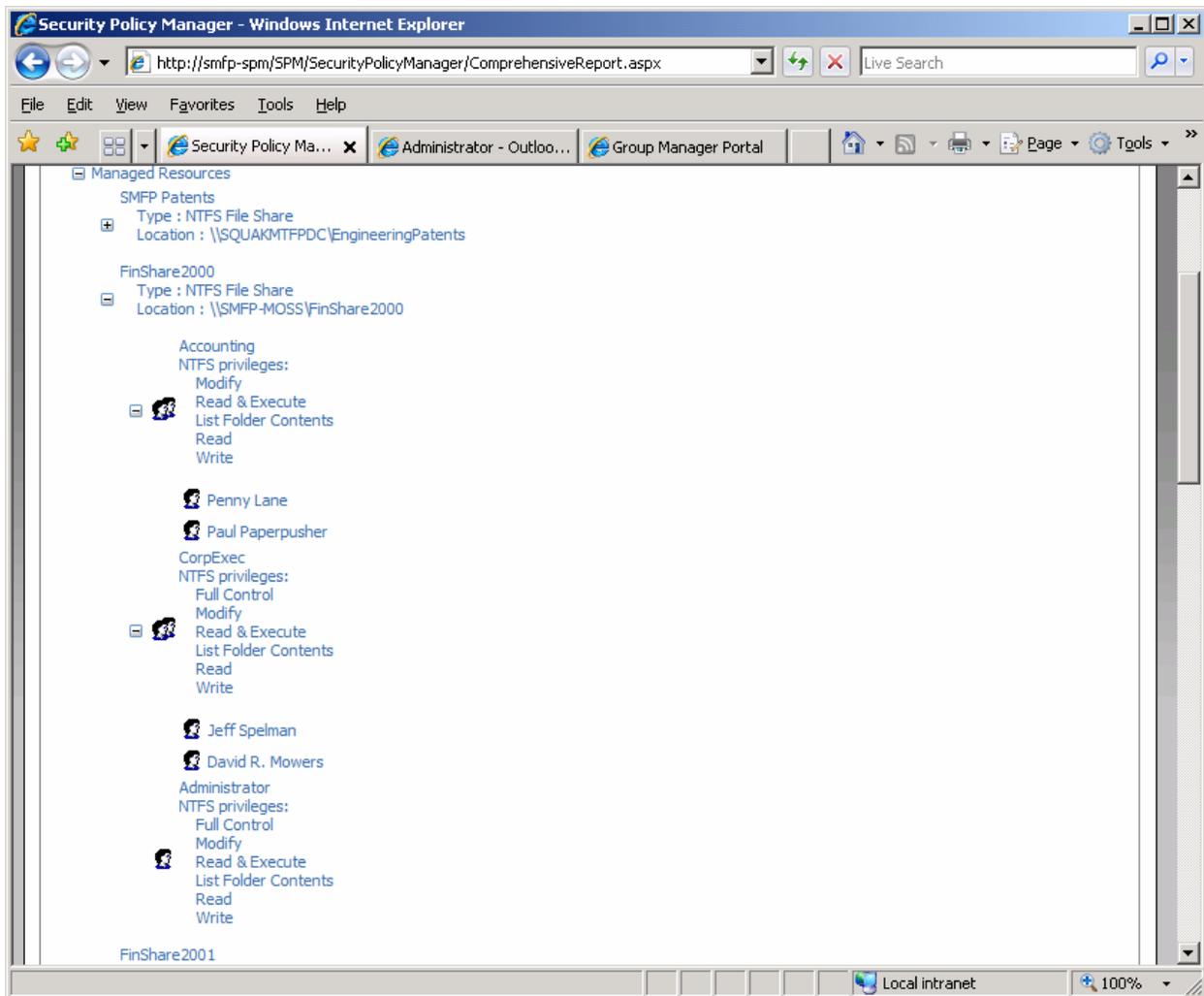
Resource Name	Type	Location	Access Privileges	
\\smfp-moss\pcidataq1_2006	NTFS File Share	\\smfp-moss\pcidataq1_2006	NTFS privileges: Read & Execute List Folder Contents Read	<a href="#">Details</a>
FinShare2000	NTFS File Share	\\SMFP-MOSS\FinShare2000	<a href="#">Read/Update/Execute</a>	<a href="#">Details</a>
FinShare2001	NTFS File Share	\\SMFP-MOSS\FinShare2001	<a href="#">Read/Update/Execute</a>	<a href="#">Details</a>
FinShare2002	NTFS File Share	\\SMFP-MOSS\FinShare2002	<a href="#">Read/Update/Execute</a>	<a href="#">Details</a>
SharePoint Financials	SharePoint Site	http://smfp-moss/Financials	<a href="#">Read/Update/Execute</a>	<a href="#">Details</a>

At the bottom of the table area, there is a button labeled "Write to CSV File".

### User Access Report

#### Show All of the Users with Access to a Network Resource

For high-value and critical systems, it is often a requirement to produce a report that shows everyone that may have some level of access.

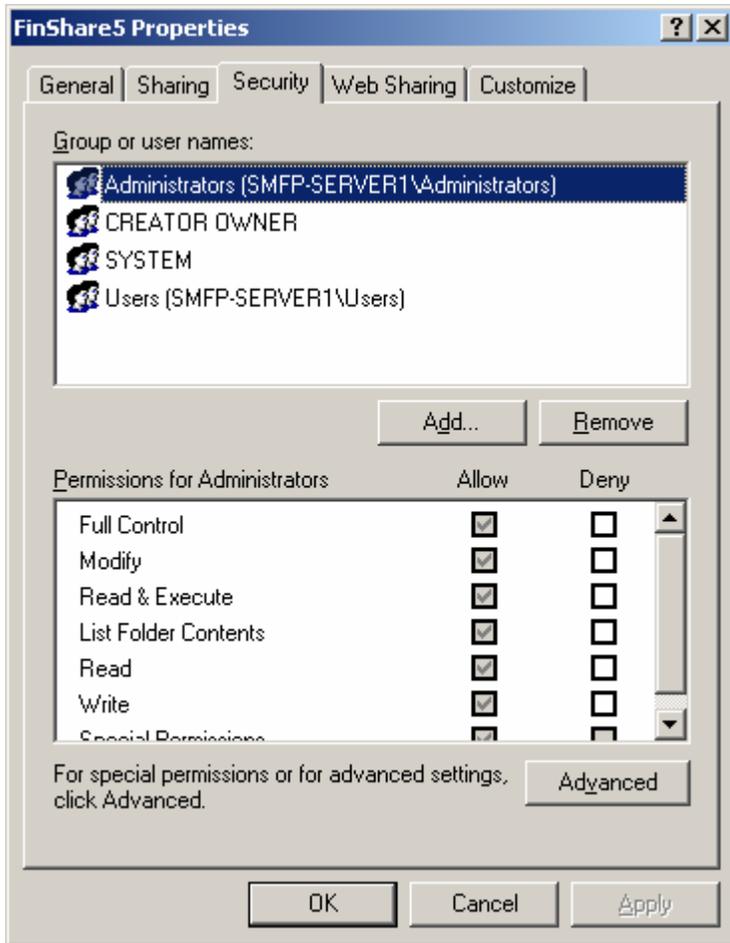


### *Comprehensive Access Report*

With Security Policy Manager's intuitive web interface, it is a simple process to easily look at every resource in the network and determine exactly who has access, to what level, and what group was used to grant access.

### **Centralize the Administration of Security Permissions**

In the Windows world, access management is largely a decentralized process. Most everyone with enough interest in this topic to make reading this paper worthwhile will be familiar with the Access Control List (ACL) Editor. This UI can be accessed by right-clicking on any file, directory, file share or printer object on a Windows client or server operating system, clicking on Properties and then clicking on the Security tab.



### Windows ACL Editor

This ACL Editor interface shown above is functional, but suffers from the limitations that it requires a significant number of clicks to perform basic permission management and also that it must be accessed on the machine for which you need to manage permissions. In large organizations that have scaled out network resources across many, many servers the UI becomes inefficient and impractical to use. For IT resources that may be responsible for permission management across a large number of servers, the number of clicks required using the native interface or the requirement to logon to a server adds unacceptable overhead to the administrative process.

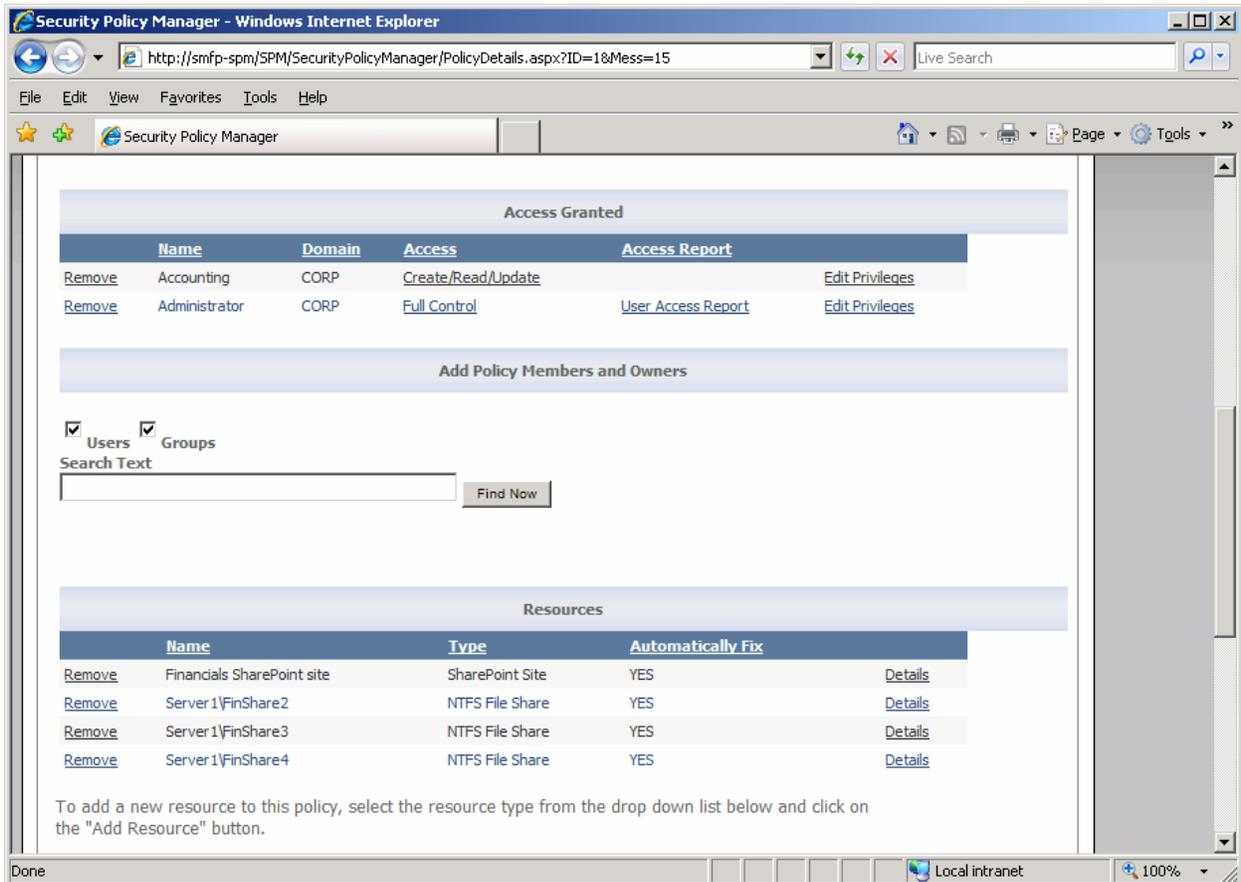
The following table summarizes the number of UI interactions needed in single and multiple server scenarios when using the native interface:

Operation	One Server Resource	Five Server Resources	Ten Server Resources
Add an access level for a group or user	9	45	90
Change an access level for a group or user	7	35	70

Remove a user or group's access	7	35	70
---------------------------------	---	----	----

Note that the additional overhead of logon/logoff actions is not included in the above table

The administrative overhead of permission management of Windows-hosted resources can be greatly reduced by providing the capability to centrally manage network resources through a single user interface. A central interface for the administration of multiple network resources is a primary feature of Security Policy Manager.



### Centralized Administration of Network Resources

Using the Security Policy Manager interface, the number of clicks required to view or modify permission levels to resources with similar data is greatly reduced without the need to logon to the servers being administered.

Operation	One Server Resource	Five Server Resources	Ten Server Resources
Add an access level for a group or user	5	5	5
Change an access level for a group or user	3	3	3

Remove a user or group's access	2	2	2
---------------------------------	---	---	---

Note that there is no additional overhead for logging on or off of any servers in order to set make these permission modifications reducing even further the administrative overhead of these operations.

This table shows two things: the number of interactions that administrators are required to perform can be reduced even for a single server environment. More importantly, administrative overhead can be reduced even further in environments with large numbers of servers and network resources. One implication is that the organization can decide to scale out network resources hosting similar data without incurring any penalty for permission management.

### **Simplify Permissions Management for a Group of Resources Containing Data with the Same Classification**

Data classification is an effort to categorize data elements that may be found in a large computing environment. This is an important idea for data security because it lets organizations construct high-level security policies and processes for data that has similar security characteristics no matter where it might be found. For example data that contains customer credit card numbers falls under specific regulatory guidelines including the Payment Card Industry Data Security Standard (PCI DSS). A specific requirement of PCI DSS is to **Restrict access to cardholder data by business need-to-know**.

One possible approach to meeting this requirement is to analyze all of the different data repositories where PCI data may reside, for example the organization's mainframe, file systems, databases, etc., and devise separate access control policy enforcement mechanisms for each system. The downside to this approach is that management across three systems can be difficult to synchronize – all the more so because in most organization there would be different administrative teams to manage the different infrastructure components.

A better approach would be to create an umbrella policy enforcement platform that can enforce the same access policies based on the user role across all systems. Security Policy Manager meets this requirement by being extensible and able to enforce consistent access controls on nearly any data repository that contains similarly classified data. Figure 2 above shows that 2 different types of resources, Windows File Shares and Windows SharePoint sites can be managed as specific elements in a single policy.

This capability can provide even greater potential to increase the efficiency of access permission management than simply managing multiple resources of a single type. Not only does the policy definition exist in only one system instead of being maintained across several such systems, but changes to policy can be performed through a single intuitive user interface. With Security Policy Manager an employee in the organization can be tasked with managing security policies without having to give that employee broad administrative privilege in all the targeted systems or having to train that employee on the interfaces used to manage permissions for each system.

### **Provide the Ability to Delegate Permission Management from IT to the Business Unit**

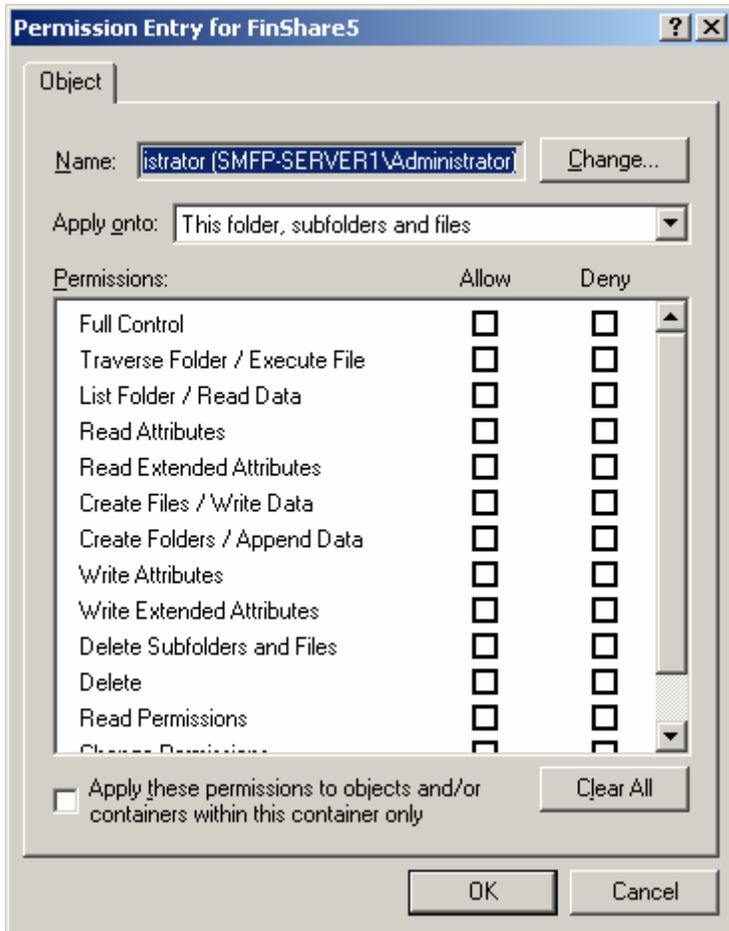
A roadblock that is often encountered in the implementation of effective access control management is that IT administrators often end up with the lion's share of the administrative tasks associated with the control process. This is counter to the end goal of effective permission management for at the least the following reasons:

- IT administrators are frequently unfamiliar with the nature and peculiarities of both the data that they are managing permissions on and the user roles that be used to grant access
- Overburdened administrators can become a roadblock to users being able to access the data they need to do their job
- Business units loose the sense of ownership over their own data that is needed for effective compliance efforts

Security Policy Manager is built with delegation scenarios in mind and any user in the organization can be granted the ability to establish and manage access permission policies. Often this will be done as a partnership operation with an IT administrator helping to establish policies and join resource servers to policies using their administrative credentials. Once a resource is joined to a policy it can be administered by any policy owner or co-owner with thorough tracking of every policy management operation performed using Security Policy Manager.

### **Simplify the Interface for Security Permission Management**

A potential barrier to delegating permission management to less technical non-administrators in the business units is the terminology and complexity of the granular permissions associated with most network resource types.



*Complete set of permission levels for NTFS objects*

The figure above demonstrates the complexity of setting permission on a shared directory on a file server. Beyond the simple fact that this interface is four levels deep, it presents a somewhat bewildering array of permissions that are sure to confuse anyone who is not a Windows file system expert. Mistakes made in this interface would not be terribly surprising and could easily lead to a situation where the organization is out of compliance.

Security Policy Manager overcomes this challenge by managing permissions at a less-granular level when the situation warrants this approach. The permissions are abstracted to a more intuitive set of access levels represented by the mnemonic CRUDE.

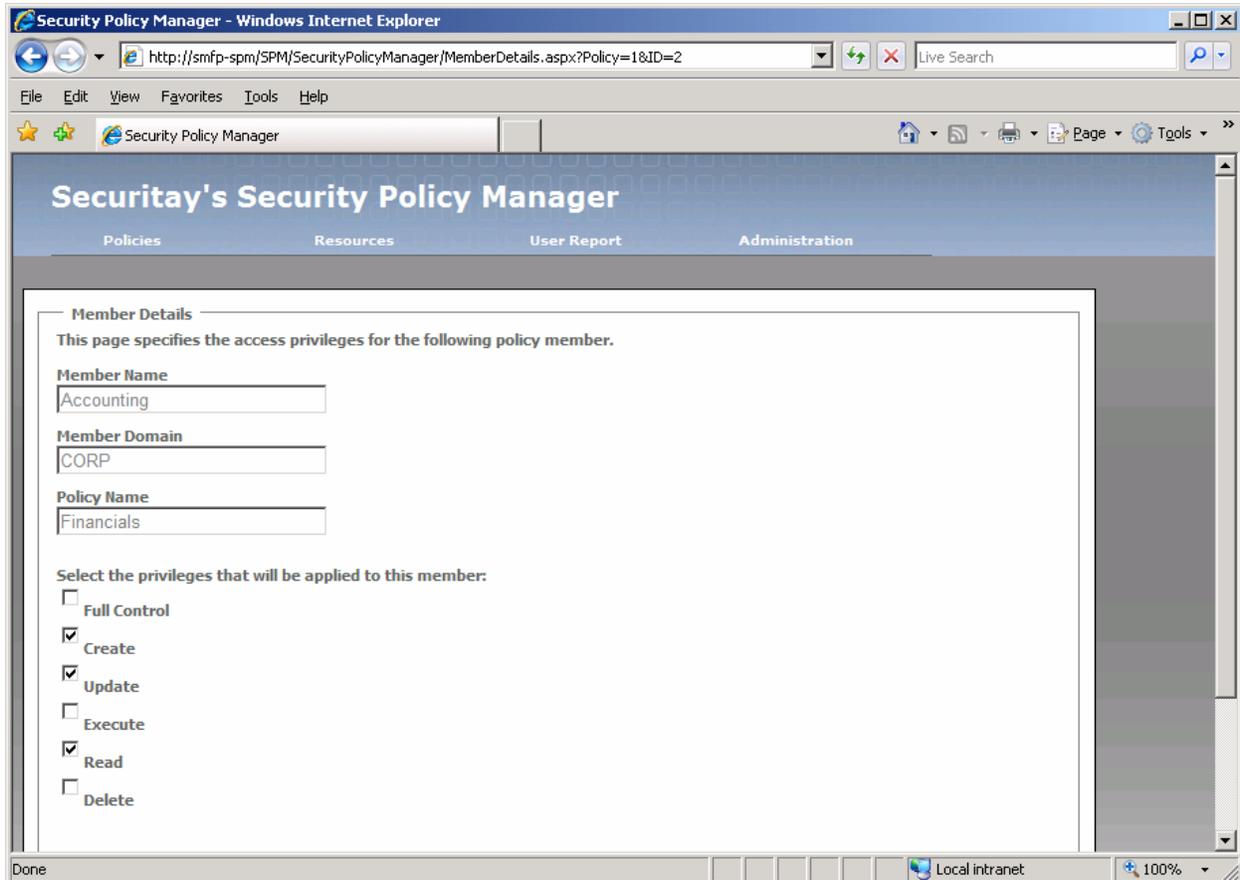
C – Create. Create means different things on different types of resources, but the intuitive understanding of Create is consistent. Create generally allows a user to create a new object such as a file or database table

R – Read. Across all types of data this is an intuitive access level that allows for the reading of the data.

U – Update. This permission allows a user to modify and existing data source such as a file or database table.

D – Delete. Allows a user to delete an object in the container or higher level object being managed.

E – Execute. Allows a user to run executables, database stored procedures and scripts in the managed container or object.



### *Simplified Access Levels used by Security Policy Manager*

The previous figure demonstrates the simplicity of permission management using Security Policy Manager. Any business unit employee can be trained to understand the meaning of these broad access levels and stands a much better chance of managing permissions correctly which allows the organization to remain in compliance.

### **Provide Manage-anywhere Capability using a Web Interface**

When an organization decides to take advantage of delegation in order to spread the burden of access permission management, it is critical to provide an interface that is widely available. Only a web application can provide such capability since only a web application alleviates the need for client application installation. Furthermore, Security Policy Manager does not require additional passwords and userids since it uses Windows integrated authentication to provide a single sign-on (SSO) experience.

## Provide a Change Management Database for Permission and Security Policy Changes

Understanding the current permission levels of any particular user or who has been granted access to particular resources is often not sufficient for many audit scenarios. Just as important is the ability to understand how the policy achieved it's current state. Since all permission management actions are stored in the Security Policy Manager database, the complete chain of actions that led to a particular policy state can be recalled and analyzed.

The screenshot displays the Security Policy Manager web interface in Internet Explorer. The browser address bar shows the URL: `http://smfp-spm/SPM/SecurityPolicyManager/PolicyDetails.aspx?Id=1`. The page title is "Security Policy Manager".

The main content area is divided into several sections:

- Owner Information:** A table with columns "Owner Name", "Domain", and "Type". It lists two users: "Administrator" (CORP) and "David R. Mowers" (CORP), both of type "User". Each entry has a "Remove" link.
- Closed Issues:** A section with a "Show Closed Issues" checkbox, which is currently unchecked.
- Policy History:** A section with a "Show Policy History" checkbox, which is checked. Below it is a table with columns "Date", "Action", "Owner", and "Details".

Owner Name	Domain	Type	
<a href="#">Remove</a>	Administrator	CORP	User
<a href="#">Remove</a>	David R. Mowers	CORP	User

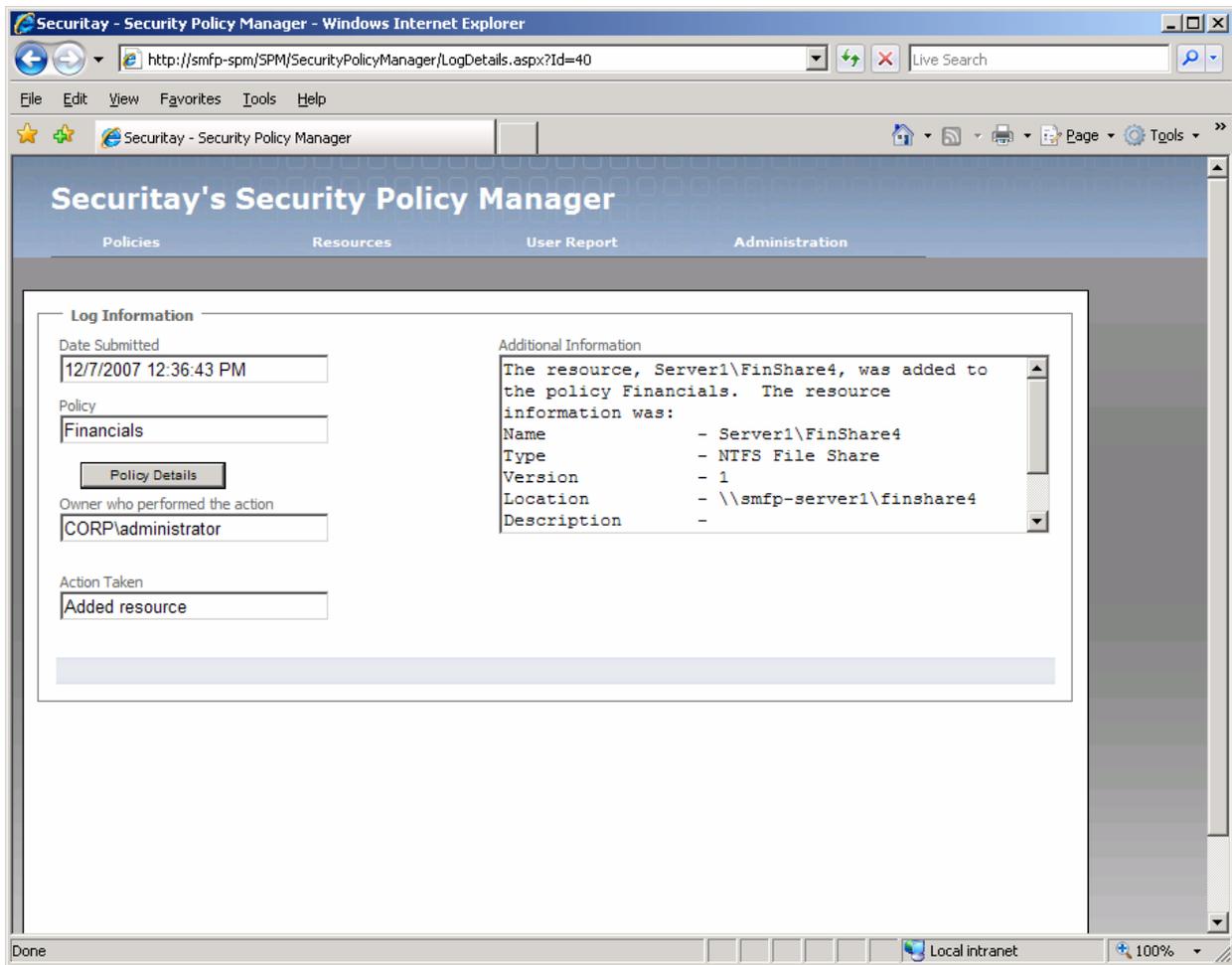
  

Date	Action	Owner	Details
11/1/2007 6:44:42 AM	Created policy	CORP\administrator	<a href="#">Details</a>
11/1/2007 6:44:42 AM		CORP\administrator	<a href="#">Details</a>
11/1/2007 6:44:42 AM	Added policy member	CORP\administrator	<a href="#">Details</a>
11/1/2007 6:48:09 AM	Added resource	CORP\administrator	<a href="#">Details</a>
11/1/2007 6:49:08 AM	Added policy member	CORP\administrator	<a href="#">Details</a>
11/1/2007 7:58:16 AM		CORP\administrator	<a href="#">Details</a>
11/1/2007 7:58:16 AM	Added policy member	CORP\administrator	<a href="#">Details</a>
11/1/2007 8:32:56 AM	Added resource	CORP\administrator	<a href="#">Details</a>
11/1/2007 11:37:02 AM		CORP\administrator	<a href="#">Details</a>
11/1/2007 11:52:21 AM	Updated resource	CORP\administrator	<a href="#">Details</a>

At the bottom of the history table, there is a pagination control showing "1 2 3 4" and a "Delete Policy" button.

### Access Policy History

The figure above shows a snap shot of the policy history maintained by Security Policy Manager. The details screen shown in Figure 8 summarizes the complete details pertinent to a particular policy modification.



### *Example Log Detail*

Organizations are not restricted to generating reports through the interface. Packaged database queries are provided for out of the box use or can be modified to suit the requirements of specific organizations and scenarios.

### **Make it possible to manage other aspects of endpoint security, such as encryption, through the same interface used to manage access controls**

Security Policy Manager is designed to be flexible enough to administer other aspects of resource security policy beyond access controls. A common scenario that Security Policy Manager can enable is the ability to enforce data encryption. As an example of the capabilities, Encrypting File System (EFS) is an encryption mechanism provided at no extra cost in the Windows environment. A problem with EFS has been that it can be extremely difficult to manage using the tools provided with Windows. While EFS can be used for File Shares, the scenario fails when access to the file share is granted using Security Groups – a necessary practice in all but the simplest network environments.

Security Policy Manager is able to make the EFS file share scenario work because it can create the complete list of all users who can access a particular resource and then make the appropriate EFS API calls in order to enable decryption by the users who should have access to the files on the share.

The EFS example described is just one such example and Security Policy Manager will continue to be integrated with other security mechanisms in order to enforce additional levels of security in order to create a highly secure and well managed network environment.

### **Easily extended to support additional resource types as needed**

Security Policy Manager ships with the capability to manage common resource types including Windows File Shares, SharePoint, Windows Servers, and LOB applications when using our PDP interfaces. Over time, this list will grow to include other resources including Active Directory, Printers, Physical Access Control Systems and others as indicated by customer demand. But most organizations have a surprising variety of network resource types and Securitay did not create a solution that limits an organization to securely managing only a few resources or only those resource types that Securitay supports in the product.

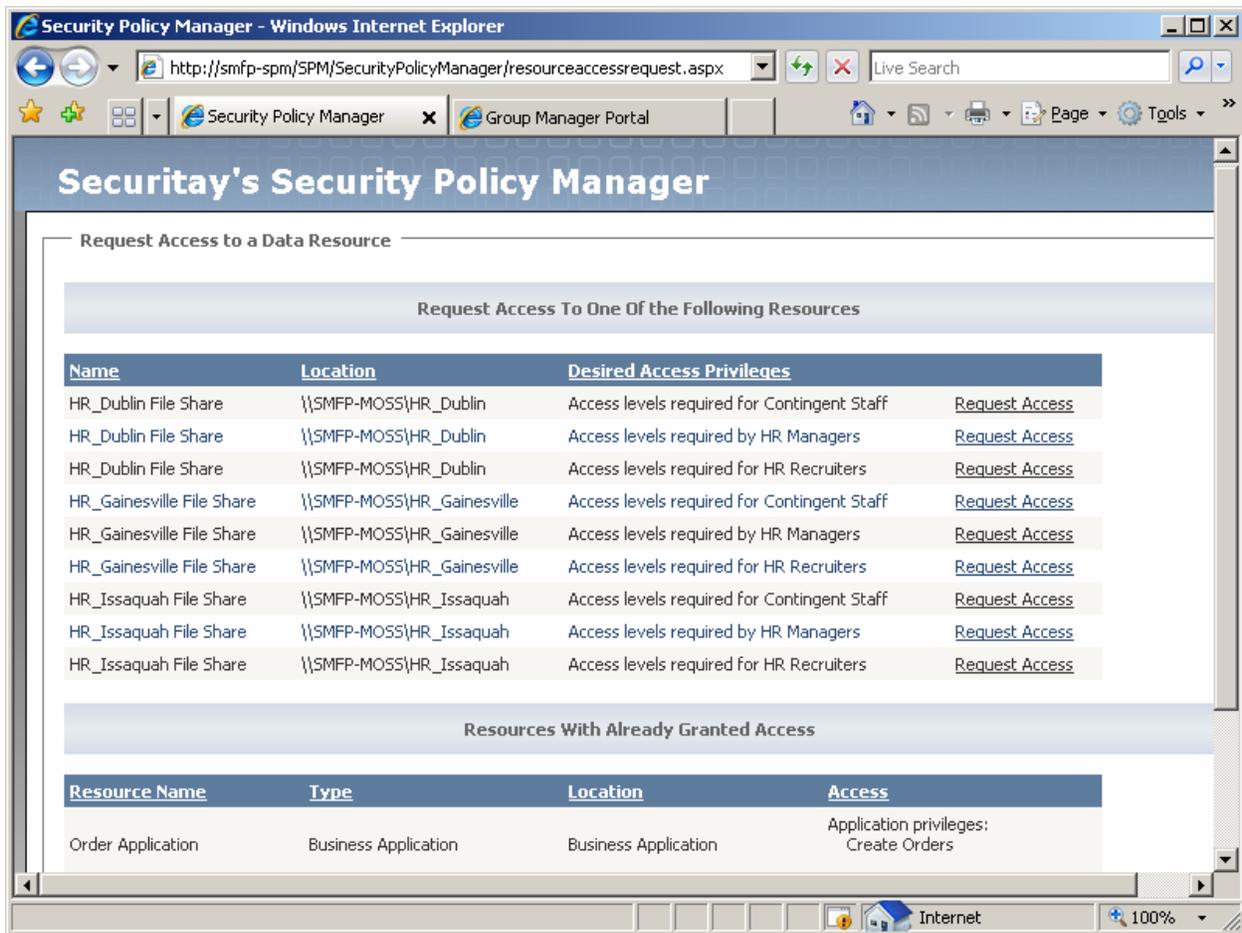
With this in mind, Security Policy Manager is built as an easily extensible platform which can manage access policy on nearly any type of network resource that exposes a remote API for managing access. Our solution integrator partners or moderately skilled developers in your organization can use the Security Policy Manager SDK to create new functionality.

### **Easy to deploy**

Complicated deployment processes is often a barrier to product adoption and we have made this task easier by offering a flexible model that provides exactly the capability that your organization requires while making deployment as easy as possible. Security Policy Manager supports either agent or agent-less modes of operation. Using agents, an organization can attain near real-time monitoring and management of critical systems with reduced network bandwidth usage. For those organizations with less stringent security requirements, agent-less operation eliminates the need to install **any** component on the managed system.

### **Enable Self-Service Access Requests**

In combination with our self-service group management application, Group Management Portal, Security Policy Manager can provide self-service access request capability to your organization.



### *Self-service Access Request*

Using the workflow and approval mechanisms provided by Group Management Portal, any user in your organization can navigate to a web interface and see, at a glance, resources that they can request access to at the privilege level appropriate for their job function.

### **Provide Policy Decision Point (PDP) Interfaces for LOB Applications**

The OASIS [XACML Profile for Role Based Access Control \(RBAC\)](#) defines a Policy Decision Point that evaluates an access request against a policy to produce an access decision. Creating a standardized interface for access decisions is a worthy goal that has been adopted by many organizations. Security Policy Manager supports interfaces compatible with the XACML Profile along with basic Web Services interfaces that make it easy for application developers to use our flexible policy store directly from a Line of Business application.

### **Conclusion**

We think that Security Policy Manager will change how administrators view the problem of managing endpoint security and access control. If the features and functionality described in this paper align with pain points that your organization suffers from, then visit [www.securitay.com](http://www.securitay.com) where you can find out

more about our products, solutions, and people. If you need more information or details about any of our products, please call us at 425-392-0203, or send an e-mail to [sales@securitay.com](mailto:sales@securitay.com).