



Guidelines

# WORKSPACE SECURITY MANAGER (WSM)

---

Simplify security, set walls, and easily create  
need-to-know security with WSM

**netdocuments**<sup>®</sup>

# Contents

<b>INTRODUCTION.....</b>	<b>3</b>
<b>WHAT IS WORKSPACE SECURITY MANAGER?.....</b>	<b>3</b>
WSM Policy Manager Security Groups.....	5
<b>APPLYING WSM POLICIES.....</b>	<b>6</b>
<b>WSM CONTROLS.....</b>	<b>7</b>
Set the Policy as a Wall.....	7
Inclusionary and Exclusionary Walls.....	7
Allow Need-to-know Sharing via CollabSpaces.....	8
Effective Rights Reporting.....	9
<b>WSM AND FLEXIBILITY IN APPLYING SECURITY TO DOCUMENTS.....</b>	<b>9</b>
<b>WSM AND FLEXIBILITY IN APPLYING WALLS.....</b>	<b>10</b>
<b>WSM CONSTRAINTS.....</b>	<b>10</b>
<b>WORKING WITH WSM SECURITY POLICIES VIA API'S.....</b>	<b>11</b>
<b>SUMMARY.....</b>	<b>11</b>

## INTRODUCTION

*NetDocuments continues to build* on the highest levels of technical excellence to provide extremely secure repositories for your documents and other content. However, most NetDocuments users are not Information Security specialists, but rather busy professionals who want to easily apply security policies, ensuring that only the people who need to can see the information that is stored in workspaces organized by Matters, Project Numbers, Practice Areas etc.

NetDocuments aims to provide customers with full Information Assurance capabilities, defined by NIST as:

- **Confidentiality** – restricting access or limiting the actions that can be taken with information
- **Integrity** – ensuring that information can only be accessed or modified by authorized users
- **Availability** – ensuring information is available and ready for use by authorized users
- **Authentication** – ensuring users are who they say they are
- **Non-repudiation** – ensures that actions taken on information cannot be denied

As part of our Information Assurance strategy, Workspace Security Manager (“WSM”) is designed to be a fundamental part of the enhanced security and governance measures provided by the PROTECT solution. It provides a mechanism to decentralize the creation and management of security policies to those who are close to the content, and who as part of their day to day work know who should have access to it, and at what level.

This document addresses how the NetDocuments WSM capabilities can help you manage your security, how it fits with existing products you may own and what benefits it brings as part of your security strategy.

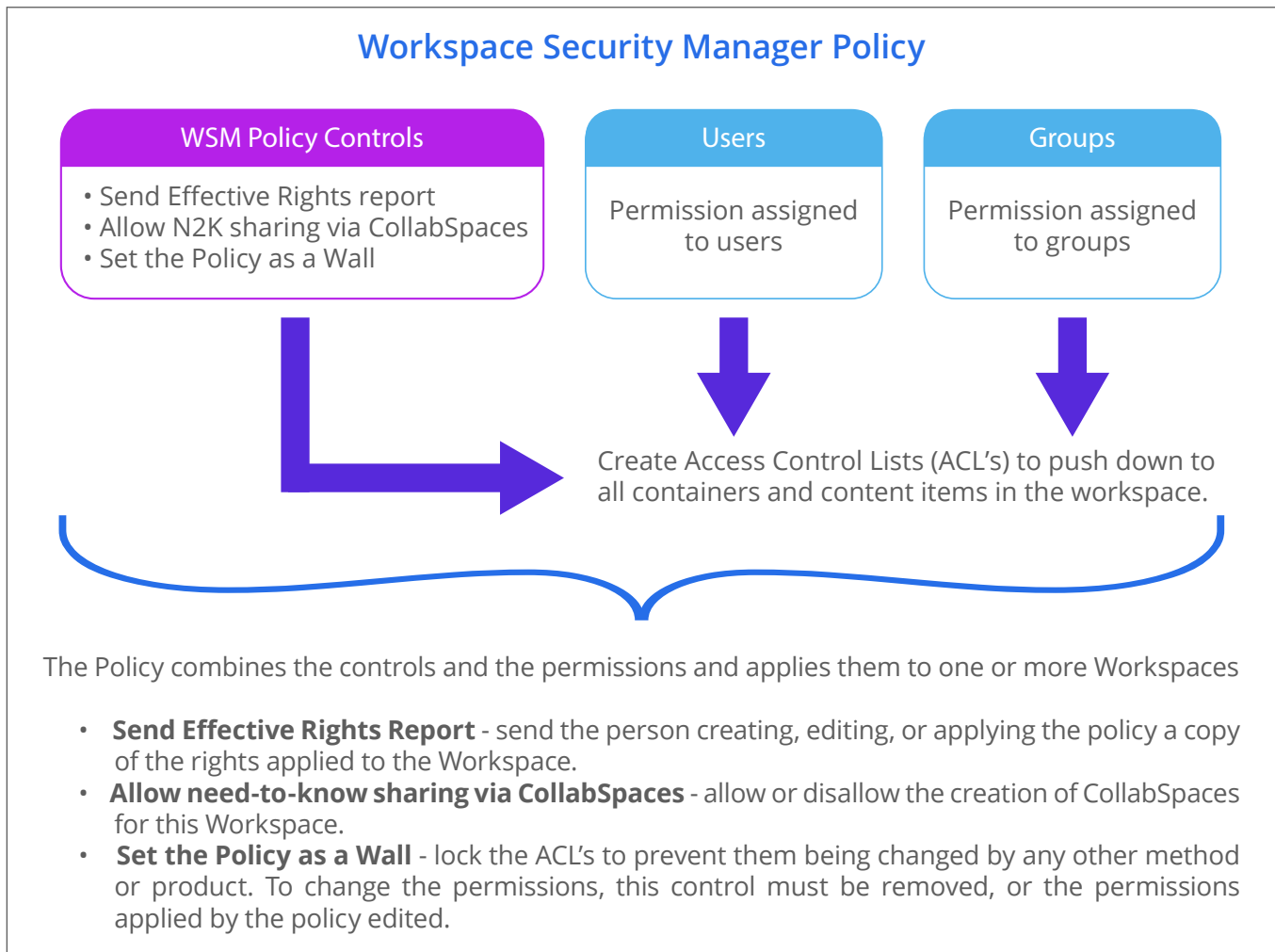
## WHAT IS WORKSPACE SECURITY MANAGER?

Workspace Security Manager helps you manage security at a workspace level by creating, managing and applying policies. A policy has two required workflows: 1) adding users and/or groups and assigning permissions to them and 2) configuring a set of controls.

The three controls are:

- **Send Effective Rights Report** – send the person creating, editing or applying the policy a copy of the rights applied to the Workspace
- **Allow “Need-to-Know” sharing via CollabSpaces** – allow or disallow the creation of CollabSpaces for this Workspace
- **Set the Policy as a Wall** – lock the Access Control Lists (ACLs) to prevent them being changed by any other method or product, to change the permissions this control must be removed, or the permissions applied by the policy edited

The permissions and controls are combined in a Policy which can be applied to many Workspaces within a single cabinet. A Workspace can only have a single policy applied to it.



#### Important Note:

ACLs that are applied to content as part of a WSM policy override all other security mechanisms. WSM Policies are not additive, the permissions applied through the policy completely replace the existing permissions, implementing the ACLs from the policy. *This means that applying a WSM policy will replace existing ACLs set by:*

- Folder Inheritance
- Filing to a workspace or folder
- Metadata attribute-based security (Profile Based Security & Absolute Profile Based Security)
- Link to User (a specific form of attribute-based security)
- Save as Private (ndOffice)
- Save to recipients (ndMail)

Once new permissions have been applied to content by applying a WSM policy to a workspace, they can then be modified by all the above mechanisms UNLESS the permissions are locked by applying the Wall control as discussed in the section above. Once locked the only way to manage permissions on affected content is by editing the WSM policy.

When a WSM policy is edited, any changes to the permissions are again pushed down to all content items in the relevant workspace. This means that if you did not lock the permissions using the Wall control, and other mechanism were then used to change the ACLs on specific items, those ACLs will be overwritten by the application of the edited policy.

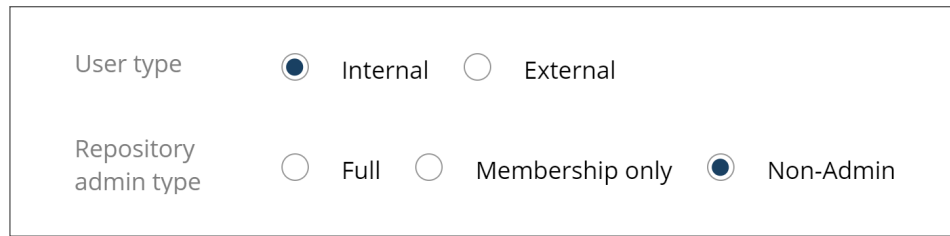
## WSM Policy Manager Security Groups

WSM Policies are managed at the Cabinet level to provide flexibility in creating, managing, and applying the policies to Workspaces. When a WSM Policy Manager uses the tool, they choose the Cabinet for which they want to create, manage, and apply policies. WSM Policies in one Cabinet cannot be applied in another.

You can create a single user group for your organization, ensuring that group has access to all your Cabinets, or you can be more fine grained all the way down to creating a specific group for each Cabinet. The ability for a group to be assigned the ability to manage WSM policies is part of the security group creation dialogue:

The screenshot shows a configuration dialog for a security group. The 'DETAILS' tab is selected. The 'Group Name' is 'Litigation Cabinet WSM Policy Managers'. The 'Membership' is set to 'Internal'. Under 'Group options', the following settings are visible: 'Hide group membership' (off), 'Do not display in user group list' (on), 'Members are allowed to create new cabinets' (on), 'Members are allowed to upload lookup tables' (on), 'Members are allowed to manage devices' (off), and 'Members are allowed to manage WSM Policies' (on, highlighted with a red circle). Under 'Other options', 'Send welcome email' is off. 'CANCEL' and 'UPDATE' buttons are at the bottom right.

When you add a user to a group for which the WSM Policy management is enabled, the user's account is automatically modified to give them the 'Membership Admin' capability in order to apply new permissions:



The image shows a configuration box with two rows of radio button options. The first row is labeled 'User type' and has two options: 'Internal' (selected with a blue dot) and 'External' (unselected). The second row is labeled 'Repository admin type' and has three options: 'Full' (unselected), 'Membership only' (unselected), and 'Non-Admin' (selected with a blue dot).

You can decentralize control, and assign the ability to create, manage, and apply WSM policies to the right people in your organization, those who understand the structure and purpose of your information. This may be your Legal Operations team, a KM Lawyer, a Practice Area manager etc., but importantly these individuals do not need to be Repository or Cabinet Administrators.

You can add individuals to multiple WSM manager groups if you setup different groups for different Cabinets, and WSM will check the individual's permissions only allowing them to apply policies in the Cabinets to which they have access.

## APPLYING WSM POLICIES

When you have created your policies, you can apply them to multiple Workspaces. The Workspaces tab of the WSM admin page provides the ability to search for Workspaces, based on the organizing attribute used for the Cabinet. For example, you can search based on Client, Matter, or Project, and if you find 6 matters related to litigation with ACME Corp as the client, you can select them all in the UI and apply a single policy.

If you need to apply policies to large numbers of Workspaces, there is a bulk application method. WSM Policy managers can create a .CSV file with a column for the Workspace identifiers and a column for the WSM policy name. Upon upload the .CSV file will be evaluated, and the policies will be applied to the Workspaces.

### Important Note:

The more containers and content items there are in a Workspace, the longer it will take to apply the permissions from the policy to the ACL of each container and content item. For very large workspaces this could take hours. Therefore, if you upload a .CSV file with hundreds or thousands of very large workspaces, the changes could take a long time to be applied. It is good practice to consider both the size of the Workspace (the number of containers and content items) and the number of workspaces to be included, when applying WSM policies in bulk.

## WSM CONTROLS

What sets WSM apart from being just another way to assign security permissions to all the content in a Workspace is the additional controls that are managed within the policy. The controls are an intrinsic part of the policy, so for example if a policy is first applied without the Wall being set, a member of the WSM policy managers group can edit the policy and set the Wall control, locking the permissions, and this will be recorded for audit purposes in the policies history.

### Set the Policy as a Wall

If you leave this control set to off, then the action of applying the policy will push the new permissions to the ACL's of all the containers and content items in the Workspaces to which the policy is applied. Once applied, those with appropriate Admin permissions, or mechanisms such as Profile Based Security (PBS) and Absolute Profile Based Security (APBS) will still be able to change those ACL's. This maybe an appropriate stance to take if you are using a third-party partners product to manage security including ethical walls, for example Intapp Walls.

If you wish to lock the ACL's in place after distributing the new permissions in the WSM policy, then you set this control to on. A flag is now set on all containers and content items in all Workspaces to which the policy has been applied, which prevents other mechanisms from changing them. For example:

- Users with Admin Rights will not be able to change the ACL
- Metadata based security, such as profile-based security, will not be able to change the ACL
- Any item placed into the Workspace will automatically inherit the permissions from the policy

#### **Important Note:**

If you set this simple wall in place by locking the permissions, this will also prevent third party partner products, such as Intapp Walls, from functioning. The only way to unlock the permissions is to edit the control within the policy, or to revoke the policy from a Workspace. This will leave the current permissions in place, but once again allow them to be changed by other methods.

### Inclusionary and Exclusionary Walls

There is no default setting for a policy, as deciding whether a wall is inclusionary or exclusionary is dependent upon the permissions assigned to individual users or groups within the policy.

Defining the different types of walls:

- Inclusionary walls use one or more groups to give access to documents
- Exclusionary walls use one or more groups to deny access to documents

Individual users or groups can be assigned the No Access permission (N rights) to make a wall exclusionary. In NetDocuments, if a user is assigned the No Access (N) permission either explicitly or via group membership, this will override any other VESA rights granted to the user elsewhere on the ACL. A user with N rights cannot view a document, CollabSpace, or folder etc.

If a individual is a member of both Group A and Group B and we assign the following rights to these groups within the policy:

- Group A – VESA
- Group B – N

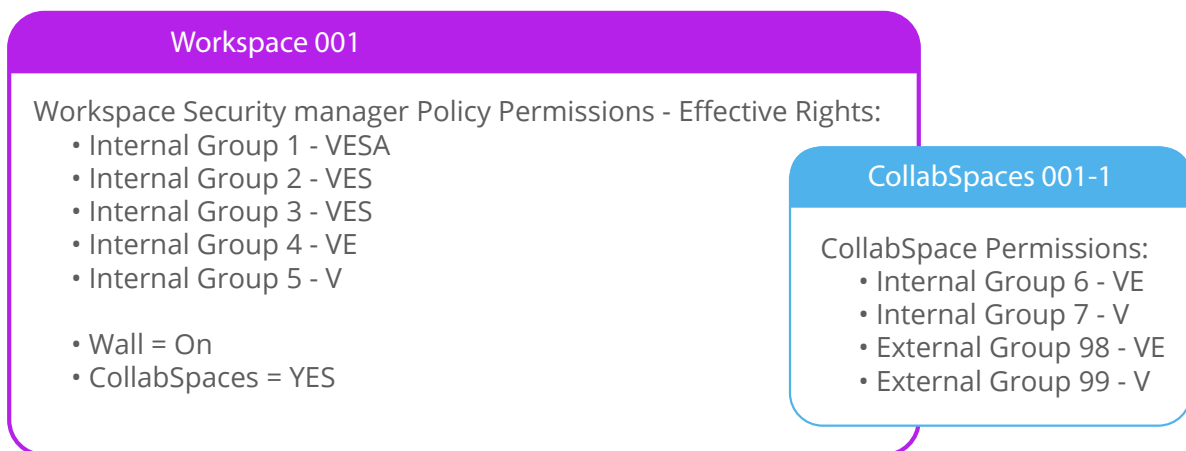
Then the N rights take precedence and the individual will be excluded from the Workspace and its content by the policy.

A WSM policy must include some users or groups with inclusionary access, even if its main purpose is to operate as an exclusionary policy, as if only N rights are assigned in the policy, then no users will be able to access the Workspace.

## Allow Need-to-know Sharing via CollabSpaces

If a policy is applied to a Workspace with this control set to off, you will not be able to create a CollabSpace within the Workspace. If you set this control to on, you are providing users with the ability to create CollabSpaces in the Workspaces to which the policy is applied. The permissions applied to content within the CollabSpace are set through the normal CollabSpace security mechanism. This provides a way to enable need to know sharing of sub-sets of content from the originating Workspace, without having to open up the permissions or add additional users to the Workspace itself.

If you have locked the permissions by setting a Wall, and also allowed the creation of CollabSpaces, you are providing a need to know sharing mechanism that is analogous to putting a gate in your wall. This is depicted below:





Following the best practice of assigning permissions only through group membership, we can see that a particular set of groups have been added to what might be a litigation matter, through their addition to an appropriate WSM policy that has been applied to the matter Workspace.

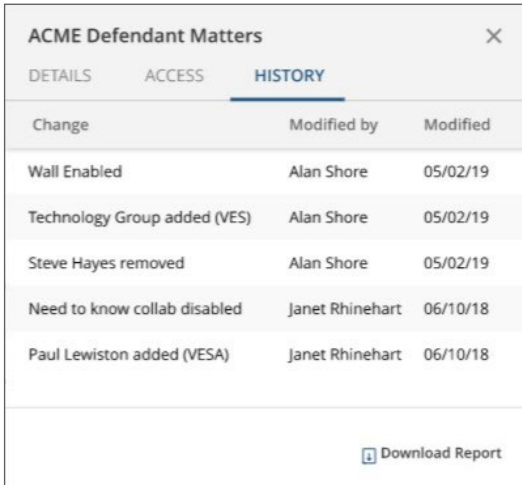
However, there are no tax experts on the litigation team, and there is a requirement for both in-house tax lawyers and the firms external forensic accounting partners to examine some documents. This sub-set of content is copied to the CollabSpace, which has its permissions set to give the tax and forensic accounting experts the appropriate access.

Once this stage of the matter has been completed, any edits made to copies of documents in the CollabSpace can be merged with the original versions or saved as new versions, and the CollabSpace can be deleted, ensuring access is now returned to only those firm employees who are members of the groups assigned permissions by the WSM policy.

### Effective Rights Reporting

The collection of permissions given to different groups and/or individual users by the WSM policy constitutes the effective rights assigned to the Workspace and all its content. The policy also allows for a report of the effective rights defined by the policy to be emailed to the individual creating or editing the policy. This provides a copy of the rights that can be kept outside of the system for reference or audit purposes. Note that the report is only sent to the person who created the policy.

Each policy also has an history of the changes made to that policy. This is accessed by selecting a specific policy on the policy tab on the WSM admin page. Information on a policy is provided on 3 tabs – the details, access and history tabs. On the history tab all changes to the policy can be seen and at the bottom of the information pane, a link is provided to download a copy of the policies history:



ACME Defendant Matters		
DETAILS	ACCESS	HISTORY
Change	Modified by	Modified
Wall Enabled	Alan Shore	05/02/19
Technology Group added (VES)	Alan Shore	05/02/19
Steve Hayes removed	Alan Shore	05/02/19
Need to know collab disabled	Janet Rhinehart	06/10/18
Paul Lewiston added (VESA)	Janet Rhinehart	06/10/18

[Download Report](#)

Policy history tab and download link

The effective rights are also displayed within the workspace, allowing users of the Workspace to gain a quick understanding of who has what access to the content.

### WSM AND FLEXIBILITY IN APPLYING SECURITY TO DOCUMENTS

WSM provides an easy-to-use method for applying and managing permissions to all content items at the workspace level. However, it is not the only way you can organize and manage the security of your content. A WSM policy can be applied to a single Workspace, or hundreds of Workspaces

within a Cabinet, but because the policy is not applied at the Cabinet level, you can mix and match the use of WSM Policies and other mechanisms, such as Cabinet Defaults and Profile Based Security.

As noted above, a WSM security policy, when applied, will override any existing permission set by any other method, and this design approach sticks to our mantra of simplicity. However, if you wish to leverage a highly flexible, nuanced approach to setting permissions, using WSM policies does not prevent you from using Profile Based Security to set permissions for content in different Workspaces.

For example, you could use a WSM security policy to change the permissions of all the content items in a Workspace, but not lock the permissions by using the Wall setting. This would then allow authors of documents or other users who have been granted admin rights to change the permissions on their documents as part of the business processes or workflows.

## WSM AND FLEXIBILITY IN APPLYING WALLS

WSM also provides flexibility if you wish to lock permissions to create simple ethical walls. There are many business reasons for locking the permissions set by a WSM policy, from Federal, State or international regulatory requirements to client requirements for confidentiality, to moving away from 'open by default' security models. The ability to lock the permissions means that they cannot be changed by any other NetDocuments or third-party product security mechanisms. This also provides a single point of control to change or edit the permissions being the policy itself. Separate, downloadable history files for each policy provide a full audit trail of what changes have been made, by whom, and when.

NetDocuments works closely with our globally renowned partner Intapp to integrate their highly sophisticated product called Intapp Walls. If you use the WSM capability to lock the permissions applied by a policy, you will not be able to use Intapp Walls with the content to which that policy has been applied. As noted above WSM security overrides all other security mechanisms, including Intapp Walls.

However you could use us a WSM security policy without the lock set, to apply permissions to all the content items in one or more workspaces, and then lever your existing investment in Intapp Walls to manage ethical walls across NetDocuments content, your time and billing system and your CRM.

## WSM CONSTRAINTS

There are several NetDocuments security features that either constrain WSM behavior, or do not work with WSM security policies:

- Multi-Value Profile Attributes – When the workspace organizing attribute (for example the Matter field) is designated as an MVP field, selecting multiple values will cause any content items to appear in multiple workspaces. The content items access will be determined by the

primary value. The primary value is the first value in the field. When using MVP's all ACLs are determined by this primary value

- Save as Private (ndOffice) – save as private will not work when saving into a workspace which has a WSM policy applied. An ndOffice user will be informed by a dialogue box that the ACL selected will not be applied to the document, and the document will inherit the permissions set by the policy
- Save to Recipients (ndMail) – save to recipients will not work when saving into a workspace which has a WSM policy applied. An ndMail user will be informed by a dialogue box that the permissions will not be set to the recipients, and the message will inherit the permissions set by the policy

## WORKING WITH WSM SECURITY POLICIES VIA API'S

A full set of public API's will be published to allow integration with third party tools and custom and integrations. These API calls will allow you to get the WSM policies available in given cabinet, modify an existing policy, apply a policy to a list of workspaces, or find the workspaces to which a policy has been applied, and many more.

## SUMMARY

[NetDocuments Workspace Security Manager](#) provides an easy-to-use way of creating, managing and applying security policies that include permissions assigned to users and groups, and settings to lock the applied permissions, and allow or disallow the use of CollabSpaces for need to know sharing.

WSM takes a simple approach to applying permissions, overriding existing permissions, with content being added to a Workspace where a policy is applied automatically inhering the permissions of that policy.

To create an exclusionary Wall, create a WSM Policy and assign users or groups the No Access permission.

When a WSM policy includes the setting to lock the permissions, it cannot be overridden by any other NetDocuments security mechanism, or by a third-party tool such as Intapp Walls.

A WSM policy can allow or disallow the use of CollabSpaces as a mechanism for need to know sharing, a mechanism with its own permissions management, and this capability can be enabled even when the permissions are locked to facilitate a simple wall.

WSM can be used in a mix-and-match style with other NetDocuments security mechanisms such as Profile Based Security, providing great flexibility in managing the security of your content.

**Learn more about managing security policies with Workspace Security Manager by contacting NetDocuments today at (866) 638-3627.**