



Quest[®] Security Explorer[®] 9.9

User Guide



© 2020 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (<https://www.quest.com>) for regional and international office information.


Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, Security Explorer and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Security Explorer User Guide
Updated - June 2020
Software Version - 9.9

Contents

Getting Started with Security Explorer	11
Starting Security Explorer	11
Using the Navigation pane	11
Using the Objects pane	12
Using the Permissions pane	13
Customizing the view	13
Choosing an interface mode	14
Using the Tasks tab	14
Using the status bar	14
Using the loading progress bar	15
Managing module buttons	15
Completing a process	15
Managing permissions	16
Viewing permissions	16
Granting permissions	17
Using the Browse tab to grant permissions	17
Using the Grant task	19
Revoking permissions	19
Using the Browse tab to revoke permissions	20
Revoking permissions on unknown accounts	21
Revoking permissions on disabled accounts	22
Using the Revoke tasks	22
Cloning permissions	23
Using the Browse tab to clone permissions	23
Using the Clone task	26
Creating permission templates	26
Copying permissions	27
Copying permissions to subfolders and files	27
Setting ownership	28
Using the Browse tab to set ownership	28
Using the Set Ownership task	28
Modifying permissions	29
Reducing permissions to read only	30
Managing group memberships	30
Renaming accounts	31
Deleting permissions	31
Deleting permissions by searching	32
Printing permissions	32
Running a report using the Browse tab	33
Running a report using the Reports or Tasks tab	33
Searching	34

Using the Browse tab to search	34
Managing saved searches	35
Adding a search scope	36
Setting search criteria	36
Group and user search criteria	37
Permission search criteria	38
Folder and file search criteria	39
Service and task search criteria	39
Group and user search criteria	39
Advanced search options	40
Registry key search criteria	40
Using the Search tasks	40
Replacing permissions	41
Scheduling a search	41
Managing search tasks	42
Managing security	44
Backing up security	44
Using the Browse tab to back up security	45
Using the Backup task	46
Scheduling a backup	46
Using the backup scheduler	47
Restoring security	48
Comparing security	50
Purging backup files	51
Scheduling a backup purge	51
Exporting security	52
Using the Browse tab to export security	52
Using the Export task	54
Scheduling an export	54
Managing export tasks	55
Managing objects	57
Managing folders and files	57
Creating a new folder	57
Deleting a folder or file	58
Viewing folder and file properties	58
Showing open files	58
Opening files	59
Editing files	59
Opening a folder in Windows Explorer	59
Managing shares	60
Creating a new share	60
Removing a share	60
Finding a share path	61
Managing registry keys	61
Creating a new registry key	61

Deleting a registry key	62
Modifying registry values	62
Managing services	62
Starting, stopping, pausing, or restarting a service	63
Setting logon accounts	63
Changing the password for a logon account	64
Scheduling logon account password changes	64
Removing a service	65
Modifying service properties	65
Managing tasks	66
Running a task	67
Setting account information	67
Creating a new task	67
Copying a task	68
Exporting a task	68
Removing a task	69
Modifying task properties	69
Managing groups and users	69
Viewing accounts	70
Creating a new group	70
Creating a new user	71
Modifying group and user properties	72
Modifying group or user Active Directory properties	72
Modifying properties of multiple users	73
Modifying group memberships	73
Viewing group and user memberships	74
Changing user passwords	75
Modify memberships of multiple local groups	76
Clearing the local administrator group	76
Deleting groups and users	77
Creating a new Managed Service Account	77
Modifying Managed Service Account properties	78
Modifying Managed Service Account Active Directory properties	78
Viewing Managed Service Account memberships	78
Deleting Managed Service Account	79
Managing Favorites	79
Adding Favorites	79
Exporting Favorites	80
Importing Favorites	80
Removing Favorites	81
Managing Enterprise Scopes	81
Creating an Enterprise Scope while browsing	81
Creating an Enterprise Scope	82
Editing an Enterprise Scope	83
Removing an Enterprise Scope	83
Updating licenses	83
Managing network drives	84

Mapping a network drive	84
Disconnecting a network drive	84
Working with Microsoft SQL Server	85
Viewing SQL Server permissions	85
Granting SQL Server permissions	86
Revoking SQL Server permissions	86
Cloning SQL Server permissions	87
Modifying SQL Server permissions	88
Searching for SQL Server objects and permissions	88
Setting SQL Server search criteria	89
Backing up and restoring SQL Server security	90
Exporting SQL Server database permissions	90
Managing SQL Server objects	91
Copying SQL Server objects	91
Copying SQL Server permissions	91
Managing SQL Server databases	92
Managing logins	94
Managing server roles	95
Managing Security SQL Reporting Services	96
Managing system roles	97
Managing catalog roles	97
Managing catalog items	98
Setting options for SQL Server	102
Modifying SQL Server security settings	103
Managing SQL Server network settings	103
Working with Microsoft Exchange	105
Checking minimum requirements	105
Viewing Exchange permissions	106
Granting Exchange permissions	106
Revoking Exchange permissions	107
Cloning Exchange permissions	108
Searching for Exchange server objects and permissions	109
Setting Exchange security search criteria	109
Backing up and restoring Exchange server security	110
Modifying Exchange permissions	110
Managing Exchange group memberships	111
Exporting Exchange security permissions	111
Creating Exchange databases	112
Creating public folder mailboxes	113
Managing Exchange administrators	113
Adding Exchange administrators	113
Modifying Exchange administrators	113
Deleting Exchange administrators	114
Managing Exchange distribution groups	114
Adding distribution groups	114

Modifying distribution groups	114
Deleting distribution groups	115
Managing mail contacts	115
Creating mail contacts	115
Modifying mail contacts	115
Deleting mail contacts	116
Managing mail users	116
Creating mail users	116
Modifying mail users	116
Deleting mail users	117
Managing mailboxes	117
Creating mailboxes	117
Modifying mailbox settings	117
Deleting mailboxes	118
Managing mailbox folders	118
Creating mailbox folders	119
Managing permissions on mailbox folders for multiple users	119
Deleting mailbox folders	119
Managing public folders	119
Creating public folders	120
Modifying public folder settings	120
Deleting public folders	121
Using role based access control	121
Managing user roles	121
Managing role groups	122
Managing roles	123
Managing custom scopes	125
Setting options for Exchange security	126
Working with Microsoft SharePoint	129
Using the SharePoint menu	129
Adding SharePoint farms or sites	130
Managing SharePoint farms or sites	130
Previewing SharePoint objects	131
Deploying the SharePoint web service	131
Deploying the SharePoint web service manually	132
Managing SharePoint permissions	133
Viewing SharePoint permissions	133
Granting SharePoint permissions	134
Revoking SharePoint permissions	134
Cloning SharePoint permissions	135
Modifying SharePoint permissions	136
Modifying SharePoint permissions levels	137
Repairing limited access permissions	137
Removing permissions on deleted accounts	138
Removing permissions on disabled accounts	138
Managing SharePoint groups	139

Removing accounts from SharePoint groups	140
Searching for SharePoint objects	140
Setting SharePoint security search criteria	141
Modifying SharePoint properties	142
Backing up and restoring SharePoint security	143
Exporting SharePoint permissions	143
Deleting export tasks	144
Setting SharePoint options	144
Removing the SharePoint web service	145
Removing the SharePoint web service manually	146
Working with Access Explorer	148
Access Explorer components	148
Managed domain	148
Registered forest	149
Managed computer	149
Access Explorer agent	149
Scopes	150
Database	151
Service accounts	151
Setting up Access Explorer	152
Setting up the Access Explorer database	152
Setting up the first managed domain (includes the service account)	152
Updating Access Explorer configuration	153
Adding managed domains	153
Adding forests	154
Editing managed domains or forests	154
Adding service accounts	154
Editing service accounts	155
Deleting service accounts	155
Collecting Access Explorer data	156
Setting up a managed computer	156
Installing the Access Explorer agent locally	157
Installing the Access Explorer agent remotely	158
Managing managed computers	160
Modifying managed computer properties	161
Managing Access Explorer agents	162
Viewing Access Explorer objects	166
Viewing groups and users	166
Viewing computers	167
Viewing resource groups	167
Viewing permissions	167
Searching Access Explorer servers	167
Using the Access Explorer permission wizard	167
Changing all permissions	168
Cloning all permissions	169
Deleting all permissions	170

Exporting all permissions	171
Backing up permissions	171
Setting options for Access Explorer	171
Working with Microsoft Active Directory	173
Viewing Active Directory permissions	173
Granting Active Directory permissions	174
Revoking Active Directory permissions	175
Cloning Active Directory permissions	175
Searching for Active Directory objects	176
Modifying Active Directory permissions	177
Modifying group memberships	178
Modifying Active Directory properties	179
Deleting Active Directory permissions	179
Backing up and restoring Active Directory security	180
Exporting Active Directory permissions	180
Using the Active Directory Export task	180
Setting options for Active Directory Security	181
Customizing Security Explorer	182
Setting general options	182
Setting view options	184
Setting alternate credentials for workgroups	185
Setting alternate credentials for services and tasks	185
Setting alternate credentials NAS devices	186
Setting advanced options	187
Controlling access to Security Explorer	189
Using the command line	190
Opening a command prompt window	190
SxpBackup.exe	191
SxpClone.exe	191
SxpExport.exe	192
SxpGrant.exe	193
SxpHomeDir.exe	194
SxpInheritance.exe	195
SxpOwner.exe	195
SxpRestore.exe	196
SxpRevoke.exe	196
SXPActiveDirectoryBackup	197
SxpSearch.exe	197
Using PowerShell cmdlets	199
What are cmdlets?	199
Using Security Explorer cmdlets	200
Creating or editing the PowerShell.exe.config file	200
Installing Security Explorer cmdlets	201

Installing Security Explorer cmdlets manually	201
Removing Security Explorer cmdlets	202
Using cmdlets to set up Access Explorer	202
Creating the Access Explorer database	202
Adding a service account	203
Adding a domain to manage	203
Adding managed computers	204
Using cmdlets to get information about Access Explorer objects	205
Getting service account information	205
Getting managed domain information	205
Getting managed computer information	206
Getting security information for a resource	207
Getting resource access information	208
Using cmdlets to manage Access Explorer agents	210
Identifying agents on a managed computer	210
Changing the agent configuration on a managed computer	211
Restarting the agent	212
Restarting a single agent	212
Updating an agent	213
Changing the service account password	213
Changing the SQL account password	214
Using cmdlets to remove Access Explorer objects	214
Removing a managed computer	214
Removing a managed domain	214
Removing a service account	215
Troubleshooting	216
Repairing inheritance	216
Creating test folders and files	216
Using log files	217
SharePoint web service removal fails	217
Uninstalling Security Explorer	218
About us	219
Technical support resources	219

Getting Started with Security Explorer

Quest® Security Explorer® has a robust interface that adapts to the explorer module you select so you are able to focus on the task at hand. In this chapter, you will find information about the overall user interface, such as menus, icons, and adjusting the display.

Topics:

- [Starting Security Explorer](#)
- [Customizing the view](#)
- [Completing a process](#)

Starting Security Explorer

To start Security Explorer

- Click **Start**, point to **All Programs | Quest| Security Explorer**, and choose **Security Explorer**.

i | **NOTE:** Users who are not local administrators can start Security Explorer, but the functionality is limited to actions that do not require local administrator rights.

The first time you open Security Explorer®, the **Browse** tab opens to display three panes. The Navigation pane on the left contains the tree from which you can drill down to objects on your system and the Security Explorer modules available to you. The Objects and Permissions panes are used to further drill down to view the permissions of objects.

Topics:

- [Using the Navigation pane](#)
- [Using the Objects pane](#)
- [Using the Permissions pane](#)

Using the Navigation pane

The Navigation pane on the left contains the tree for the selected module. You can browse the tree and select an object. You can select objects from the local computer, or browse the Network Neighborhood or Active Directory®. You can also group objects into Favorites or Enterprise Scopes. See [Managing Favorites](#) and [Managing Enterprise Scopes](#).

i | **NOTE:** *NTFS Security only.* If you select a network share for which you have no rights to read any resource in that network share, you are presented with a dialog to enter custom credentials. You can save the custom credentials to Windows® Credentials. If you do not save the custom credentials, Security Explorer® uses them until you log off.

The Navigation pane has five tabs.

Table 1. Navigation pane tabs

Tab	Description
Tasks	Display the Home Page for the selected module. You can browse the tree and select tasks from the Home Page, Tool Bar, or Menu Bar. NOTE: The Tasks tab is hidden by default. To view the Tasks tab, select View Tasks tab .
Browse	Display the Browse tab where you can view the Navigation tree. Some options on the Tasks tab automatically open the Browse tab.
Reports	When displaying All Management Targets, the Reports tab lists reports available for all modules. You also can select a specific module and select reports from shortcut menus.
Search	Create search criteria to locate specific permissions. Search becomes available when a module is selected. See Using the Browse tab to search .
Status	Display status of current processes. The information is also available on the status bar, which is hidden by default. See Using the status bar .

Security Explorer is organized around modules: NTFS Security, Share Security, Registry Security, Printer Security, Service Security, Task Management, Group and User Management, SharePoint Security, SQL Server Security, Exchange Security, and Active Directory Security. For example, click the **Share Security** button to manage share permissions or click the **Printer Security** button to manage printer permissions.


Other components of the main window are optional and can be hidden from view. The Menu Bar and Tool Bar provide options and icons to perform functions in Security Explorer. The Loading Progress Bar displays the progress of loading permissions and allows you to stop the load if necessary.

Using the Objects pane

The Objects pane in the **Browse** tab displays the contents of the item selected in the Navigation pane. The path to the object displays in the **Path** box.

NOTE: If you see in the tree in the Navigation pane, the item was loaded from the cache, which is also indicated by CACHE in the status bar. You can disable the cache indicator by clearing the **View indicator when items loaded from cache** check box on the **Tools | Options | Advanced** tab. See [Setting advanced options](#).

Table 2. Objects pane tool bar

Button	Description
	Go up one level in the tree displayed in the Navigation pane.
Go	Go to the path displayed in the Path box. <i>SharePoint Security module only.</i> Add the URL displayed in the Path box to the Favorites list.
Set	Set the root node in the Navigation pane based on the path or URL displayed in the Path box.
Reset	Reset the path to the default selection.
Show All	<i>NTFS Security module only.</i> You can filter the list to show only folders or files, show both folders and files, or show no folders or files.

Using the Permissions pane

The Permissions pane in the **Browse** tab displays the permissions for the object selected in the Objects pane. You can modify permissions of the parent object. If the permissions are inherited and cannot be changed, the list is gray.

- The **Object** box displays the object selected in the Objects pane.
- The **Owner** box displays the owner account name and SID.

Table 3. Permissions pane options

Option	Description
Allow inheritable permissions from parent to propagate to this object	Select this option to propagate permissions to the selected object from the parent. If you select this check box, a warning box displays the selected object and its parent along with the parent's permissions so you can decide whether or not to continue. Inherited permissions display in gray and cannot be changed. If you clear the Allow inheritable permissions from parent to propagate to this object check box, a warning box displays the choices you have for preventing propagation of permissions from the parent. <ul style="list-style-type: none">• To copy the inherited permissions to the object, click Copy.• To remove the inherited permissions, click Remove.
Show Permissions	Select to display permissions (default) for a selected object. Clear the check box to prevent the display of permissions in all windows and dialog boxes. This setting reverts to the default each time you open Security Explorer®.
Show Cluster File Shares	<i>Share Security module only.</i> Select to view cluster file shares when browsing a computer that is a member of a cluster. Cluster file shares display in bold. If selected when the computer is not a member of a cluster, a message displays. NOTE: If the Auto-detect computers that are members of a cluster check box is selected on Tools Options Advanced tab, the check box is selected automatically for computers that are members of a cluster. For computers not members of a cluster, the Show Cluster File Shares check box is disabled even if the Auto-detect computers that are members of a cluster check box is selected. See Setting advanced options .

Customizing the view

Security Explorer® has many interface elements that you can show or hide to customize your experience. The most common operations performed in Security Explorer can be accessed through the tool bar on the **Browse** tab. Other interface options include the **Tasks** tab and the Control Buttons bar. You can show or hide interface elements on the **View** menu.

You can size the panes by dragging the vertical and horizontal split bars. The size of the panes and the selections on the View menu are saved by default. When you start Security Explorer the next time, the display returns as you left it. To restore the display to the factory default, select **View | Reset View to Defaults**, or select **Tools | Options**, and clear the **Reload window state (size and view menu entries)** check box.

Topics:

- [Choosing an interface mode](#)
- [Using the Tasks tab](#)

- [Using the status bar](#)
- [Using the loading progress bar](#)
- [Managing module buttons](#)

Choosing an interface mode

There are three interface modes that you can select from on the View menu: Standard Mode, Classic Mode, and Basic Mode. You also can choose the individual elements to create your own unique interface. No matter which view or options you choose, the same view is restored each time you start Security Explorer®. To reset the options to the default, select **View | Reset View to Defaults**.

Table 4. Interface modes

Interface Type	View Menu Selections
Standard Mode Interface	Tool Bar, Status Bar, and Control Buttons Bar
Classic Mode Interface	Tool Bar, Status Bar, and Control Buttons Bar
Basic Mode Interface	None selected
Reset View to Defaults	None selected

Using the Tasks tab


The **Tasks** tab displays commonly used features in Security Explorer® as icons.

- To use the Tasks tab, select **View | Tasks Tab**.

Using the status bar

The status bar displays along the bottom of the Security Explorer® window. The right-side of the status bar displays the number of selected objects and permissions. **CACHED** indicates that the information displayed was loaded from the cache.

To reload the information

- Click  or **Reload**.
- Press **F5** or **Alt+F5**.
- Select **View | Reload Current Path** or **View | Reload Current Path (No Progress)**.
- On the **Browse** tab, choose **Reload Current Path** from the shortcut menu.

To show or hide the status bar

- Select **View | Status Bar**.

To disable or enable the CACHE feature

- Select **Tools | Options | Advanced** tab. See [Setting advanced options](#).



Using the loading progress bar

The loading progress bar displays the progress when loading large folders or containers, such as registry keys or computers. You can click **Stop** to stop the load, except when Security Explorer® is locating computers. Once the load is complete, click **Reload** to reload objects and permissions.

i | **NOTE:** You can show or hide the loading progress bar from the **View** menu. If you experience slower than expected browsing, you also can show or hide the **Stop** button and the progress display.

Managing module buttons

i | **NOTE:** By default, unlicensed modules display in the Navigation pane. To hide unlicensed module buttons, clear **View | Unlicensed Modules**.

- To hide buttons, drag the split bar down. You also can click , and select **Show Fewer Buttons**.
- To show buttons, drag the split bar up. You also can click , and select **Show More Buttons**.

To show or hide modules

- 1 Click **All Management Targets**.
- 2 Open the **Tasks** or the **Browse** tab.
- 3 Select **View | Filters**.
- 4 Point to **Filters** to view the filter selections. You can choose **All**, **None**, or select specific modules to display.

Completing a process

With most Security Explorer® processes, a progress dialog box displays. When the process is complete, the number of objects processed and the elapsed time displays. The **Errors** area displays any errors that occur during the process.

i | **NOTE:** If any errors occur during processing, you can click **Save Error Log** to save the displayed errors (path and description) to a text (.TXT) file.

Table 5. Progress options

Option	Description
Display progress (clearing this option will speed-up processing)	Select to display the progress in real time. Clear the check box to stop the display.
Close this dialog when processing completes	Select to close the box when the processing is complete. To always close this box, see Setting general options .

Managing permissions

To help you manage security, Security Explorer® is organized into modules, which organize the permissions that are available to manage. First, click the module button that matches the permissions you want to manage. For ease of use, each module functions similarly, although menu choices and buttons may vary from module to module.

i | **NOTE:** This chapter covers managing permissions. While the permissions vary from module to module, the process is basically the same, so several modules are covered in this chapter. Other functions in Security Explorer, including the Task Management and Group and User Management modules, are covered in the [Managing security](#) and [Managing objects](#) chapters.

Topics:

- [Viewing permissions](#)
- [Granting permissions](#)
- [Revoking permissions](#)
- [Cloning permissions](#)
- [Creating permission templates](#)
- [Copying permissions](#)
- [Copying permissions to subfolders and files](#)
- [Setting ownership](#)
- [Modifying permissions](#)
- [Reducing permissions to read only](#)
- [Managing group memberships](#)
- [Renaming accounts](#)
- [Deleting permissions](#)
- [Printing permissions](#)

Viewing permissions

To view permissions

- 1 Open the module that reflects the permissions you want to view.
- 2 Open the **Browse** tab.

–OR–

Open the **Tasks** tab, and click **View Permissions**.

i | **NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

- 3 Select an item in the Navigation pane. The location displays in the **Path** box. The Objects pane displays objects along with the extended information. Depending on how far you drill down in the navigation tree, you may need to select an object in the Objects pane to view permissions.
- 4 If necessary, select an object in the Objects pane. The Permissions pane displays permissions for the selected object. The **Owner** box displays the user or group that owns the selected object.

i **TIP:** If you know the path to the permissions you need, type the path, in either drive letter notation or UNC pathname format, in the **Path** box, and click **Go**.

NOTE: *SharePoint Security module only.* To add a URL to the Favorites list, type the URL in the **Path** box, and click **Go**.

- If the object you chose contains a large number of sub items, you may see a message box. You can choose to show or hide the progress display.
- If loading is taking too long, you can click **Stop** in the loading progress bar. See [Using the loading progress bar](#).
- In the Permissions pane, icons next to each account name indicate the type of user or group. Domain users and disabled users can be highlighted if the option is set on the **Tools | Options | View** tab. See [Setting view options](#).

- 5 Set options for the displayed permissions. See [Using the Permissions pane](#).

Granting permissions

You can grant permissions to users and groups without affecting any other user's permissions. First, choose the permissions to grant, and select a user or group. You can grant different permissions for several users and groups with one operation. In the NTFS Security module, you can create a schedule to temporarily grant a permission.

The type of permission granted depends on the selected module. For example, if you want to grant permissions for a printer, open the Printer Security module.

i **NOTE:** For NetApp Clustered mode, to see changes after a permission action on folders and shares, you must refresh the tree in the Navigation pane.

NOTE: To customize the grant process in the NTFS module, you can set options for modifying permissions. See [Setting advanced options](#).

There are two methods for granting permissions:


- [Using the Browse tab to grant permissions](#)
- [Using the Grant task](#)


Using the Browse tab to grant permissions


To use the Browse tab to grant permissions

- 1 Open the module for the type of permission you want to grant.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane.
–OR–
Type a path in the **Path** box, and click **Go**.
- 4 Select an object in the Objects pane or a permission in the Permissions pane.
- 5 Select **Security | Grant Permissions**.

-OR-

Click , click **Grant** on the Control Buttons Bar; or right-click the object or permission, and choose **Grant Permissions**.

The **Grant Folder Permissions** dialog box displays the path, and the associated groups and users for the current object. The navigation tree is hidden by default. To view the navigation tree, click .

- 6 Select the groups and users to apply the permission. There are a few methods for selecting groups and users.
 - Choose from the list of local and domain groups and users in the navigation tree.
 - To filter the list in the left pane, type a server name or base path in the box, and click **Set**.
 - To return the full list to view, click **Reset**. The list returns to full view the next time you open Grant Permissions.
 - Select from the list of groups and users associated with the current object.
 - To change to another domain or to the local computer, select the domain or the local computer from the **List Names From** list.
 - To display users in the list, click **Show Users**. To return the list to show only groups, click **Refresh**.
 - To select a group/user not displayed, type a name or click **Advanced User Selection**.
 - Browse for a group or user.
- 7 From the Permission list, select the permissions to grant.
 - If you select **Special**, a **Permission** tab specific to the module opens. You also can open the tab by clicking **Advanced Permission Selection**. The **Permission** tab displays the permissions based on the selection in the **Permission** list. If you make any changes, the Permission type changes to Special with the selected permissions in parenthesis.
 - *NTFS security module only.* Selecting the **List Folder Contents** permission grants a Read and Execute permission, but excludes files. The scope for Read and Execute includes files; the scope for List Folder Contents excludes files.
- 8 *Windows Server® 2012 or Windows® 8 only.* In the **Conditions** box, you can type a condition expression or click **Condition Selection** to build an expression.
- 9 From the **Applies To** list, select how to apply the permissions.
- 10 From the **Action** list, select whether to replace or add to the group/user's current permissions.
- 11 To add the group/user to the **List of users and groups to grant** list, click **Add**.
 -  **TIP:** To add additional groups or users to the List of users and groups to grant list with the selected permission settings, you can hold down CTRL or SHIFT, and click a group or user from the list or double-click a group or user in the navigation tree.

- 12 Choose options.

Table 1. Grant options

Option	Description
Overwrite ALL permissions with the groups and users listed below (use with caution)	Select to overwrite the permissions on the selected folders, subfolders, and/or files with the specified permissions.
Include protected objects (objects with 'Inherit Permissions from Parent' disabled)	Select to grant permissions on protected objects.

- 13 *NTFS Security module only.* You can temporarily grant this permission by creating a schedule.

To temporarily grant a permission

- a Click **Schedule**.
- b Type a name for the task and browse for the account under which to run the grant process.
- c Click **OK**.
- d If the task was scheduled successfully, you are asked if you want to open the task. If you see a message that the task is already scheduled, open Windows® Task Scheduler to edit the task.
- e Click **Yes** to open the task.
- f On the **Triggers** tab, click **New**.
- g Set the schedule and click **OK**.

14 Click **OK**. The **Granting Permissions** box displays the progress. See [Completing a process](#).

Using the Grant task

The Grant task provides a quick way to grant permissions. For more options, add at least one path, and click **Switch to Security Explorer Classic (Advanced)**. See [Using the Browse tab to grant permissions](#).

i | **NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To grant permissions using the Grant task

- 1 Open the module for the type of permission you want to grant.
- 2 Open the **Tasks** tab, and click **Grant**.
- 3 Click **Add** to select paths.
- 4 Click **Add** to select permissions.
- 5 To include objects that do not inherit permissions from the parent object, select the check box.
- 6 Click **OK**. The **Granting Permissions** box displays the progress. See [Completing a process](#).

Revoking permissions

You can revoke access for users and groups. The type of permission revoked depends on the selected module. For example, if you want to revoke permissions for a printer, open the Printer Security module.

In the NTFS Security module, you can create a schedule to temporarily revoke a permission.

i | **NOTE:** For NetApp Clustered mode, to see changes after a permission action on folders and shares, you must refresh the tree in the Navigation pane.

NOTE: To customize the revoke process in the NTFS module, you can set options for modifying permissions. See [Setting advanced options](#).

Topics:

- [Using the Browse tab to revoke permissions](#)
- [Revoking permissions on unknown accounts](#)
- [Revoking permissions on disabled accounts](#)
- [Using the Revoke tasks](#)

Using the Browse tab to revoke permissions

To revoke permissions using the Browse tab


- 1 Open the module for the type of permission you want to revoke.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane.


–OR–

Type a path in the **Path** box, and click **Go**.


- 4 Select an object in the Objects pane or a permission in the Permissions pane.
- 5 Select **Security | Revoke Permissions**.

–OR–

Click  on the Tool Bar; click **Revoke** on the Control Buttons Bar; or right-click the object or permission, and choose **Revoke Permissions**.

The **Revoke Folder Permissions** dialog box displays the path, and the associated groups and users for the current object. The navigation tree is hidden by default. To view the navigation tree, click .

- 6 Select the groups and users to revoke the permission. There are a few methods for selecting groups and users.
 - Choose from the list of local and domain groups and users in the navigation tree.
 - To filter the list in the left pane, type a server name or base path in the box, and click **Set**.
 - To return the full list to view, click **Reset**. The list returns to full view the next time you open Revoke Permissions.
 - Select from the list of groups and users associated with the current object.
 - To change to another domain or to the local computer, select the domain or the local computer from the **List Names From** list.
 - To display users in the list, click **Show Users**. To return the list to show only groups, click **Refresh**.
 - To select a group/user not displayed, type a name or click **Advanced User Selection**.
 - Browse for a group or user.
- 7 From the **Permission** list, select the permissions to revoke, and whether or not to Allow or Deny. If the choice is not available in the list, click **Advanced Permission Selection** to create a custom choice.
- 8 To add the group/user to the **List of users and groups to revoke** list, click **Add**.

 **TIP:** To add additional groups or users to the List of users and groups to grant list with the selected permission settings, you can hold down CTRL or SHIFT, and click a group or user from the list or double-click a group or user in the navigation tree.

- 9 Choose options.

Table 2. Revoke options

Option	Description
Revoke all permissions (Allow and Deny) for the selected user	<i>Not available in the Task Management and Groups and Users modules.</i> Select to revoke all permissions (Allow and Deny) for the selected user.
Include SID history search when adding permissions for revoking	Select to invoke a SID history search when you click Add to add the selected group/user to the List of users and groups to revoke list. Since there may be more than one SID associated with the selected account, selecting this check box adds all existing SIDs to the List of users and groups to revoke list so that all existing permissions are revoked.
Advanced Revoke Options	If you select this check box, a warning message displays and the Revoke Folder Permissions dialog box becomes inactive, so the other users/groups and permissions you selected are not included in this action. To continue, click Yes .
Revoke all unknown and deleted accounts	Select to revoke permissions on unknown or deleted accounts.
Revoke all disabled accounts	Select to revoke permissions on all disabled accounts.
Log Actions	Select to create a log file. Browse to name the log file.
Include protected objects (objects with 'Inherit Permissions from Parent' disabled)	Select to revoke permissions on protected objects.

10 *NTFS Security module only.* You can temporarily revoke this permission by creating a schedule.

To temporarily revoke a permission

- a Click **Schedule**.
- b Type a name for the task and browse for the account under which to run the revoke process.
- c Click **OK**.
If the task was scheduled successfully, you are asked if you want to open the task. If you see a message that the task is already scheduled, open Windows® Task Scheduler to edit the task.
- d Click **Yes** to open the task.
- e On the **Triggers** tab, click **New**.
- f Set the schedule and click **OK**.

11 Click **OK**. The **Revoking Permissions** box displays the progress. See [Completing a process](#).

Revoking permissions on unknown accounts

You also can use the Revoke Unknown advanced task to revoke all permissions on unknown and deleted accounts. See [Using the Revoke tasks](#).

To revoke all permissions on unknown accounts

- 1 Open the module for the type of permission you want to revoke.
 - 2 Open the **Browse** tab.
 - 3 Select an item in the Navigation pane.
- OR–
- Type a path in the **Path** box, and click **Go**.

- 4 Select **Advanced Revoke Options**.
- 5 Click **Yes**.
- 6 Select **Revoke all unknown and deleted accounts**.
- 7 Click **OK**. The **Revoking Permissions** box displays the progress. See [Completing a process](#).

Revoking permissions on disabled accounts

You also can use the Revoke Unknown advanced task to revoke all permissions on disabled accounts. See [Using the Revoke tasks](#).

To revoke all permissions on disabled accounts

- 1 Open the module for the type of permission you want to revoke.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane.
–OR–
Type a path in the **Path** box, and click **Go**.
- 4 Select **Advanced Revoke Options**.
- 5 Click **Yes**.
- 6 Select **Revoke all disabled accounts**.
- 7 Click **OK**. The **Revoking Permissions** box displays the progress. See [Completing a process](#).

Using the Revoke tasks

The Revoke task provides a quick way to revoke permissions. You also can use the Revoke All, Revoke Unknown, Revoke Disabled, and Revoke SID History advanced tasks to easily revoke permissions for those specific situations. For more options, add at least one path, and click **Switch to Security Explorer Classic (Advanced)**. See [Using the Browse tab to revoke permissions](#).

i | NOTE: The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To revoke permissions using the Revoke tasks

- 1 Open the **Tasks** tab.
- 2 Open the module for the type of permission you want to revoke, and click **Revoke**, **Revoke All**, **Revoke Unknown**, **Revoke Disabled**, or **Revoke SID**.
- 3 Click **Add** to select paths.
- 4 If you clicked **Revoke** or **Revoke All**:
 - Click **Add** to select permissions.
 - To include objects that do not inherit permissions from the parent object, select the check box.
- 5 Click **OK**. See [Completing a process](#).

Cloning permissions

Use the Clone feature to copy individual permissions, permissions in an entire domain, or permissions relating to a user's SID history. The type of permission cloned depends on the selected module. For example, if you want to clone permissions for a printer, open the Printer Security module.

- NOTE:** For NetApp Clustered mode, to see changes after a permission action on folders and shares, you must refresh the tree in the Navigation pane.
- NOTE:** To customize the clone process in the NTFS module, you can set options for modifying permissions. See [Setting advanced options](#).


Topics:

- [Using the Browse tab to clone permissions](#)
- [Using the Clone task](#)

Using the Browse tab to clone permissions

To clone permissions using the Browse tab

- 1 Open the module for the type of permission you want to clone.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane.
- OR–
- Type a path in the **Path** box, and click **Go**.
- 4 Select an object in the Objects pane or a permission in the Permissions pane.
- 5 Select **Security | Clone Group or User**.
- OR–

Click  on the Tool Bar, click **Clone** on the Control Buttons Bar; or right-click the object or permission, and choose **Clone Group or User**.

The **Clone Folder Permissions** box opens to the **Manual User/Group Selection** tab and displays the path to the selected object and the associated groups and users.

There are five ways to select users and groups for cloning:

- To select individual users and groups to clone, use the **Manual User/Group Selection** tab. See [Selecting users and groups manually](#).
 - To select entire domains to clone, use the **Automatic User/Group Selection** tab. See [Selecting users and groups automatically](#).
 - To update Access Control Lists (ACLs) with SIDs relating to the user's SID in the new domain, use the **SID History** tab. See [Updating permissions relating to a user's SID history](#).
 - To import a .CSV file of users/groups to clone, use the **Import User/Group Selection** tab. See [Importing users and groups](#).
 - To load a previously saved Security Explorer Clone List (.dat), click **Load**. *Not available in the SQL Server Security, SharePoint Security, and Exchange Security modules.*
- 6 Select options.

Table 3. Clone options

Option	Description
Clone Permissions	By default, permissions are cloned.
Clone Ownership	Select to clone ownership.
Clone group memberships	Select to add the destination account to the groups of which the source user is a member. If you choose this check box, a warning message displays. The destination is cloned into the same parent groups as the source. The contents of the groups selected as the source are not cloned.
Replace source permissions with destination permissions	Select to change the source permissions to match the destination permissions.
Include protected objects when cloning (objects with 'Inherit Permissions from Parent' disabled)	<i>Not available in the SQL Server Security, SharePoint Security, Exchange Security, and Active Directory Security modules.</i> Select to include those objects for which the Allow inheritable permissions from parent to propagate to this object check box is unavailable. See Viewing permissions .

- 7 To save the selections as a Security Explorer Clone List (.dat) for reuse, click **Save**. *Not available in the SQL Server Security, SharePoint Security, Exchange Security, and Active Directory modules.*
- 8 Click **OK**. See [Completing a process](#).

Selecting users and groups manually

With the manual method, you select permissions one at a time. For example, use the **Manual User/Group Selection** tab to clone the permissions on the Everyone group to the BobV user account. The BobV user account will have the same access rights as the Everyone group

To select users and groups manually

- 1 Open the **Manual User/Group Selection** tab.
- 2 In the **Source Group or User** area, select the domain or object from which to pull the permissions. The default is the current object, whose path displays in the top box.

In the **Destination Group or User** area, select the domain or object to receive the cloned permissions. The default is the current object, whose path displays in the top box.

- To add all users to the **Source** and **Destination** lists, click **Show Users**.
- To select a specific user to add to the **Source** and **Destination** lists, click **Advanced User Selection**.
- To return the **Source** and **Destination** lists to groups only, click **Refresh**.

i | IMPORTANT: Do not select a pair of accounts where the source is the same as the target. The permissions for the accounts will be deleted as a result of the cloning process.

- 3 Click **Add**.
- 4 Continue with step 6 of the clone process. See [Using the Browse tab to clone permissions](#).

Selecting users and groups automatically

The Clone feature is useful when you are migrating domains. After you create all the new groups and users in the new domain, use the **Automatic User/Group Selection** tab to copy the permissions from the old domain to the new domain.

i | **NOTE:** The Automatic User/Group Select tab is not available in the SQL Server Security, SharePoint Security, Exchange Security, and Active Directory Security modules.

TIP: You also can use the Auto Clone advanced task to automatically pair accounts for cloning. Once you enter a path, and click **OK**, the **Automatic User/Group Selection** tab opens with the path list automatically populated.

To select users and groups automatically

- 1 Open the **Automatic User/Group Selection** tab.
- 2 From the **Source** list, select the domain to use as the source.
- 3 From the **Destination** list, select the domain to use as the destination.
- 4 Select to search for groups and/or users.
- 5 Click **Start Automatic Selection**.
- 6 Scroll through the list of pairs that display in the bottom pane and remove any pairs you do not want to clone.
- 7 Continue with step 6 of the clone process. See [Using the Browse tab to clone permissions](#).

Updating permissions relating to a user's SID history

Use SID History to update Access Control Lists (ACLs) with SIDs relating to the user's SID in the new domain.

i | **NOTE:** You also can update ACLs with SIDs in the Group and User Management module. Right-click one or more domain users, choose **Clone Permissions (using SID History)**, and choose the path. The SID History tab displays any pairs found.

To select users and groups based on SID history

- 1 Open the **SID History** tab.
- 2 In the **Domain** and **AD Query** boxes, create a query filter to find the user or group in Active Directory®.

i | **NOTE:** For assistance in constructing a query filter, see [Creating a Query Filter](#).

To display a progress bar while Security Explorer® searches Active Directory, select the **Display Progress** check box.

- 3 Click **Find SID History Accounts**.

Security Explorer finds a set of groups and users based on the specified domain and AD query, and steps through each of the groups and users looking for any SID history.

When the process is complete, the number of groups and users checked display.

- 4 Click **Close**.
- 5 To see the groups and users checked during the process, click **Browse SID History**.

The **Browse SID History** dialog box displays the domain and AD query entered on the **SID History** tab. You can change the domain and AD query, if necessary.

- To include the SID in the display, select the **Include SID** check box.

- 6 Click **Load**. The groups and users are listed as they are checked.
 - To sort the list in alphabetical order, click **Sort**.
 - If you selected the **Include SID** check box, you can use the scroll bar to view the entire SID, or point the cursor to group or user.
- 7 Continue with step 6 of the clone process. See [Using the Browse tab to clone permissions](#).

Importing users and groups

You can import source/destination pairs for cloning. The CSV file must contain a list of source and destination accounts, where each pair is separated by a new line and the source and destination are separated by a comma. For example: ACME\BSmith,ACME\JAdams.

To import users and groups from a .CSV file

- 1 Open the **Import User/Group Selection** tab.
- 2 Type the path to the import file or browse for the file.
- 3 Specify optional domain controllers for both the source account and the destination account. The domain controller is used to perform a SID lookup during the import operation.
- 4 Click **Execute Import**.
- 5 Continue with step 6 of the clone process. See [Using the Browse tab to clone permissions](#).

Using the Clone task

The Clone task provides a quick way to clone permissions. For more options, add at least one path, and click **Switch to Security Explorer Classic (Advanced)**. See [Using the Browse tab to clone permissions](#).

You also can use the Auto Clone advanced task to automatically pair accounts for cloning. See [Selecting users and groups automatically](#).

i | **NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To clone permissions using the Clone task

- 1 Open the **Tasks** tab.
- 2 Open the module for the type of permission you want to clone, and click **Clone**.
- 3 Click **Add** to select paths.
- 4 Click **Add** to select the source and destination accounts. You can type the account or click **Advanced User Selection** to choose an account.
- 5 Click **OK**. See [Completing a process](#).

Creating permission templates

Security Explorer® provides six built-in permission templates that you can use to apply permissions. You cannot modify the built-in permission templates, but you can create custom permission templates.

To create a permission template

- 1 Open the **NTFS security** module.
- 2 Select **Security | Permission Templates**.

The **NTFS Permission Templates** dialog box displays the Full Control permission template. The other built-in templates are Modify, Read and Execute, List Folder Contents, Read, and Write.

i | **NOTE:** If you want to edit an existing custom template, select it from the list, and go to step 4. You cannot modify built-in templates.

- 3 To create a new permission template, click **New**.
- 4 Type a name for the template, and click **OK**.



- 5 Select or clear the check boxes to create the template.
- 6 Click **Close**. When you apply permissions, the template is available for selection.

Copying permissions

To save time when granting permissions, you can copy and paste permissions.

- NOTE:** The Copy Permissions function is not available in the Task Management, Group and User Management, and Active Directory Security modules.
- NOTE:** For NetApp Clustered mode, to see changes after a permission action on folders and shares, you must refresh the tree in the Navigation pane.

To copy permissions

- 1 Locate the permission(s) to copy. See [Viewing permissions](#).
 - 2 Select a permission.
To select all permissions in the list, select **Security | Select All**.
-OR-
Press **Ctrl-A**; or right-click any permission, and choose **Select All**.
 - 3 Select **Security | Copy Permissions**.
-OR-
Click  on the Tool Bar; press **Ctrl-C**; or right-click the permission, and choose **Copy Permission**.
 - 4 Open the object where you want to paste the selected permissions.
 - 5 Select **Security | Paste Permission**.
-OR-
Click  on the Tool Bar; press **Ctrl-V**; or right-click any permission, and choose **Paste Permission**.
The **Grant Folder Permissions** dialog box opens showing the pasted permissions in the **List of users and groups to grant** list.
 - 6 Complete the Grant process. See [Granting permissions](#).
- NOTE:** If the same permission exists in the object, the copied permission overwrites the permission. If the permission does not exist, the copied permission is added to the object.

Copying permissions to subfolders and files

You can copy permissions from a parent folder to its subfolders and files. The permissions on the parent folder do not change; the subfolders and files inherit the permissions from the parent. Use the **Copy Security** basic task to copy permissions from multiple folders.

- NOTE:** For NetApp Clustered mode, to see changes after a permission action on folders and shares, you must refresh the tree in the Navigation pane.

To copy permissions to subfolders and files

- 1 Open the **NTFS Security** module.

- 2 To copy permissions from one folder, select a folder in the Navigation pane, and select **Security | Copy to Subfolders and Files**.

To copy permissions from multiple folders, open the **Tasks** tab, select a folder in the Navigation pane, and click **Copy Security**. The path appears in the **Paths** list. Click **Add** to select additional paths, and click **OK**.

A warning message displays. If you proceed with the copy, all explicitly-defined permissions on all child subfolders and files are removed. The child subfolders and files inherit permissions from the parent.
- 3 Click **Yes**. See [Completing a process](#).

Setting ownership

You can set the owner on a file or folder, which is very helpful when setting up home directories. Choose the user or group to be the owner of the file or folder, and choose how to apply the ownership.

Topics:


- [Using the Browse tab to set ownership](#)
- [Using the Set Ownership task](#)

Using the Browse tab to set ownership

To set ownership using the Browse tab

- 1 Open the **NTFS Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Object pane, select an object.
- 4 Select **Security | Set Ownership**.

-OR-

Click  on the Tool Bar; or right-click the object, and choose **Set Ownership**.
- 5 Type an account in the **Owner** box or select a group from the list.

i | NOTE: By default only groups display. To view a list of users, click **Advanced User Selection**.
- 6 Choose whether to set the ownership on files and/or folders. To target specific file types, enter a wildcard, such as *.exe. You also can choose to recurse across subfolders.

i | NOTE: To grant permissions to the current folder only, clear all check boxes in the **Folder Options** area. To grant permissions to all files and folders, and recurse through all subfolders, select all check boxes.
- 7 Click **OK**. See [Completing a process](#).

Using the Set Ownership task

The Set Ownership task provides a quick way to set ownership on folders and files. For more options, click **Switch to Security Explorer Classic (Advanced)**. See [Using the Browse tab to set ownership](#).

- i | NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To set ownership using the Set Ownership task

- 1 Open the **NTFS Security** module.
- 2 Select the folder or file in the Navigation pane.
- 3 Open the **Tasks** tab, and click **Set Ownership**.
- 4 Click **Add** to select paths.
- 5 Type an account or browse to select an account.
- 6 Click **OK**. See [Completing a process](#).

Modifying permissions

Modify the permissions of groups or users on the selected folder or file. Use this feature for quick changes to accounts displayed in the permissions list. Use the Grant feature to give permissions to accounts that are not displayed in the permissions list. See [Granting permissions](#).

- i** | **IMPORTANT:** You cannot modify inherited permissions directly. Inherited permissions are indicated by **Allow (I) in the Type** column. To modify these permissions, you must modify the parent object
- NOTE:** For NetApp Clustered mode, to see changes after a permission action on folders and shares, you must refresh the tree in the Navigation pane.
- NOTE:** For the NTFS Security module, you can set options for modifying permissions. See [Setting advanced options](#).
- NOTE:** The ability to select multiple permissions to modify is limited to the NTFS Security module.

To modify permissions


- 1 Locate the permissions to modify. See [Viewing permissions](#).
 - i** | **NOTE:** The permissions listed vary depending on the module and object selected. If you want to change the display to different users or groups, click **Change**.
- 2 Select the permissions.
 - i** | **NOTE:** If you choose multiple permissions, the selected permissions must be under the same path or object. If the paths are not the same, you receive a warning message.
- 3 Select **Security | Modify Permission**.
-OR-
Click  on the Tool Bar, click **Modify** on the Control Button Bar; or right-click the permissions, and choose **Modify Permission**.
- 4 From the **Permissions** lists, select the permission and how to apply it. The resultant permissions display in the check boxes. If you make changes to the check boxes, the permission type changes to Special Access.
 - i** | **NOTE:** You also can create custom permission templates to refer to non-standard sets of permissions. See [Creating permission templates](#).
- 5 Select whether to modify permissions on protected objects manually (default) or automatically.

Table 4. Modify options

Option	Description
Only apply permissions to objects directly inside this folder (No Propagate)	Select to apply the permissions inside the current folder. Permissions are not propagated down the directory tree.
Include protected objects	Select to modify permissions on the selected account down the directory tree even if a file or folder is protected.

- 6 Click **OK**.

You are asked to verify that the selected permissions will be revoked and the new permissions you selected will be granted.

- 7 Click **Yes**.

Reducing permissions to read only

You can quickly reduce permissions on an object to Read Only.

To reduce permission to read only

- 1 Open the **NTFS security** module.
- 2 Open the **Browse** tab, select an object, and select **Security | Reduce to Read Only**.

-OR-

Click  on the Tool Bar; or open the **Task** tab, click **Reduce to Read Only**, add a path, and click **OK**.

The **Grant Folder Permissions** box displays the Read configuration for all users for the selected object. See [Using the Browse tab to grant permissions](#).

- 3 Click **OK**.

Managing group memberships

- NOTE:** The Manage Group feature is not available in the Task Management or SQL Security modules.
- To manage groups in the SharePoint Security module, see [Managing SharePoint groups](#).
 - To manage groups in the Group and User Management module, see [Managing groups and users](#).

To manage group memberships

- 1 Open the module for the type of group membership you want to manage.
- 2 Select to view either a group or a user.
 - To view the members of a selected group, select **Tools | Display Group Contents**.

-OR-

Click **Contents** in the Control Button Bar; or right-click a group, and choose **Display Group Contents**.

 - To view the groups of which a selected user is a member, select **Tools | Display Memberships**.

-OR-

Right-click a user and choose **Display Memberships**.
- 3 Select a user or group, and click a button corresponding to the action you want to perform.

Table 5. Manage group membership options

To:	Click:
Add members to the selected group.	Add
Remove selected members from the selected group.	Remove
Refresh the list after adding or removing a member	Refresh
Print the list	Print
Save the list as a .txt file	Save
View the members of a selected group	Show Group Contents
Show the groups of which the selected group or user is a member	Show Memberships
Close the Group contents box	Close

Renaming accounts

To rename accounts

- 1 Locate the type of permission for the account to rename. See [Viewing permissions](#).
- 2 In the Permissions pane, right-click a group or user, and choose **Rename Group or User**.
- 3 Type a new name. Do not include any domain information.
- 4 Click **OK**.


Deleting permissions


- i** **NOTE:** You cannot delete inherited permissions, which are indicated by **Allow (I) in the Type** column of the Permissions pane. Navigate up the directory tree to locate the parent, and continue with the delete process.
- TIP:** *NTFS Security module only.* If you want to delete both explicit and inherited permissions, use the Search module. See [Deleting permissions by searching](#).
- NOTE:** For NetApp Clustered mode, to see changes after a permission action on folders and shares, you must refresh the tree in the Navigation pane.
- NOTE:** To customize the delete process in the NTFS module, you can set options for modifying permissions. See [Setting advanced options](#).

To delete permissions

- 1 Locate the type of permission to delete. See [Viewing permissions](#).
- 2 In the Permissions pane, select the permission(s), and select **Security | Delete Permission**.

-OR-

Click  on the Tool Bar, click **Delete** on the Control Button Bar; or right-click the selected permission(s), and choose **Delete Permission**.

- i** **IMPORTANT:** If permission(s) are not selected when you click  on the Tool Bar or click **Delete** on the Control Button Bar, the currently selected object(s) (folders, files, registry keys, or services) are deleted.

- 3 Determine if you want to force deletion down the entire tree, including protected objects, even if a file or folder is protected. (*NTFS and Registry Security modules only*)

- 4 To delete the permission(s), click **Yes**.

Deleting permissions by searching

NTFS Security module only. You can use the Search module to easily delete both explicit and inherited permissions on a specific user on specified folders.

To delete permissions by searching

- 1 Set the search scope to indicate the parent location. See [Adding a search scope](#).
- 2 On the **Group/User Search Criteria** tab, specify the group/user. See [Group and user search criteria](#).
- 3 On the **Permission Search Criteria** tab, select the **Inherited Permissions** and **Explicit Permissions** check boxes. See [Permission search criteria](#).
- 4 On the **File and Folder Search Criteria** tab, specify the folders and files, if necessary. See [Folder and file search criteria](#).
- 5 From the search results, delete selected permissions.

Example

Peter has explicit access permission on the Customer folder, and all subfolders have inherited permissions. You want to remove Peter's permission on all folders with Internal in the folder name.

- C:\Customer\ Internal1\
- C:\Customer\ Internal1\Internal2
- C:\Customer\ Mixed\Internal3
- C:\Customer\ External1\

To delete Peter's permissions on the Internal folders

- 1 Open the **Search** tab.
- 2 Add the search scope C:\Customer.
- 3 On the **Group/User Search Criteria** tab, browse to locate Peter's account.
- 4 On the **Permission Search Criteria** tab, select **Inherited Permissions** and **Explicit Permissions**.
- 5 On the **File and Folder Search Criteria** tab, type ***Internal*** as a wildcard.
- 6 Click **Search**.
All permissions that belong to Peter on all folders with Internal in the name display.
- 7 From the search results, delete selected permissions.

Printing permissions

Use the **Reports** tab to run reports easily. The **Reports** tab displays all the available reports. Reports specific to a particular module are available on the **Tasks** tab.

Topics:

- [Running a report using the Browse tab](#)
- [Running a report using the Reports or Tasks tab](#)

Running a report using the Browse tab

There are three ways you can create a report on the **Browse** tab.

To run a report from the Browse tab

- Search for permissions, and click **Report**. See [Using the Browse tab to search](#).
- Export permissions, and select **Generate Report** as the output. See [Exporting security](#).
- Select **File | Print** to format the permissions displayed in the Permissions pane for printing. *Available only in the NTFS Security, Share Security, Registry Security, Printer Security, and Service Security modules.*

Running a report using the Reports or Tasks tab

To run a report from the Reports or Tasks tab

- 1 Open the **Reports** tab or open the module **Tasks** tab for the type of report you want to create.

i | NOTE: The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

For more options, add at least one path, and click **Switch to Security Explorer Classic (Advanced)**. See [Running a report using the Browse tab](#).

- 2 Select the report, and click **Add** to select paths.
- 3 Select how to create the report.

Table 6. Generate report options

Option	Description
Generate a report by executing a simple report	<i>Not available in the Registry Security or Printer Security modules.</i> Select to create the same report you could create by exporting permissions. See Exporting security . <ol style="list-style-type: none">1 Click OK. See Completing a process.2 When the process is complete, click Close. You can save, print, or export the report.
Generate a report by searching for permissions	<i>Not available in the SharePoint Security module.</i> Select to create the same report you could create by searching for permissions. The search is based on the default selections. See Using the Browse tab to search . When you click OK , a message box displays and the search opens a new window. If the search is taking too long, click Stop Search or Stop . <ol style="list-style-type: none">1 Click OK. The Search results display. You can choose to set more criteria and start the search again. See Setting search criteria.2 When the search is complete, click Report. You can save, print, or export the report.

Searching

Have you ever wondered just which files and directories on your network the group Everyone can delete permissions on? Finding information like this is a snap with Security Explorer®. Simply choose a group or user, and a set of permissions to search for, and begin your search. When the search results display, you can click on any files or directories in your search results to modify their permissions immediately.


i | **NOTE:** For searching the SQL Security module, see [Searching for SQL Server objects and permissions](#). For searching the Exchange Security module, see [Searching for Exchange server objects and permissions](#). For searching in SharePoint Security module, see [Searching for SharePoint objects](#). For searching the Active Directory Security module, see [Searching for Active Directory objects](#).

Topics:

- [Using the Browse tab to search](#)
- [Managing saved searches](#)
- [Adding a search scope](#)
- [Setting search criteria](#)
- [Using the Search tasks](#)
- [Replacing permissions](#)
- [Scheduling a search](#)
- [Managing search tasks](#)

Using the Browse tab to search

To use the Browse tab to search

- 1 Open the module for the type of search.
- 2 Open the **Browse** tab.
- 3 Select an object in the Navigation or Objects pane, and select **Search | New Search Window (Empty)**.
-OR-
Click , press **Shift + F3**, or right-click an object, and choose **Search in a New Window**.
- 4 If you want to change the search scope, see [Adding a search scope](#).
- 5 Add criteria for the search. See [Setting search criteria](#).
- 6 Click **Start Search**.

The **Permissions** column in the Permissions pane may list abbreviations of some permissions.

To see what permissions are set, right-click the permission, and choose **Modify Permission**.

-OR-

Click **Modify** in the Control Button bar, or select **Security | Modify Permission**.

- 7 Select **Auto-update results** to automatically update the search results after you select to grant, revoke, clone, replace, modify, or delete a permission. The search is performed again during the refresh, so if you have a search that takes a long time, you may want to clear this check box.
- 8 Use the buttons to manage the results. You can save the search, save the search results, generate a report, or export the results.

Table 1. Search tab buttons

Button	Description
Add Scope	Add a Search Scope, which is what you want to search, such as domains, computers, or folders. See Adding a search scope .
Load from Share	<i>NTFS Security module only.</i> Load saved search scope and criteria from an XML file exported from the Share Security module.
Load from NTFS	<i>Share Security module only.</i> Load saved search scope and criteria from an XML file exported from the NTFS Security module.
Save	Save the Search Scope and selected criteria to reuse at a later time. The saved search displays under User Searches.
Start Search	Start the search based on the current Search Scope and selected criteria.
Stop Search	Stop the search process.
Clear Results	Clear the results area.
Defaults	Return to the default selections on all search criteria tabs.
Save Results	Save the results as a .txt file.
Report	Display the results in a report format that you can save, print, or export.
Export	<i>Service Security and Task Management modules only.</i> Export the results. See Using the Browse tab to export security .
Schedule	Schedule a search using the current Search Scope and selected criteria. See Scheduling a search .

Managing saved searches

You can save the search scope and selected criteria to reuse. You also can export the scope and settings to an XML file for later import into another module. Saved searches appear under **Saved Searched | User Searches**.

To managed saved searches

- Right-click a saved search, and choose from the menu.

Table 2.

Option	Description
Load	Load a saved search to run.
Delete Saved Search	Delete the saved search.
Import	Import the search scope and search criteria from an exported XML file. NOTE: You can only import an XML file that was exported from the same module with the exception of the NTFS Security and Share security modules. In these modules, you can import an XML file that was exported by the other module.
Export	Export the search scope and search criteria to an XML file.

Adding a search scope

The Search Scope determines what objects to search, such as domains, computers, or folders.

To add a search scope

- 1 Click **Add Scope**.
- 2 Select from the tree.

-OR-

Type a location (*all modules*) or LDAP path (*Service Security and Active Directory Security modules only*) in the box. If you enter a location or LDAP path, you must select a type: Domain, Computer, Folder (*NTFS Security module only*), AD Forest, AD OU, or AD Container (*Service Security module only*).

i **TIP:** Use the **Select all children for the current item** or **De-select all children for the current item** check boxes to help you create the scope.

NOTE: In the Service Security module, you can import a list of servers. Click **Import**, and choose a text file.

NOTE: In the Group and User Management module, you can select individual computers, computers in a Network node, or Active Directory® organizational units and containers that contain computers. When the Active Directory tree is used in the search scope, Security Explorer® searches only local users and groups for the computers in the selected organizational unit or container, or local users and groups for selected computers. Security Explorer does not search domain users and groups in Active Directory. If you want to search for domain users and groups, select computers in the Network node.

- 3 Click **OK**.

i **NOTE:** In the Group and User Management module, you can select to save any failed computers to the search scope to repeat the search with only the failed computers. This option is helpful when trying to reset passwords. You can repeat the search with the failed computers, right-click the results, and choose **Change Password**. See [Changing user passwords](#).

Setting search criteria

Each module has a set of search criteria grouped into tabs. As you set criteria, you can update the results by clicking **Start Search** at any time.

Topics:

- [Group and user search criteria](#)
- [Permission search criteria](#)
- [Folder and file search criteria](#)
- [Service and task search criteria](#)
- [Group and user search criteria](#)
- [Advanced search options](#)
- [Registry key search criteria](#)

Group and user search criteria

Table 3. Group and user search criteria options

Option	Description
Group/User	Type groups or users separated by semi-colons in the Group/User box, or click Browse or Advanced User Selection to browse for groups or users.
SID	<p>Type a full or partial SID to search. You can use the * wildcard to match any number of characters. Use the ? wildcard to match a single character. The comparison is not case sensitive.</p> <p>You might pair the SID search with other search options, such as Include group results, Include user results, Search for unknown accounts, Search for permissions (DACL), and Search for owner.</p>
Include all group memberships	<p><i>Disabled if there is more than one group or user in the Group/User box.</i> Select to include all groups of which the selected group or user is a member.</p> <p>NOTE: To search for Access Explorer Memberships, select an Access Explorer server, and select Include all group memberships and Include nested group memberships.</p>
Include nested group memberships	<i>Active only when the Include all group memberships check box is selected.</i> Select to include any accounts that may be nested under the parent account.
Include "BUILTIN\Users" memberships	<i>Active only when the Include all group memberships check box is selected.</i> Select to include the permissions for BUILTIN\Users if the account entered in the Group/User box is a member of the BUILTIN\Users group.
Include "Domain Users" memberships	<i>Active only when the Include all group memberships check box is selected.</i> Select to include the permissions for Domain Users if the account entered in the Group/User box is a member of the Domain Users group.
Include "Everyone" Group	Select to include the Everyone group in the search.
Include "Authenticated Users" Group	Select to include the Authenticated Users group in the search.
Include "Network" Group	Select to include the Network group in the search.
Include "Interactive" User	Select to include the Interactive user in the search.
Include group results	<i>Applies only to NTFS Security module.</i> Select to include groups in the search.
Include user results	<i>Applies only to NTFS Security module.</i> Select to include users in the search.
Search for unknown accounts	Select to include unknown accounts in the search.
Search for disabled accounts	Select to include disabled accounts in the search.
Include SID history	Select to include a SID history search. If any additional SIDs are found in the history, these additional SIDs are included in the search with the primary SID.
Show Only SID history permissions	<i>Applies only to NTFS Security module. Active only when the Include SID history check box is selected.</i> Select to display only the SID history permissions.

Permission search criteria

Table 4. Permission search criteria options

Option	Description
Search for permissions (DACL)	<i>Applies only to NTFS Security module.</i> By default, the Discretionary Access Control List (DACL) is searched for any allow or deny permissions. Inherited and explicit permissions are included.
Search for owner	<i>Applies only to NTFS Security module.</i> Select to include the owner of the selected file or folder in the search.
Folder File	In the boxes, select the permissions to search. Browse to define special permissions in the NTFS Security module. To define special permissions in the Share Security, Registry Security, and Printer Security modules, click Advanced Permission Selection .
Search for exact permissions (as set above)	Perform the search using the exact permissions settings. For example, if you search for Write (W), only that permission is included in the results. NOTE: Selecting some permissions, such as Write (W), select other permissions automatically (Rp, Ad, Wd, Wa, Wx). If you do not want to include those permissions in the results, click Advanced Permission Selection to manually clear those selections.
Search for exact permissions or better	Include the exact permissions settings, along with any other permissions that include the permissions specified. For example, if you search for Write (W), Full Control (All) is also included in the results, along with any Special permissions that include Write (W).
Invert results set (applies to DACL only)	Select to search for permissions other than those specified. For example, if you are searching for Write (W), the search results return all permissions except Write (W). NOTE: Selecting some permissions, such as Write (W), select other permissions automatically (Rp, Ad, Wd, Wa, Wx). If you select the Invert permissions result set check box, those permissions are not included in the results. If you want to include those permissions in the results, click Advanced Permission Selection to manually deselect those permissions. This rule does not apply to Full Control (All), so even though you searched for permissions other than Write (W), Full Control (All) is included in the results.
Search cluster file shares	<i>Applies only to Share Security module.</i> Select to search cluster file shares. Cluster file shares display in bold.
Inherited Permissions	<i>Applies only to NTFS Security module.</i> Includes inherited permissions in the search results. Inherited permissions are indicated by (I) in the Type column.
Explicit Permissions	<i>Applies only to NTFS Security module.</i> Includes explicit permissions in the search results.
Show duplicate permissions (advanced search option) (i.e., explicit ACE's where there is an exact matching inherited ACE)	<i>Applies only to NTFS Security module.</i> Select to show duplicate permissions, that is explicit ACEs where there is an exact matching inherited ACE.
Protected Folders/Files Only (i.e., folders/files which do not inherit permissions from their parent	<i>Applies only to NTFS Security module.</i> Select to search only protected folders/files, which are those folders/files that do not inherit permissions from their parent.

Folder and file search criteria

Applies to NTFS Security module only. By default, a search includes folder and file permissions and all subfolders.

Table 5. Folder and file search criteria options

Option	Description
Search for folder permissions	Select to include folder permissions in the search results.
Search for file permissions	Select to include file permissions in the search results.
Recurse all subfolders	Select to include all subfolders in the search results.
Recurse to Depth	Select to include subfolders to the depth specified in the box. The default depth is 1, which is one level below the folder displayed in the path box.
Wildcard	Use * to match any number of characters. Use ? to match any single character. The search is not case sensitive.
Invert results set	Select to search for permissions other than those specified. For example, if you are searching for Write (W), the search results return all permissions except Write (W).

Service and task search criteria

The Service Security and Task Management modules have Predefined Searches that you can use to quickly search for services/tasks and permissions. In addition, you can add multiple criteria by clicking **Add Criteria** for each criterion.

NOTE: To search for disabled accounts in the Service Security and Task Management modules, you must select Logon Account as the field to search.

- To delete a criterion, right-click the criterion on the **Search** tab, and choose **Delete Search Item**.
- To delete all criteria but the default, right-click, and choose **Clear**.
- To export the results, click **Export**. See [Using the Browse tab to export security](#).

Group and user search criteria

Applies to Group and User Management Security module only.

Table 6. Group and user search criteria options

Option	Description
Group/User Name Full Name Comment SID	<p>You can search for a group or user name, a full name, text in the comment, or the SID. You can use wildcards to search. Browse for a group or user, or click Advanced Group/User Selection.</p> <p>NOTE: One of the fields returned with the search results is Last Logon. Security Explorer® queries the Primary Domain Controller (PDC). In environments with multiple domain controllers, the PDC may or may not have the latest logon data for the user at the time you submit your search request.</p>
Search for local administrator accounts	Select to return local administrator accounts. This is a convenient method to quickly locate accounts when you need to change passwords. Once the search is finished, right-click on the account, and choose Change Password .

Table 6. Group and user search criteria options

Option	Description
Search for groups	By default, both groups and users are searched. To remove a criterion, clear the check box.
Search for users	
Return only group members	Select to return only members of the specified group. Selecting this option may slow search performance.
Search for disabled accounts	Select to search for disabled accounts. Disabled accounts are indicated with a red X.

Advanced search options

Applies to Group and User Management Security module only.

Table 7. Advanced search options

Option	Description
Include group memberships	By default, group memberships are not included in the search. If you want group memberships included in the search, select this check box.
Return all results	Active only when the include group memberships check box is selected. By default all results are returned.
Return only parent groups which contain the specified group/user account	Active only when the include group memberships check box is selected. Select to return only the parent groups that contain the groups/users being searched for.
Return only groups which DO NOT contain the specified group/user account	Active only when the include group memberships check box is selected. Select to return only groups that do not contain the groups/users being searched for.

Registry key search criteria

Applies to Registry Security module only.

From the list of search results, you can easily manage registry keys. You can add a new registry key, delete an existing registry key, or modify the values of a selected registry key. Right-click a registry key, and choose **New Registry Key**, **Delete Registry Key**, or **Display Registry Values**. See [Managing registry keys](#).

Table 8. Registry key search criteria options

Option	Description
Wildcard	Use * to match any number of characters. Use ? to match any single character. The search is not case sensitive.
Invert results set	Select to search for permissions other than those specified. For example, if you are searching for Write (W), the search results return all permissions except Write (W).

Using the Search tasks

The Search basic task provides a quick way to search for permissions. For more options, click **Switch to Security Explorer Classic (Advanced)**. See [Using the Browse tab to search](#).

You also can use the Find Unknown, Find Disabled, and Find SID History advanced tasks to easily search permissions for those specific situations.

i | NOTE: The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To use the Search tasks

- 1 Open the module for the type of search.
- 2 Open the **Tasks** tab.
- 3 Click **Search, Find Unknown, Find Disabled, or Find SID History**.
- 4 Click **Add** to select paths.
- 5 For Search and Find SID History, click **Add** to select accounts.
- 6 Click **OK**. An information message displays.
- 7 Click **OK**. A new Security Explorer® window opens displaying the search progress on the **Status** tab. When the search is complete, the results display in the right pane. See [Using the Browse tab to search](#).

Replacing permissions

i | NOTE: Replacing Permissions is not available in the SQL Server Security, SharePoint Security, Exchange Security, and Active Directory Security modules.

In the **Search Results** area, you can select one or more permissions, and replace them with the permissions of a selected user or group.

To replace permissions

- 1 Right-click one or more of the permissions displayed in the **Search Results** area, and choose **Replace**.
i | NOTE: Only explicit permissions can be replaced. If any of the selected permissions are inherited, a warning message box displays.
- 2 In the **Select Group or User** area, select a group or user whose permissions will be used as the replacement.
 - You can select from the **Account Selection Chooser** area. The name displays in the **Group or User** box.
 - You can select a domain from the **Domain** list. By default, only the groups display. To include users in the list, click **Show Users**. Select a group or user from the list. The name displays in the **Group or User** box.
 - You can type a group or user name in the **Group or User** box or click **Advanced User Selection** to select a group or user name from a list.
- 3 Click **OK**.


Scheduling a search

If you would prefer to run the search at a set time, schedule it as a Windows® task.

i | NOTE: The Search Scheduler is available only in the NTFS Security, Share Security, Registry Security, Printer Security, Group And User Security, SharePoint Security, SQL Security, Exchange Security, and Active Directory modules.

To schedule a search

- 1 Open the module for the type of search.

- 2 Open the **Browse** tab.
- 3 Select an object in the Navigation or Objects pane, and select **Search | New Search Window (Empty)**.
-OR-
Click , press **Shift + F3**, or right-click an object, and choose **Search in a New Window**.
- 4 If you want to change the search scope, see [Adding a search scope](#).
- 5 Add criteria for the search. See [Setting search criteria](#).
- 6 Click **Schedule**.
- 7 In the **File Name** box, browse to locate the destination for the Security Explorer Report File (.pdf). A search status file (<report file name>_status.txt) will be also saved in the destination along with the report.
- 8 In the **Account** box, browse to locate an account under which to run the export. Make sure the account has access to the resources you export. If you do not enter an account, the export task runs under the local system account.
- 9 To receive an email notification when the search completes, select **Send email when task completes**, and click **Configure Email** to enter the email recipients and subject. The email contains the report as attachment if the size of the report file is not larger than 10 MB. For a report file that is larger than 10 MB, the email provides the report location information in the message body instead of containing the report as attachment.

i **NOTE:** Before you select this option, enable **Email Notification** and configure SMTP settings on **Tools > Options > General**. See [Setting general options](#) for details.

NOTE: The email notification will be sent under the local system account if you do not enter any account in the **Account** box. To make sure the email notification has been enabled for the local system account:

 - 1 Enable **Email Notification** and configure SMTP settings on **Tools > Options > General**. See [Setting general options](#) for details.
 - 2 Copy the file `C:\Users\[user_name]\AppData\Local\Quest\Security Explorer\v9\PersistentData.xml` to
`C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Quest\Security Explorer\v9` (for 32-bit Security Explorer)
 or
`C:\Windows\System32\config\systemprofile\AppData\Local\Quest\Security Explorer\v9` (for 64-bit Security Explorer)
 (If a file named PersistentData.xml already exists in the target folder, replace the file with the one you copied)
- 10 To save the report to a shared folder when the search completes, select **Deliver report to a shared folder**, and click the ellipsis (...) to select the folder.

i **NOTE:** Saving the report to a shared folder will fail if the task runs under the local system account with no access to the shared folder.
- 11 Click **Schedule**. The task is assigned the default run time of Weekly, every Monday at midnight.

i **NOTE:** Errors that occur during the task are captured in the logs located at `C:\ProgramData\Quest\Security Explorer\v9\Logs`. The file names are prefixed by "SXPSEARCH".

Managing search tasks

The Search Scheduler provides a central location for management of search tasks. You can add new search tasks, edit existing search tasks, and delete selected search tasks.

i | **NOTE:** The Search Scheduler is available in the NTFS Security, Share Security, Registry Security, Printer Security, Group And User Security, SharePoint Security, SQL Security, Exchange Security, and Active Directory modules.

To manage search tasks


- 1 Open a module.
- 2 Select **Search | Search Scheduler**.
-OR-
Click  on the Tool bar.
- 3 Use the Tool bar to manage search tasks.

Table 9. Search Scheduler options

Option	Description
Open Task Dialog	Open the task in Task module.
Edit	Edit an existing search task.
Delete	Delete selected search tasks.

Managing security

With Security Explorer®, administrators can back up and restore their NTFS permissions, providing the ability to recover permissions. Additionally, permissions can be exported for reporting and backup.

Topics:

- [Backing up security](#)
- [Scheduling a backup](#)
- [Using the backup scheduler](#)
- [Restoring security](#)
- [Comparing security](#)
- [Purging backup files](#)
- [Scheduling a backup purge](#)
- [Exporting security](#)

Backing up security

Before modifying any security permissions, make a backup in case you need to restore the permissions to their original state. You also can back up permissions on files for which you do not have access. As long as you are an administrator, or have the **Backup files and directories** user right, you can back up and restore permissions on all files, which is helpful when backing up and restoring a user's home directories.

NOTE: The Backup function is available only in the NTFS Security, Share Security, Registry Security, Printer Security, SharePoint Security, SQL Server Security, Exchange Security, and Active Directory Security modules. You can back up only SQL databases in the SQL Server Security module.

Table 1. Backup file types

Module	File Type	File Extension
NTFS Security	Security Explorer NTFS Backup File	*.sec /*.tmp
Registry Security	Security Explorer Registry Backup File	*.ser
Share Security	Security Explorer Share Backup File	*.ses
Printer Security	Security Explorer Printers Backup File	*.sep
SharePoint Security	Security Explorer SharePoint Backup File	*.spb
SQL Server Security	Security Explorer SQL Backup File	*.sqb
Exchange Security	Security Explorer Exchange Backup File	*.exb
Active Directory Security	Security Explorer Active Directory Backup File	*.adb

Topics:

- [Using the Browse tab to back up security](#)
- [Using the Backup task](#)

Using the Browse tab to back up security


To back up security using the Browse tab

- 1 Open the module with the permissions you want to back up.
- 2 Open the **Browse** tab.
- 3 From the Navigation or Object pane, select an object.

Acceptable objects are Enterprise Scopes, volumes, folders, shares, or Active Directory® objects. Files cannot be backed up individually, but can be backed up within the parent folder.

- 4 Select **Security | Backup Security**.

-OR-

Click  on the Tool Bar; or right-click an object, and choose **Backup Security**.

- 5 In the **Backup File Name** box, browse to locate a path and name the backup file.

i | IMPORTANT: *SharePoint Security module only.* It is strongly recommended that root backup objects do not inherit permissions from their parents.

- 6 To add additional paths, click **Add** to browse for a path.

-OR-

Type the full path name in the **New Path** box, and click **Add**. *Available only in the NTFS Security module.*

-OR-

Click **Load** to load a previously saved Security Explorer Backup List (*.bkn) file. *Not available in the Registry Security, SharePoint Security, SQL Server Security, Exchange Security, and Active Directory Security modules.*

- 7 Set options for the backup.

Table 2. Backup options

Option	Description
Recurse all subfolders and files for supplied paths	<i>Available only in NTFS Security module.</i> By default, all subfolders and files in the selected path are backed up. To select the level to which the subfolders and files are backed up, clear the check box, and type a number in the (Depth) box.
Perform a check/repair inheritance operation before executing backup	<i>Available only in NTFS Security module.</i> Select to check and repair inheritance before backing up the selected paths. NOTE: If you select this check box and want to schedule the backup, the task needs to run under an account that has sufficient privileges to make changes to permissions on the target computer.
Include System Access Control List (SACL) in backup	<i>Available only in NTFS Security module.</i> Select to include System Access Control List in the backup.
File Filter Wildcard Node Filter Wildcard	<i>Not available in the Registry Security, SharePoint Security, SQL Server Security, Exchange Security, and Active Directory modules.</i> To back up only specified file types, type a value, such as *.exe, in the Wildcard box.
Backup Scheduler Job Name	<i>Not available in the Registry Security and SharePoint Security modules.</i> To schedule the backup, type a name for the backup job in the Job Name box, and click Schedule . See Scheduling a backup .

- 8 To save the list of paths to a Security Explorer Backup List (*.bkn) file for reuse, click **Save**. *Not available in the Registry Security, SharePoint Security, SQL Server Security, Exchange, and Active Directory Security modules.*
- 9 To schedule the backup, type a name for the job in the **Job Name** box, and click **Schedule**. See [Scheduling a backup](#).
- 10 Click **Backup Security**. See [Completing a process](#).

Using the Backup task

The Backup task provides a quick way to back up selected paths. For more options, click **Switch to Security Explorer Classic (Advanced)**. See [Using the Browse tab to back up security](#).

i | **NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To back up security using the Backup task

- 1 Open the module with the permissions you want to back up.
- 2 Select a folder or object.
- 3 Open the **Tasks** tab.
- 4 Click **Backup**.
- 5 Click **Add** to add additional paths.
- 6 Click **Browse** to locate and name a backup file.
- 7 Click **OK**. See [Completing a process](#).

Scheduling a backup

If you would prefer to run the backup at a set time, schedule it as a Windows® task.

i | **NOTE:** The Backup Scheduler is available only in the NTFS Security, Share Security, Registry Security, SharePoint Security, SQL Security, Exchange Security, and Active Directory modules.

To schedule a backup

- 1 Create the backup job. See [Backing up security](#).
- 2 Type a name for the job in the **Job Name** box, and click **Schedule**.

The **Schedule a Backup** dialog box opens. Depending on if the backup job is local or remote, the appropriate option is selected.

Table 3. Backup options

Option	Description
Local Backups	<p>If the backup paths are local, the Create single scheduled task on local machine check box is selected. The Job Name, Wildcard, and Backup Name carry over from the previous screen.</p> <p>In the Account box, browse to locate an account under which to run the backup. If you do not enter an account, the backup runs under the local system account.</p>
Remote Backups	<p>If the backup paths are on remote computers, select Create separate scheduled task(s) on remote machine(s). The Job Name, Wildcard, and Backup Name carry over from the previous screen.</p> <p>To create a scheduled task on remote computers</p> <ol style="list-style-type: none"> 1 Double-click a job, or select a job, and click Edit. The Edit dialog box opens displaying the Job Name, Wildcard, and Backup Name from the previous screen. 2 Make any needed changes to the backup job. 3 In the Account box, browse to locate an account under which to run the backup. 4 To copy the changes to all remote scheduled jobs, click Copy to All. A warning box appears. 5 Click Yes to continue.

- 3 To set an auto-pause time for the backup task, select the **Auto-Pause Time** check box and set a time. The task will automatically pause at the time you set, and will automatically resume when the task runs again.
- 4 Click **Schedule**. The task is assigned the default run time of Weekly, every Monday at midnight.

- i** **NOTE:** To change the run time, edit the backup using the Backup Scheduler. See [Using the backup scheduler](#).
- NOTE:** Errors that occur during the task are captured in the Windows Event Log.

Using the backup scheduler


The Backup Scheduler provides a convenient place in which to create, edit, and delete backup jobs.

- i** **NOTE:** The Backup Scheduler is available only in the NTFS Security, Share Security, Registry Security, SharePoint Security, SQL Security, Exchange Security, and Active Directory Security modules.
- TIP:** You can use the Scheduled Backups basic task to manage scheduled backups.

To use the Backup Scheduler to schedule a backup

- 1 Select **Security | Backup Scheduler**.

-OR-

Click  on the Tool Bar; or right-click an object, and choose **Backup Scheduler**.

The **Backup Scheduler Task List** box lists the currently defined backup jobs in ascending alphabetical order by computer name.

To sort the columns, click the column heading for ascending order and again for descending order.

- 2 To create a new backup job, click **New**. See [Using the Browse tab to back up security](#).
- 3 Click **Schedule**.
- 4 Click **Close**.

Restoring security

You can restore your permissions from a backup file created by using the Backup function. You can restore some or all of the backup file. You can restore to multiple paths. Prior to initiating the restore process, you can verify the permissions against the current permissions.


i | **NOTE:** The Restore function is available only in the NTFS Security, Share Security, Registry Security, SharePoint Security, SQL Server Security, Exchange Security, and Active Directory Security modules.

TIP: You can use the Restore basic task to select a backup file to restore. After you locate the backup file and click **OK**, the **Restore Security** dialog box opens with the **Backup File** box populated.

To restore a backup file

- 1 Open the module that is associated with the object[s] you want to restore.
- 2 Open the **Browse** tab.
- 3 Select **Security | Restore Security**.

-OR-

Click  on the Tool Bar; or right-click an object, and choose **Restore Security**.

- 4 In the **Backup File** box, type the full path and name for the backup file, or click **Load** to locate a backup file. The contents of the backup file display in the left pane.
- 5 Expand the backup file and examine the contents. You can choose specific objects to restore by selecting the box next to the object. Use **De-select all children** and **Select all children** to help you select objects to restore.

i | **NOTE:** When restoring from the Share Security, Registry Security, SharePoint Security, SQL Server Security, and Active Directory modules, the check boxes and the **Advanced** button are unavailable. The **Restore to different paths** check box is available in the SharePoint Security module. The **Restore permissions** check box is selected by default.

Table 4. Restore options

Option	Description
Show differences (folders and files only)	<i>Applies to NTFS Security module only.</i> Select to show the folders and files that have different permissions than the ones in the backup file. If you select this check box, a message box displays. If you click Yes to proceed, the backup file reloads. If the permissions for a folder or file are different than those in the backup file, the name displays in red in the tree. Any differences between the current permissions and the backed up permissions are highlighted in yellow. NOTE: To compare permissions of two folders, see Comparing security .
Include files when previewing backup	<i>Applies to NTFS Security module only.</i> Select to include files in the display. By default, only folders display. If you select this check box, the backup file reloads to display all the files. NOTE: Only select this check box if you are restoring a small number of individual files. If you are restoring a large number of objects, selecting this check box can slow the loading of the backup file.
Restore owner Restore permissions	<i>Applies to NTFS Security module only.</i> By default, both the owner and permissions are restored. Clear the appropriate check box for the item you do not want to restore.
Restore missing folders	<i>Applies to NTFS Security module only.</i> Select to recreate folders that are present in the backup file, but are no longer present in the destination path.

Table 4. Restore options

Option	Description
Restore SACL	Select to restore System Access Control List (SACL). Available only if SACL was included in the backup. See Backing up security .
Restore to different paths	<p><i>Applies to NTFS Security, SQL Security, and SharePoint Security modules only.</i> Select to restore the permissions to different paths.</p> <p>Browse to locate a path. Repeat to add additional paths if desired. Each path you select appears in the drop-down list.</p> <p>NOTE: If you want to restore to a single path, select the path from the drop-down list.</p> <p>When you click Restore, you can choose to restore to the path displayed in the box, or to all paths listed in the drop-down list.</p> <p>IMPORTANT: <i>Applies to NTFS and SQL Security modules only.</i> The alternate restore location must have the same structure as the backup file.</p> <p>IMPORTANT: <i>Applies to SharePoint Security module only.</i> If the alternate restore location does not have the same structure as the backup file, only the permissions for identical site items are restored. All other permissions are ignored.</p>

- 6 Available only in the NTFS Security module. Click **Advanced** to set more options for the restore process. See [Setting advanced options for the restore process](#).

- 7 Click **Restore**. See [Completing a process](#).

i | **NOTE:** If you selected to restore to a different path, you are asked if you want to restore to the selected path that displays in the box, or to all paths in the drop-down list.

Setting advanced options for the restore process

Available only in the NTFS Security module. On the **Advanced Restore Settings** dialog, you can filter the back up file to help you find permissions to restore. You also can select how the permissions are restored.

To set advanced options for the restore process

- 1 On the **Restore Security** dialog (see [Restoring security](#)), click **Advanced** to set more options for the restore process.
- 2 To help you find and select parts of the backup file to restore, you can filter the path and the accounts.

i | **NOTE:** The Path Filter wildcards are applied to the selection first, and the Permission Accounts wildcard is applied second.

Filtering the path

Filter the path if the backup file is exceptionally large, say over 1,000,000 paths. If you try to load the full tree, the process could be slow, so you might want to load only the portion of the backup file that you plan to restore.

In addition to the default option of filtering all the paths, you can choose to apply the filters to root paths only. This option is useful if you have a large number of root paths in your backup, i.e., a flat list of paths. Alternatively, you can apply the filters to all paths except the root paths. This option is useful if you have a large backup in a more complicated tree-like structure.

You can use multiple wildcards, separated by commas. Use the * wildcard to match any number of characters. Use the ? wildcard to match a single character.

Table 5. Path wildcard examples

Selected Paths	Wildcard = *docs	Wildcard = *test*	Wildcard = *test?
Folder1 = c:\work	skipped	skipped	skipped
Folder2 = c:\work\docs	restored	skipped	skipped
Folder3 = c:\work\test	skipped	restored	skipped
Folder4 = c:\work\test1	skipped	restored	restored
Folder5 = c:\work\test2	skipped	restored	restored

Filtering permission accounts

Filtered out permissions do not display and are not restored. Use the * wildcard to match any number of characters. Use the ? wildcard to match a single character. For example, *smith will skip any group or user that does not include smith in the path. To select a group or user, click **Advanced User Selection**.

- 3 Select the restore mode.

You can overwrite all permissions, restore permissions only for accounts from the backup file, or add permissions from the backup file to the existing permissions. In any case, the restore process skips paths for which no permissions are loaded from the backup, so those permissions remain unchanged.

- 4 Select the scope mode.

You can restore permissions for only the paths and subpaths that are visible and selected in the tree, or for all subpaths of the paths selected in the tree, including those that are filtered out or not selected.

- 5 Click **OK**.


Comparing security

You can compare permissions of two folders (including their sub-folders) in the NTFS Security module.


To compare permissions of two folders

- 1 Open the **NTFS Security** module.
- 2 Open the **Browse** tab.
- 3 Select **Security | Compare Security**.

-OR-

Click  on the Tool Bar; or right-click one or two folders, and choose **Compare Security**.

- 4 Browse and select two folders in the dialog box, and click **Compare**.
- 5 In the **Compare Security** dialog box, navigate one of the trees and select the folder you want to compare in the left pane. The corresponding folder in the other tree is selected automatically. The folder permissions are displayed in the right pane. Any differences between the two folders are highlighted in yellow.

 **NOTE:** To show and compare files in the trees as well, select **Include files**.

The folder and file names in the trees show in different colors depending on the comparison result.


Table 6. Folder and file name colors

Color	Description
Black	Permissions are same with the folder or file in the other tree.
Red	Permissions are different from the folder or file in the other tree, or errors occurred while retrieving permissions.
Highlighted in yellow	The folder or file does not exist in the other tree.

Purging backup files



In the NTFS Security module, you can purge backup files.

To purge backup files

- 1 Select **Security | Purge Backup**.
- 2 Browse to locate the folder that contains the backup files.
 **NOTE:** Only files in the selected folder are deleted; subfolders are not processed.
- 3 Adjust the number of days that determine which files are purged. The default is 30 days.
Backup files older than the specified number of days are purged every day at midnight. If you enter 0 days, all backup files are purged.
- 4 Click **OK** to purge the files.

Scheduling a backup purge

The Purge Backup Scheduler provides a convenient place in which to create, edit, and delete purge backup jobs.

- 
- NOTE:**
- The Purge Backup Scheduler is available only in the NTFS Security module.
-
- 
- NOTE:**
- The option to create tasks remotely is unavailable when purging.

To use the Purge Backup Scheduler to schedule a backup purge

- 1 Select **Security | Purge Backup Scheduler**.
The **Purge Backup Scheduler Task List** box lists the currently defined purge backup jobs in ascending alphabetical order by computer name.
To sort the columns, click the column heading.

- 2 Use the options to manage the list of tasks.

Table 7. Purge Backup Scheduler Task list options

Option	Description
New	<p>Creates a new task.</p> <ol style="list-style-type: none">1 Select the Create single scheduled task on local machine check box.2 Browse for the target folder where the backup files are located. NOTE: Only files in the selected folder are deleted; subfolders are not processed.3 To back up only specified file types, type a value, such as *.exe, in the Wildcard box.4 In the Account box, browse to locate an account under which to run the backup. If you do not enter an account, the backup runs under the local system account.5 Click Schedule.
Edit	Edits the selected task.
Delete	Deletes the selected tasks.

- 3 Click **Close**.

Exporting security

By default, permissions are exported to a report, which you can save, print, or export. You can export permissions on a folder to a Microsoft® Access® 2000 database (.mdb file), a SQLite database, or a delimited file for use with Microsoft Excel®. You also can export a list of tasks, groups, and users. The list of groups or users includes the account name, type of group or user, account SID, account description, when the account last logged on, number of times the account has logged on, and whether the account is disabled, locked, or expired.

The Export Scheduler displays all the current export tasks. You can add, edit, and delete export tasks.

- i** **NOTE:** Exporting is not available in the Registry Security and Printer Security modules. The Export Scheduler is available in the NTFS Security, Share Security, Task Management, Service Security, Group and User Management, SQL Server Security, Exchange Security, SharePoint Security, and Active Directory Security modules only.
- NOTE:** For exporting Active Directory permissions, see [Exporting Active Directory permissions](#).

Topics:

- [Using the Browse tab to export security](#)
- [Using the Export task](#)
- [Scheduling an export](#)
- [Managing export tasks](#)

Using the Browse tab to export security

To export permissions using the Browse tab

- 1 Open the module that is associated with the permissions you want to export.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select a folder or type a path in the **Path** box.

4 Select **Security | Export**.

 **TIP:** You also have the option **Export NTFS Permissions** in the Share Security module.

-OR-

Click  on the Tool Bar; or right-click a folder, and choose **Export**.

5 *Available in NTFS Security module only.* Set folder and file options for the export.


 **NOTE:** If you selected specific files to export, the **Folder and File Options** area is unavailable as only the file permissions are exported.

Table 8. Export folder and file options

Option	Description
Export folder permissions	Select to export the folder permissions (default).
Export file permissions	Select to export the permissions of the files (default).
Recurse subfolders	Select to retrieve the subfolders and sub files of the parent directory (default).
Recurse all subfolders	<i>Available in NTFS Security module only.</i> Select to retrieve all of the subfolders and sub files of the parent directory (default).
Recurse to depth	<i>Available in NTFS Security module only.</i> Select to choose how many directory levels to export. For example, if you are only concerned with the subfolders, and not the sub-sub-folders, then choose to recurse to a depth of 1.
File wildcard	<i>Available in NTFS Security module only.</i> If you want to export only files with a certain extension, type the extension in the File Wildcard box. For example, if you are only concerned with exporting the permissions of all executable files, type *.exe in the File wildcard box.

6 *Available in NTFS Security module only.* Browse to select files and folders to exclude from the export.

7 *Available in the Service Security module only.* Select to include the permissions on the selected service[s].

8 *Available in NTFS Security and Active Directory Security modules only.* Set group membership options. *Available only if **Generate Report** or **Save to Microsoft Excel Spreadsheet** is selected.*

Table 9. Group membership options

Option	Description
Show group members	Select include the members of groups.
Include nested groups	Select to include members of nested groups.
Include "Domain Users" group members	Select to include members of the Domain Users group.

9 Set output options.

Table 10. Output options

Option	Description
Generate report	By default, permissions are exported to a report, which you can save, print, or export. NOTE: When exporting to a report, use the Advanced button to choose what columns of data to include in the output file.

Table 10. Output options

Option	Description
Save to Microsoft Excel spreadsheet	Select to save to a delimited file for use with Microsoft® Excel®. Select either Comma-delimited file (.CSV) or Tab-delimited file (.TXT) . Browse to locate a destination for the file. NOTE: When exporting to an Excel spreadsheet, use the Advanced button to choose what columns of data to include in the output file.
Save to database	<i>Not available in the Service Security, Task Management, Group and User Management and Active Directory Security modules.</i> Select to save to a Microsoft Access® .mdb database or a SQLite database. Browse to locate a destination for the file. IMPORTANT: Do not overwrite the Security Explorer system file, SXP.mdb, which is located in the Security Explorer install folder.
Summary mode: export only when permissions differ from parent	<i>Not available in the Service Security, Task Management, Group and User Management, Access Explorer, and Active Directory modules.</i> Select to export only permissions that differ from the parent.

- 10 To schedule the export task, select **Create a schedule export task**, type a name in the **Job Name** box, and click **Schedule**.
 - a Browse to locate the destination for the Security Explorer Report File (.pdf).
 - b In the **Account** box, browse to locate an account under which to run the export. If you do not enter an account, the export task runs under the local system account.
 - c Click **Schedule**. The task is assigned the default run time of Weekly, every Monday at midnight.
- 11 Click **OK**.

i | **NOTE:** To edit or delete an export task, see [Managing export tasks](#).

Using the Export task

The Export task provides a quick way to export permissions to a report that you can save, print, or export. For more options, click **Switch to Security Explorer Classic (Advanced)**. See [Using the Browse tab to export security](#).

i | **NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To export permissions using the Export task

- 1 Open the module associated with the permissions you want to export.
- 2 Open the **Tasks** tab.
- 3 Select a folder, and click **Export**.
- 4 Click **Add** to add additional paths.
- 5 Click **OK**.

Scheduling an export


If you would prefer to run the export at a set time, schedule it as a Windows® task.

To schedule an export

- 1 Open a module.

- 2 Select **Security | Export Scheduler**.

-OR-

Click  on the Tool bar.

- 3 Browse to set the scope for the export.
- 4 Set the export job options. See [Using the Browse tab to export security](#) for details on the **Export Permissions** dialog.
- 5 Type a name for the export job, and click **Schedule**.
- 6 In the **File Name** box, browse to locate the destination for the Security Explorer Report File (.pdf).
- 7 In the **Account** box, browse to locate an account under which to run the export. Make sure the account has access to the resources you export. If you do not enter an account, the export task runs under the local system account.
- 8 To receive an email notification when the export completes, select **Send email when task completes**, and click **Configure Email** to enter the email recipients and subject. The email contains the report as attachment if the size of the report file is not larger than 10 MB. For a report file that is larger than 10 MB, the email provides the report location information in the message body instead of containing the report as attachment.

i **NOTE:** Before you select this option, enable **Email Notification** and configure SMTP settings on **Tools > Options > General**. See [Setting general options](#) for details.

NOTE: The email notification will be sent under the local system account if you do not enter any account in the **Account** box. To make sure the email notification has been enabled for the local system account:

- 1 Enable **Email Notification** and configure SMTP settings on **Tools > Options > General**. See [Setting general options](#) for details.
- 2 Copy the file `C:\Users\[user_name]\AppData\Local\Quest\Security Explorer\v9\PersistentData.xml` to
to
`C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Quest\Security Explorer\v9` (for 32-bit Security Explorer)
or
`C:\Windows\System32\config\systemprofile\AppData\Local\Quest\Security Explorer\v9` (for 64-bit Security Explorer)
(If a file named PersistentData.xml already exists in the target folder, replace the file with the one you copied)

- 9 To save the report to a shared folder when the export completes, select **Deliver report to a shared folder**, and click the ellipsis (...) to select the folder.

i **NOTE:** Saving the report to a shared folder will fail if the task runs under the local system account with no access to the shared folder.

- 10 Click **Schedule**. The task is assigned the default run time of Weekly, every Monday at midnight.

i **NOTE:** Errors that occur during the task are captured in the logs located at `C:\ProgramData\Quest\Security Explorer\v9\Logs`. The file names are prefixed by "SXPEExport".

Managing export tasks

The Export Scheduler provides a central location for management of export tasks. You can add new export tasks, edit existing export tasks, and delete selected export tasks.

To manage export tasks


- 1 Open a module.
- 2 Select **Security | Export Scheduler**.
-OR-
Click  on the Tool bar.
- 3 Use the Tool bar to manage export tasks.

Table 11. Export Scheduler options

Option	Description
New	Create a new export task. See Scheduling an export .
Edit	Edit an existing export task.
Delete	Delete selected export tasks.

Managing objects

In addition to managing permissions and security, Security Explorer provides features to manage objects so you don't need to leave the application.

Topics:

- [Managing folders and files](#)
- [Managing shares](#)
- [Managing registry keys](#)
- [Managing services](#)
- [Managing tasks](#)
- [Managing groups and users](#)
- [Managing Favorites](#)
- [Managing Enterprise Scopes](#)
- [Updating licenses](#)
- [Managing network drives](#)

Managing folders and files

You can create and delete folders. You can delete, edit, and open files. Finally, before you perform certain tasks, you can show which files are open in a given location.

Topics:

- [Creating a new folder](#)
- [Deleting a folder or file](#)
- [Viewing folder and file properties](#)
- [Showing open files](#)
- [Opening files](#)
- [Editing files](#)
- [Opening a folder in Windows Explorer](#)

Creating a new folder

To create a new folder

- 1 Open the **NTFS Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select the container under which to create the new folder.

- 4 Select **Tools | New Folder**.
- OR–
- Right-click the container, and choose **New Folder**.
- 5 Type a name for the new folder, and click **OK**.

Deleting a folder or file

To delete a folder or file


- 1 Open the **NTFS Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select the folder or file.
- 4 Select **Tools | Delete Folder or File**.
- OR–
- Right-click the folder or file, and choose **Delete Folder or File**.
- 5 To delete the folder or file, click **Yes**.

i **NOTE:** If the folder is also shared, you are asked if the share should be deleted as well. To delete the share, click **Yes**.

NOTE: If the selected folder is included in an Enterprise Scope, the folder is not removed from the Enterprise Scope. You also must remove the folder by editing the Enterprise Scope. See [Editing an Enterprise Scope](#).

Viewing folder and file properties

To view folder and file properties

- 1 Open the **NTFS Security** module,
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select the folder or file
- 4 Select **Tools | Properties**.
- OR–
- Click  on the Tool Bar; or right-click the folder or file, and choose **Properties**.

Showing open files

To show open files

- 1 Open the **NTFS Security** module.
- 2 Open the **Browse** tab.
- 3 Select **Tools | Show Open Files**.
- 4 Select options.

Table 1. Open file options

Option	Description
View all open resources on Server	Select to view all open resources on a selected server. Type the server name in the box, or click Choose Server/Base Path to choose a server.
View only resources within Base Path	Select to view all open resources on a within a base path. Type a base path in the box, or click Choose Server /Base Path to choose a base path.
Auto refresh interval	Select to refresh the display at a specified interval. By default, the list refreshes every 30 seconds. To change the interval, use the up or down arrows to increase or decrease the value. To manually refresh the list, choose Refresh from the shortcut menu.

- 5 To close selected resources, right-click in the list, and choose **Close Selected Resources**.
To close all listed resources, right-click in the list, and choose **Close All Resources**.

Opening files

You can open a file in its associated application. For example, a Word file opens in Microsoft® Word, while a batch file executes. If you need to edit a file, see [Editing files](#).

To open a file

- 1 Open the **NTFS Security** module.
- 2 Open the **Browse** tab.
- 3 Select a file, and select **Tools | Open File** or press **Ctrl + O**.
-OR-
Right-click a file, and choose **Open File**.

Editing files

You can open a file in its associated application for editing.

To edit a file

- 1 Open the **NTFS Security** module.
- 2 Open the **Browse** tab.
- 3 Select a file, and select **Tools | Edit File** or press **Ctrl + E**.
-OR-
Right-click a file, and choose **Edit File**.

Opening a folder in Windows Explorer

You can select a folder in Security Explorer® and open Windows® Explorer to the same location.

To open a folder in Windows Explorer

- 1 Open the **NTFS Security** or **Share Security** module.
- 2 Open the **Browse** tab.
- 3 In the Objects pane, select a folder, and select **Tools | Open with Windows Explorer**.

-OR-

Click  on the Tool Bar; or right-click an object, and choose **Open with Windows Explorer**.

Managing shares

You can create or remove a share and locate its path.

Topics:

- [Creating a new share](#)
- [Removing a share](#)
- [Finding a share path](#)

Creating a new share

i | **NOTE:** The recommended approach when adding a new share is to browse to the source folder using the NTFS Security module.


To create a new share

- 1 Open the **NTFS Security** or **Share Security** module.
- 2 Open the **Browse** tab.
- 3 In the Objects pane, select the object in which to create the share.

i | **NOTE:** In the Share Security module, you must select an existing share in the Objects pane so that the new share has the same path as the selected existing share.

- 4 Select **Tools | Create Share**.

-OR-

Click  on the Tool Bar; or right-click the object, and choose **Create Share**.

- 5 Type a name for the share.
- 6 Type an optional free-form comment about the share.
- 7 Click **OK**.


Removing a share

To remove a share

- 1 Open the **NTFS Security** or **Share Security** module.
- 2 Open the **Browse** tab.
- 3 In the Objects pane, select the share.

- 4 Select **Tools | Remove Share**.

-OR-

Click  on the Tool Bar; or right-click the share, and choose **Remove Share**.

- 5 To remove the share, click **Yes**.

Finding a share path

You can locate the folder for a selected share.

To locate the share path

- 1 Open the **Share Security** or **All Management Targets** module.
- 2 Open the **Browse** tab.
- 3 In the Objects pane, select the share.
- 4 Select **Tools | Find Share Path**.

-OR-

Right-click the share, and choose **Find Share Path**.

Managing registry keys

Topics:

- [Creating a new registry key](#)
- [Deleting a registry key](#)
- [Modifying registry values](#)

Creating a new registry key

To create a new registry key

- 1 Open the **Registry Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select the object in which to create the key.
- 4 Select **Tools | New Registry Key**.

-OR-

Right-click the object, and choose **New Registry Key**.

- 5 Type the name of the Registry key.
- 6 Click **OK**.

Deleting a registry key

NOTE: If the selected Registry key is included in an Enterprise Scope, the Registry key is not removed from the Enterprise Scope. You also must remove the Registry key from the Enterprise Scope. See [Editing an Enterprise Scope](#).

TIP: To quickly find a registry key, use the Search module. See [Registry key search criteria](#). From the results list, right-click a registry key, and choose **Delete Registry Key**.

To delete a registry key

- 1 Open the **Registry Security** module.
 - 2 Open the **Browse** tab.
 - 3 In the Navigation or Objects pane, select the registry key.
 - 4 Select **Tools | Delete Registry Key**.
- OR–
- Right-click the Registry key, and choose **Delete Registry Key**.

Modifying registry values

You can add new values, modify values, or remove values from a selected registry key. You also can save the list of values to a .TXT file.

TIP: To quickly find a registry key, use the Search module. See [Registry key search criteria](#). From the results list, right-click a registry key, and choose **Display Registry Values**.

To display registry values

- 1 Open the **Registry Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select the registry key.
- 4 Select **Tools | Display Registry Values**.
- 5 Use the buttons to modify the values in the registry key.

Table 2. Modify registry values

Button	Description
Add	Click Add , and select a value from the drop-down list. Define the value, and click OK .
Modify	Select a value, and click Modify . Modify the value, and click OK .
Remove	Select a value, click Remove , and click OK .
Refresh	Refresh the list to display the latest values.
Save	Save the list as a .TXT file.

- 6 Click **Close**.

Managing services

Topics:

- [Starting, stopping, pausing, or restarting a service](#)

- [Setting logon accounts](#)
- [Changing the password for a logon account](#)
- [Scheduling logon account password changes](#)
- [Removing a service](#)
- [Modifying service properties](#)

Starting, stopping, pausing, or restarting a service





To start, stop, pause, or restart a service

- 1 Open the **Service Security** module.
- 2 Open the **Browse** tab.
- 3 Select one or more services in the Objects pane.
- 4 Click the icon in the Tool Bar.

-OR-

Choose the action from the **Tools** menu; or right-click a service, and choose the action.

Table 3. Managing services icons


Tool Bar	Description
	Start the selected service(s).
	Stop the selected service(s).
	Pause the selected service(s).
	Restart the selected service(s)

Setting logon accounts

For services that require a logon using a domain or local account, you can set or change the logon password. You also can change, in one step, the logon password for all the services assigned to an account.

NOTE: You can also search services by account to change the password. See [Changing the password for a logon account](#).

To set the logon account for a service

- 1 Open the **Service Security** module.
 - 2 Select a computer in the Navigation pane.
 - 3 Select **Security | Logon Accounts**.
- OR-
- Click  on the Tool Bar.
- 4 Select an account, and click **Set Password**.
 - 5 Type the password.

–OR–

Click **Generate** to generate a random password.

- 6 To change the password on the account and on all services that use that account, select **Also change all related service logon account passwords**, and click **Yes**.
- 7 To copy the password to the clipboard, click **Copy**. You can then paste the password into a document for safe keeping or into an email to notify users.
- 8 Click **OK**.
- 9 Click **Close**.

Changing the password for a logon account

You can search Windows® services by their log on account and change the password.

i | **NOTE:** You can schedule the task of changing bulk passwords. See [Scheduling logon account password changes](#). To change an individual user account password, see [Changing user passwords](#).

To change the password for a logon account

- 1 Open the **Service Security** module.
- 2 Open the **Tasks** tab.
- 3 Click **Bulk Change Password**.
- 4 Add paths to search. You can search for computers and domains.
- 5 Type an account or browse for an account.
- 6 By default, a preview report is generated. Clear the check box if you do not want to see the preview.
- 7 Select **Restart service(s) after making changes** if you want to restart services automatically after passwords are changed.
- 8 Click **OK**.
- 9 When the search is complete, you can:
 - Click **Save Log** to save the log to a .txt file.
 - Click **More info** to view a list of the services for the account.
- 10 To change the password for the account, click **Apply**.
- 11 Type the password.

–OR–

Click **Generate** to generate a random password. Select the check box to generate a different random password for all the accounts.

- 12 To copy the password to the clipboard, click **Copy**. You can then paste the password into a document for safe keeping or an email to notify users.
- 13 Click **OK**.

Scheduling logon account password changes

You can schedule the task of changing logon passwords to services

To schedule password changes for service logon accounts

- 1 Open the **Service Security** module.

- 2 Open the **Tasks** tab.
- 3 Click **Scheduled Tasks**.
- 4 Click **New**.
- 5 Add a path.
- 6 Browse to locate an account.
- 7 Set the length of the random password.
- 8 Type a job name.
- 9 Browse to locate an account with permission to run the task. If you do not specify an account, the task runs under the local system account.
- 10 Type a path to the log file, or browse to locate the log file.
- 11 Select **Restart service(s) after making changes** if you want to restart services automatically after passwords are changed.
- 12 Click **Schedule**.

A message displays stating the task will weekly every Monday at midnight by default.
- 13 Click **OK**.
- 14 To change the schedule, select the task, and click **Edit**.
- 15 Open the **Triggers** tab, and change the schedule.
- 16 Make any other changes to the task to suit your needs.
- 17 Click **OK**.

i | **NOTE:** You also can use the Task Management module to manage the task. See [Managing tasks](#).

Removing a service

To remove a service

- 1 Open the **Service Security** module.
- 2 In the Objects pane, select one or more services.
- 3 Select **Tools | Remove**.

–OR–

Right-click selected services, and choose **Remove**.
- 4 Click **Yes**.

Modifying service properties


You can select one or more services to manage properties.

i | **IMPORTANT:** If you select more than one service, the choices you make apply to all the selected services. The title bar of the **Properties** box displays the number of selected services. You can open the drop-down list to see the selected services against which all changes will apply.

NOTE: You can edit the **Description** box only if you selected a single service. If changing the properties results in an error, a temporary red X displays next to the service. The red X does not persist if you browse away from the current location or reload the current path.


Using the Browse tab to modify service properties

To modify properties using the Browse tab

- 1 Open the **Service Security** module.
 - 2 Open the **Browse** tab.
 - 3 In the Objects pane, select the services(s).
 - 4 Select **Tools | Properties**.
- OR-
- Click  on the Tool Bar; or right-click the selected services(s), and choose **Properties**.
- 5 Modify the properties.
 - 6 Click **OK**.

Using the Properties task

The Properties advanced task provides a quick way to select services to modify.

 | **NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To modify service properties using the Properties task

- 1 Open the **Service Security** module.
- 2 Open the **Tasks** tab, and click **Properties**.
- 3 Click **Add** to select paths.
- 4 Click **OK**.
- 5 Modify the properties.
- 6 Click **OK**.

Managing tasks

Use the **Tasks** tab to easily export, search for, and report on tasks.

Table 4. Task Management Tasks tab

Task	Description
Manage Computers	Manage the list of computer Favorites. See Managing Favorites .
Export	Export tasks. See Using the Export task .
Search	Search for tasks. See Using the Search tasks .
Find Disabled	Find tasks running under disabled accounts. See Using the Search tasks .
Task Report	Prepare a task information report.

You also can use the **Browse** tab, **Tools** menu, and shortcut menu to manage tasks.


Topics:

- [Running a task](#)
- [Setting account information](#)
- [Creating a new task](#)

- [Copying a task](#)
- [Exporting a task](#)
- [Removing a task](#)
- [Modifying task properties](#)

Running a task

To run a task

- 1 Open the **Task Management** module.
 - 2 Open the **Browse** tab.
 - 3 Select a computer in the Navigation pane.
 - 4 Select a task in the Objects pane.
 - 5 Select **Tools | Run**.
- OR-
- Click  on the Tool Bar; or right-click a task, and choose **Run**.
- 6 If the task does not have an assigned Logon Account displayed in the Logon Account Name column, you are prompted to enter an account and password.

Setting account information

Tasks must run under a user account with the rights to run the task. The currently assigned logon account displays in the **Logon Account Name** column in the Objects pane.

To set account information for a task

- 1 Open the **Task Management** module.
 - 2 Open the **Browse** tab.
 - 3 Select a computer in the Navigation pane.
 - 4 Select a task in the Objects pane, and select **Tools | Set Account Information**.
- OR-
- Right-click a task, and choose **Set Account Information**.
- 5 Type the account name, or browse to locate an account name.
 - 6 Type the password for the account.
 - 7 Click **OK**.

Creating a new task

To create a new task

- 1 Open the **Task Management** module.
- 2 Open the **Browse** tab.
- 3 Select a computer in the Navigation pane, and select **Tools | New Task**.

-OR-

Right-click a computer, and choose **New Task**.

- 4 Type a name for the task, and click **OK**.
- 5 Configure the task.
- 6 Click **OK**.

Copying a task

To copy a task from one computer to another

- 1 Open the **Task Management** module.
- 2 Open the **Browse** tab.
- 3 Select a task in the Object pane, and select **Tools | Copy Task**.

-OR-

Right-click a task, and choose **Copy Task**.

- 4 Select the computer(s) to which to copy the task, and click **OK**.
- 5 Type the account name, or browse to locate an account name.
- 6 Type the password for the account.
- 7 Click **OK**.

Exporting a task

To export a task

- 1 Open the **Task Management** module.
- 2 Open the **Browse** tab.
- 3 Select a computer to export all tasks associated with that computer.

-OR-

Select a computer, and select one or more tasks.

- 4 Select **Tools | Export Task**.

-OR-

Right-click the computer or selected tasks, and choose **Export**.

- 5 Set output options.

Table 5. Output options

Option	Description
Generate Report	By default, task properties are exported to a report, which you can save, print, or export.
Save to Microsoft Excel® Spreadsheet	Select to save to a delimited file for use with Microsoft® Excel®. Select either Comma-delimited file (.CSV) or Tab-delimited file (.TXT) . Browse to locate a destination for the file. NOTE: When exporting to an Excel spreadsheet, use the Advanced button to choose what columns of data to include in the output file.

- 6 Click **OK**.


Removing a task

To remove a task

- 1 Open the **Task Management** module.
- 2 Open the **Browse** tab.
- 3 Select a computer in the Navigation pane.
- 4 Select a task in the Objects pane, and select **Tools | Remove**.
-OR-
Right-click a task in the Objects pane, and choose **Remove**.
- 5 Click **Yes**.

Modifying task properties

To modify task properties

- 1 Open the **Task Management** module.
- 2 Open the **Browse** tab.
- 3 Select a computer in the Navigation pane.
- 4 Select a task in the Objects pane.
- 5 Select **Tools | Properties**.
-OR-
Click  on the Tool Bar; or right-click the task, and choose **Properties**.
- 6 Modify the task.

Managing groups and users

Use the Tasks tab to easily export, search for, and report on groups and users.

Table 6. Group and User Management Tasks

Task	Description
Manage Computers	Manage the list of computer Favorites. See Managing Favorites .
Search	Search for groups and users. See Using the Search tasks .
Create User/Group	Create a new group, user account, or Managed Service Account. See Creating a new group , Creating a new user , or Creating a new Managed Service Account .
Delete User/Group	Delete one or more groups or users. See Deleting groups and users or Deleting Managed Service Account .
User/Group Properties	Modify the properties of a group or user. See Modifying group and user properties or Modifying Managed Service Account properties .

Table 6. Group and User Management Tasks

Task	Description
AD Properties	Modify Active Directory® properties of a group or user. See Modifying group or user Active Directory properties or Modifying Managed Service Account Active Directory properties .
Users Properties	Modify the properties of multiple users. See Modify memberships of multiple local groups .
Groups Contents	Add or remove a user from multiple groups. See Modifying group memberships .
User/Group Membership	View groups of which a group or user is a member. See Viewing group and user memberships or Viewing Managed Service Account memberships .
Change Password	Change the passwords of one or more users. See Changing user passwords .
Bulk Change Members	Add members to or remove members from multiple local groups. See Modify memberships of multiple local groups .
Clear Local Admins	Remove all domain users from local Administrator group across multiple computers. See Clearing the local administrator group .
Local User Report	Generate a report of local users by searching. See Running a report using the Reports or Tasks tab .
Local Group Report	Generate a report of local groups by searching. See Running a report using the Reports or Tasks tab .
Local Group Members	Generate a report of group contents for multiple local groups across multiple computers. See Running a report using the Reports or Tasks tab .

Use the **Browse** tab and the Tool Bar, **Tools** menu, and shortcut menu to manage accounts.

By adjusting the columns, you easily can see how many times a user has logged on, which users are disabled or locked, and who has an expired password.

Viewing accounts

To view accounts

- 1 Open the **Group and User Management** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation pane, select a type of group or user. The groups or users display in the Objects pane.
You can size the columns to view more or less of the information, or double-click a group or user to view the properties. See [Modifying group and user properties](#).

Creating a new group


To create a new group

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Create User/Group**, and select **Group**.
- 4 Type the name of a domain (domain group) or computer (local group), or click **Select scope** to select a domain or computer.

- 5 (Optional) To create the group for multiple domains or computers, repeat step 4 to select more domains or computers.
- 6 Click **OK**. The **New Group** box displays the current selection.

i | **NOTE:** To open the New Group box on the Browse tab, select **Domain Groups** or **Local Groups** in the Navigation pane, and select **Tools | New**.

-OR-

Click  on the Tool Bar; or right-click **Domain Groups** or **Local Groups**, and choose **New**.
- 7 Create the group.

i | **NOTE:** The **SID** box is available when modifying a group.
- 8 Click **Create**.

Creating a new user

To create a new user

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Create User/Group**, and select **User**.
- 4 Type the name of a domain (domain user) or computer (local user), or click **Select scope** to select a domain or computer.
- 5 (Optional) To create the user for multiple domains or computers, repeat step 4 to select more domains or computers.
- 6 Click **OK**. The **New User** box displays the current selection.

i | **NOTE:** To open the **New User** box on the **Browse** tab, select **Domain Users** or **Local Users** in the Navigation pane, and select **Tools | New**.

-OR-


Click  on the Tool Bar; or right-click **Domain Users** or **Local Users**, and choose **New**.
- 7 Create the user and password.
- 8 Type the name with which the user logs in.
- 9 Type the full name of the user.
- 10 Type the password of the user.
- 11 Choose how to apply the password.

Table 7. Password options

Option	Description
User must change password at next logon	By default, the user is prompted to change the password when they log on for the first time.
User cannot change password	Available only when the User must change password at next logon check box is cleared.
Password never expires	Available only when the User must change password at next logon check box is cleared.

Table 7. Password options

Option	Description
Account is disabled	Select to disable the account.
Account is locked out	The Account is locked out check box is not available when creating a user.

12 Type a description of the user.

13 Select options.

Table 8. Dialog box options

Option	Description
Keep this dialog open after creating new user	By default, the New User box closes when you click Create . If you are creating multiple users, select this check box to keep the New User box open.
Refresh parent user list on completion	By default, the parent list refreshes when you click Create . If you are creating multiple users, clear this check box so you don't have to wait for the list to refresh. TIP: If you are creating more than one user, select the Keep this dialog open after creating new user check box and clear the Refresh parent user list on completion check box.

14 Click **Create**.

Modifying group and user properties

To modify group and user properties

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **User/Group Properties**.
- 4 Type a group or user account name, or click **Advanced selection**, and select a group or user.
- 5 Click **View**. The Properties for the selected group or user account displays.

i **NOTE:** To open Properties from the **Browse** tab, select a type of group or user in the Navigation pane, select a group or user in the Objects pane, and select **Tools | Properties**.
-OR-

Click **i**; double-click a group or user in the Objects pane; or right-click a group or user, and choose **Properties**.

Modifying group or user Active Directory properties

i **NOTE:** Active Directory® properties may not always be available and are never available for local groups or users. To display Active Directory properties, Administration Tools Pack (adminpak) must be installed on the client computer.

To modify group or user Active Directory properties

- 1 Open the **Group and User Management** module.

- 2 Open the **Tasks** tab.
- 3 Click **AD Properties**.
- 4 Type an account name, or click **Advanced selection**, and select a group or user.
- 5 Click **View**. The Properties for the selected group or user appears.

i **NOTE:** To open Properties from the **Browse** tab, select a type of group or user in the Navigation pane, select a group or user in the Objects pane, and select **Tools | Active Directory Properties**.
 –OR–
 Right-click a group or user in the Objects pane, and choose **Active Directory Properties**.

Modifying properties of multiple users

Use the Users Properties advanced task to modify the properties of multiple local users.

To modify properties of multiple users

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Users Properties**.
- 4 Click **Add**, and select the users to modify.
- 5 Click **View**. The Properties window displays the shared properties.

i **NOTE:** To open Properties from the **Browse** tab, select **Domain Users** in the Navigation pane, select one or more users in the Objects pane, and select **Tools | Properties**.
 –OR–
 Click **i** on the Tool Bar; or right-click a selection of one or more users in the Objects pane, and choose **Properties**.

- 6 Make the desired changes. See [Creating a new user](#).

Modifying group memberships

If you select two or more groups, you can add or remove a user from multiple groups at one time.

To modify group memberships

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Groups Content**.
- 4 Click **Add**, and select one or more groups.
- 5 Click **View**. The **Group Contents** window opens.

i **NOTE:** To open the **Group Contents** window from the **Browse** tab, select a type of group in the Navigation pane, select one or more groups in the Objects pane, and select **Tools | Display Group Contents**.

-OR-

Right-click a single group or a selection of groups in the Objects pane, and choose **Display Group Contents**.

You also can access Group Contents by clicking **Contents** on the Control Button Bar in the NTFS Security, Share Security, Registry Security, Printer Security, and Service Security modules. See [Managing group memberships](#).

To access Group Contents from Properties, click **Contents** on the Property window. See [Modifying group and user properties](#).

- 6 Use the buttons to modify the group memberships.

Table 9. Modify group membership options

Button	Description
Add	Add members to the selected group.
Remove	Remove selected members from the selected group.
Refresh	Refresh the list after adding or removing a member.
Print	Print the list.
Save	Save the list as a .txt file.
Show Group Contents	View the members of a selected group.
Show Memberships	Show the groups of which the selected group or user is a member.
Close	Close the Group contents box.

Viewing group and user memberships

Use the User/Group Membership advanced task to view the groups of which a selected group or user is a member. You can print or save the list of groups.

To view group and user memberships

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **User/Group Membership**.
- 4 Type an account name, or click **Advanced selection**, and select an account.
- 5 Click **View**. The **Group Memberships** window displays the groups to which the selected account belongs. You can print the list or save it as a .txt file.

i **NOTE:** To access the **Group Memberships** window from the **Browse** tab, select a type of group or user in the Navigation pane, select a group or user in the Objects pane, and select **Tools | Display Memberships**.

-OR-

Right-click a group or user in the Objects pane, and choose **Display Memberships**.

Changing user passwords

i **IMPORTANT:** Resetting a password could cause irreversible loss of information for the account the next time the user logs off. Use this feature only if the user has forgotten his or her password or does not have a password reset disk.

NOTE: You also can search for services by account and change the logon password for the account. See [Changing the password for a logon account](#).

TIP: To help you easily change the passwords of local administrator accounts, use the Search module. On the **Group/User Search Criteria** tab, select **Search for local administrator accounts**, and run the search. Right-click the results and choose **Change Passwords**. See [Group and user search criteria](#).

To change user passwords

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Change Password**.
- 4 Click **Add**, and select one or more users.
- 5 Click **OK**. The **Set Password box** displays.

i **NOTE:** To access the **Set Password** box from the **Browse** tab, right-click one or more user accounts in the Objects pane, and choose **Change Password**.

-OR-

Click **Change Password** from the **Properties** box of a user. See [Modifying group and user properties](#).

- 6 Type a new password, or click **Generate** to generate a random password.

i **NOTE:** If you selected multiple users, the password applies to all users in the selection.

To copy the password to the clipboard, click **Copy**. You can then paste the password into a document for safe keeping or an email to notify users.

-OR-

Select **Generate a different random password** to generate random passwords for multiple users. The passwords and account names are saved to **ChangedPasswords.log**, which you can find in the Security Explorer® installation folder. Be aware that this file is overwritten each time you generate new random passwords.

- 7 To create a log file listing each account with its new password, select **Log the change password result**. The account names and passwords are saved to **ChangedPasswordsResults.log**, which you can find in the Security Explorer installation folder. Be aware that this file is overwritten each time you change passwords.
- 8 Click **OK**.
- 9 Click **Yes**.

i **TIP:** To help you see which passwords were not reset, check the **Password last change date** column in the Object and Search Results panes.

TIP: To quickly repeat the operation on failures, save failed targets to a new scope by clicking **Save Failed Computers To Scope** on the **Search** tab. See [Adding a search scope](#) and [Group and user search criteria](#).

Modify memberships of multiple local groups

Use the Bulk Change Members advanced task to add members into multiple local groups on different computers or to remove members from these local groups.

To modify memberships of multiple local groups

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Bulk Change Members**.
 - i** **NOTE:** From the **Browse** tab, select **Tools | Bulk Change Group Contents**, or right-click in the Navigation or Objects pane, and choose **Bulk Change Group Contents**.
- 4 Click **Add** to select computers.
- 5 Select the local groups whose members you want to modify.
- 6 Click **Add** to select the members to add or remove.
 - To add the selected members to the selected groups, click **Add Members**.
 - To remove the selected members from the selected groups, click **Remove Members**.

Clearing the local administrator group

To clear the local administrator group

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Clear Local Admin**.
 - i** **NOTE:** From the **Browse** tab, select **Tools | Bulk Remove from Local Administrators**.
–OR–
Right-click in the Navigation or Objects pane, and choose **Bulk Remove from Local Administrators**.
- 4 Click **Add** to add computers one at a time or click **Add all computers from domain**.
- 5 Select options.

Table 10. Report options

Option	Description
Produce report	Select to produce a report of the domain users that were removed in the process. In the Report file path box, type a path to where you want to place the report file, or click Select file path to choose the path.
Produce report only	Select to just produce a report without actually removing the domain users. You can examine the report prior to completing the process. In the Report file path box, type a path to where you want to place the report file, or click Select file path to choose the path. NOTE: If you select Produce report only , domain users are not removed from the local Administrators group when you click Remove all domain users .

- 6 Click **Remove all domain users**.

Deleting groups and users

To delete groups and users

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Delete User/Group**.
- 4 Click **Add** to select the accounts to delete.
- 5 Click **Delete**.

i **NOTE:** From the **Browse** tab, select a type of group or user in the Navigation pane, select one or more groups or users in the Objects pane, select **Tools | Delete**.

-OR-

Click  on the Tool Bar; or right-click selected groups or users, and choose **Delete**.

Creating a new Managed Service Account

Prerequisites

Before creating a Group Managed Service Account, run the following PowerShell cmdlet:

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

This cmdlet makes domain controllers wait 10 hours for Active Directory replication convergence before the creation of a Group Managed Service Account.

To create a new Managed Service Account

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Create User/Group**, and select **Managed Service Account**.
- 4 Type a domain name, or click **Select scope** to select a domain.
- 5 Click **OK**. The **New Managed Service Account** box displays the current selection.

i **NOTE:** To open the **New Managed Service Account** box on the **Browse** tab, select **Domain Managed Service Accounts** in the Navigation pane, and select **Tools | New**.

-OR-

Click  on the Tool Bar; or right-click **Domain Managed Service Accounts**, and choose **New**.

- 6 Type the Common-Name for the new Managed Service Account in the **Name** field.
- 7 Type the SAM-Account-Name for the new Managed Service Account in the **Account Name** field.
- 8 (for Group MSA only) Type the DNS hostname.
- 9 Select a type for the new Managed Service Account.
- 10 Click **Create**.

Modifying Managed Service Account properties

To modify Managed Service Account properties

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **User/Group Properties**.
- 4 Type a Managed Service Account name, or click **Advanced selection**, and select a Managed Service Account.
- 5 Click **View**. The Properties for the selected Managed Service Account displays.

i **NOTE:** To open Properties from the **Browse** tab, select **Domain Managed Service Accounts** in the Navigation pane, select a Managed Service Account in the Objects pane, and select **Tools | Properties**.

-OR-

Click **i**; double-click a Managed Service Account in the Objects pane; or right-click a Managed Service Account, and choose **Properties**.

Modifying Managed Service Account Active Directory properties

To modify Managed Service Account Active Directory properties

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **AD Properties**.
- 4 Type a Managed Service Account name, or click **Advanced selection**, and select a Managed Service Account.
- 5 Click **View**. The Properties for the selected Managed Service Account appears.

i **NOTE:** To open Properties from the **Browse** tab, select **Domain Managed Service Accounts** in the Navigation pane, select a Managed Service Account in the Objects pane, and select **Tools | Active Directory Properties**.

-OR-

Right-click a Managed Service Account in the Objects pane, and choose **Active Directory Properties**.

Viewing Managed Service Account memberships

To view Managed Service Account memberships

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **User/Group Membership**.
- 4 Type a Managed Service Account name, or click **Advanced selection**, and select a Managed Service Account.


- 5 Click **View**. The **Group Memberships** window displays the groups to which the selected Managed Service Account belongs. You can print the list or save it as a .txt file.

i **NOTE:** To access the **Group Memberships** window from the **Browse** tab, select **Domain Managed Service Accounts** in the Navigation pane, select a Managed Service Account in the Objects pane, and select **Tools | Display Memberships**.
-OR-
Right-click a Managed Service Account in the Objects pane, and choose **Display Memberships**.

Deleting Managed Service Account

To delete Managed Service Account

- 1 Open the **Group and User Management** module.
- 2 Open the **Tasks** tab.
- 3 Click **Delete User/Group**.
- 4 Click **Add** to select the Managed Service Accounts to delete.
- 5 Click **Delete**.

i **NOTE:** From the **Browse** tab, select **Domain Managed Service Accounts** in the Navigation pane, select one or more Managed Service Accounts in the Objects pane, select **Tools | Delete**.
-OR-
Click  on the Tool Bar; or right-click selected Managed Service Accounts, and choose **Delete**.

Managing Favorites

You can add frequently-accessed objects to a list of favorites. Each module has a separate list of favorites in the Navigation pane. You can view all the favorites by clicking **All Management Targets**.

You can add an object to the Favorites list as you are browsing in a module, or, if you know what objects you want in your Favorites list, you can use **Tools | Manage Favorites** or **Tools | Manage Computer Favorites** to add them all at once.

Similarly, you can remove Favorites one at a time or in batches. Removing an object from the Favorites list does not remove the object from the system.

Computers you add as Favorites display under the **Computers** heading in the Navigation pane.

Topics:

- [Adding Favorites](#)
- [Exporting Favorites](#)
- [Importing Favorites](#)
- [Removing Favorites](#)

Adding Favorites

By using Manage Favorites or Manage Computer Favorites, you can add objects to the Favorites list regardless of the module with which the object is associated.


NOTE: In the SharePoint Security module, you can add sites (prefixed with http:// or https://) and computers (prefixed with \\) to the Favorites list.

In the SQL Server Security module, you can add only domains, computers, and SQL Server® instances to the Favorites list.

TIP: While you are browsing in modules, you can add objects quickly to the Favorites list.


- Open the module that is associated with the object[s] you want to add to the Favorites list, select the object, and select **Tools | Add to Favorites**.

-OR-

Click  on the Tool Bar; or right-click an object, and choose **Add to Favorites**.

The **Add to Favorites** box opens showing the selected path in the New Favorites list.

To add favorites

- 1 Click  or select **Tools | Manage Favorites**. The Manage Favorites (All types) box lists the objects in the Favorites list.

To manage computers only, select **Tools | Manage Computer Favorites**.

- 2 Click **New**.
- 3 To add a single object, type a path in the **Path** box, and click **Add**.

To add multiple objects while browsing, click **Browse**, select the objects, and click **OK**.

- To remove a selected path from the **New Favorites** list, click **Del**.
- To remove all paths from the **New Favorites** list, click **Clear**.


- 4 Click **OK**.

Objects display under the **Favorites** heading in the Navigation pane. Computers display under the **Computers** heading in the Navigation pane.

Exporting Favorites

If you want to copy a list of Favorites from one computer to another, you can export the Favorites list to a Favorites Export (*.xml) file that you can then import.


To export favorites

- 1 Click  or select **Tools | Manage Favorites** or **Tools | Manage Computer Favorites**.
- 2 Click **Export**.
- 3 Save the file.

Importing Favorites

You can import a list of Favorites that has been saved to a Favorites Export (*.xml) file.


To import favorites

- 1 Click  or select **Tools | Manage Favorites** or **Tools | Manage Computer Favorites**.
- 2 Click **Import**.
- 3 Select the Favorites Export (*.xml) file.
- 4 Click **Open**.

Removing Favorites

Removing an object from the Favorites list does not delete the object from the system.

To remove favorites

- 1 Right-click the object[s] in the Navigation pane, and choose **Remove from Favorites**.
–OR–
Click  or select **Tools | Manage Favorites** or **Tools | Manage Computer Favorites**.
- 2 Select the object[s], and click **Remove**.
- 3 Click **Yes**.

Managing Enterprise Scopes

i | NOTE: The Enterprise Scopes feature is available only in the NTFS Security, Share Security, Registry Security, SQL Security, SharePoint Security, and Exchange Security modules.

An Enterprise Scope is grouping of objects, similar to a folder that contains multiple files, on which you can manipulate permissions. Unlike Favorites, where you can list single paths, Enterprise Scopes can contain multiple paths.

Use Enterprise Scopes to organize objects into logical groups so that you can more easily manage the permissions associated with these objects. For example, you could target multiple drives on one or many servers located across your network. You could group together all home directories, even if they span several drives on several servers. You also could use Enterprise Scopes for quick access of frequently-used paths.

Enterprise Scopes are unique to each module, but you can view all the Enterprise Scopes by clicking **All Management Targets**. All the Enterprise Scopes are listed and identified with the module in which they were created.

i | IMPORTANT: You must select **View | Enterprise Scope Tree Node** to display Enterprise Scopes in the Navigation pane.

There are two ways to create an Enterprise Scope. As you are navigating through the Navigation and Object panes, you can select an object and add it to an Enterprise Scope. You also can create Enterprise Scopes through the Manage Enterprise Scopes feature, which is an efficient method for creating multiple scopes in an organized manner.

i | NOTE: Enterprise Scopes are associated with a specific module. For example, Enterprise Scopes that you create in the NTFS Security module do not display in the Navigation pane in the Registry Security module. To view all Enterprise Scopes, click **All Management Targets**.

Topics:

- [Creating an Enterprise Scope while browsing](#)
- [Creating an Enterprise Scope](#)
- [Editing an Enterprise Scope](#)
- [Removing an Enterprise Scope](#)

Creating an Enterprise Scope while browsing


i | NOTE: The Enterprise Scopes feature is available only in the NTFS Security, Share Security, Registry Security, SQL Security, SharePoint Security, and Exchange Security modules.

When you are navigating through the Navigation and Object panes, you can create an Enterprise Scope quickly by selecting an object and adding it to a scope.

To create an Enterprise Scope while browsing

- 1 Select an object in the Navigation or Objects pane, and select **Tools | Add to Enterprise Scope**.

-OR-

Click  on the Tool Bar, or right-click an object, and choose **Add to Enterprise Scope**.

i | **NOTE:** Computers cannot be added to an Enterprise Scope. If the selected object is a computer, you can choose from three options to add shares to the Enterprise Scope: Include all shares, Exclude ADMIN\$ shares, or Include only ADMIN\$ shares.

- 2 Select options.

Table 11. Enterprise Scopes options

Option	Description
Add to existing Enterprise Scope	Select to add the path displayed in the Paths box to an existing Enterprise Scope, and select an Enterprise Scope from the Name list. <i>Available only if at least one Enterprise Scope exists.</i>
Create and add into a new Enterprise Scope	Select to create a new Enterprise Scope for the path displayed in the Paths box, and type a name for the scope in the Name box.
Edit contents of enterprise scope	Select to open the Manage Enterprise Scope dialog box where you can edit or remove paths from the Enterprise scope. See Editing an Enterprise Scope .

- 3 Click **OK**.

If you did not select the **Edit contents of enterprise scope** check box, the scope appears under Enterprise Scope in the Navigation pane. The selected path displays under the scope name on the current module.

If you selected the **Edit contents of enterprise scope** check box, the **Edit Enterprise Scope** box appears where you can add more paths to the scope. See [Editing an Enterprise Scope](#).

Creating an Enterprise Scope

If you have several Enterprise Scopes to define, creating the scopes through the Manage Enterprise Scope feature is efficient.

i | **NOTE:** The Manage Enterprise Scope function is specific to the module. For example, to create an Enterprise Scope that contains paths to Share Permissions, open the Share Security module.


To create an Enterprise Scope

- 1 Open the module that is associated with the Enterprise Scope you want to create.

i | **NOTE:** You cannot create a new Enterprise Scope if **All Management Targets** is selected. The **New** button is unavailable in the **Manage Enterprise Scope** box.

- 2 Select **Tools | Manage Enterprise Scope**.

-OR-

Click  on the Tool Bar.

- 3 Click **New**.


- 4 Type a name for the Enterprise Scope, and click **OK**.
- 5 Select the Enterprise Scope, and click **Edit**.
- 6 Click **Browse** to select a path, or type a path in the Path box, and click **Add**.
Repeat as many times as necessary.

Editing an Enterprise Scope

To edit an Enterprise Scope

- 1 Select **Tools | Manage Enterprise Scope**.

–OR–

Click  on the Tool Bar.

If **All Management Targets** is selected, the **Manage Enterprise Scope** dialog box lists the existing Enterprise Scopes. If you are in a specific module, only those Enterprise Scopes created in that module display in the list.


- 2 Select an Enterprise Scope, and click **Edit**.
 - To add a path, click **Browse** to select a path, or type a path in the **Path** box, and click **Add**.
 - To remove a selected path from the **Name** list, click **Del**.
 - To remove all paths from the **Name** list, click **Clear**.
- 3 When you are finished editing, click **OK** to apply the changes.

Removing an Enterprise Scope

To remove an Enterprise Scope

- 1 Select **Tools | Manage Enterprise Scope**.

–OR–

Click  on the Tool Bar.

If **All Management Targets** is selected, the **Manage Enterprise Scope** box lists the existing Enterprise Scopes. If you are in a specific module, only those Enterprise Scopes created in that module display in the list.

- 2 Select the Enterprise Scope[s] to remove, and click **Remove**.
- 3 Click **Yes**.

Updating licenses

To update a license

- 1 Select **Help | About Security Explorer**.
 - To view the applied licenses, click **Licenses**.
 - To update a selected license, click **Update License**.

Managing network drives

Security Explorer lets you access Windows® functionality to help you manage your network drives easily.


i | **NOTE:** The Mapping Network Drive function is available only in the NTFS Security and Share Security modules, or All Management Targets.

Mapping a network drive

To map a network drive

- 1 Select **Tools** | **Map Network Drives**.

–OR–

Click  on the Tool Bar.


- 2 Map the drive.
- 3 Click **Finish**.

Disconnecting a network drive

To disconnect a network drive

- 1 Select **Tools** | **Disconnect Network Drives**.

–OR–

Click  on the Tool Bar.

- 2 Select the drive to disconnect.
- 3 Click **OK**.

Working with Microsoft SQL Server

With the SQL Server Security module, you can manage permissions on SQL Server® instances and databases.

Topics:

- [Viewing SQL Server permissions](#)
- [Granting SQL Server permissions](#)
- [Revoking SQL Server permissions](#)
- [Cloning SQL Server permissions](#)
- [Modifying SQL Server permissions](#)
- [Searching for SQL Server objects and permissions](#)
- [Backing up and restoring SQL Server security](#)
- [Exporting SQL Server database permissions](#)
- [Managing SQL Server objects](#)
- [Managing Security SQL Reporting Services](#)
- [Setting options for SQL Server](#)
- [Modifying SQL Server security settings](#)
- [Managing SQL Server network settings](#)

Viewing SQL Server permissions

i | **NOTE:** If the **Always open authentication dialog** check box is selected on the **SQL** tab of the **Options** dialog box, the **SQL Authentication** box appears. Enter the necessary credentials, and click **OK**. See [Setting options for SQL Server](#).

To view SQL Server® permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
–OR–
Click **View Permissions** on the **Tasks** tab.
- 3 Select an item in the Navigation pane.
–OR–

Type a path, in either drive letter notation or UNC pathname format, in the **Path** box, and click **Go**.


The location displays in the **Path** box. The top right Objects pane displays objects along with the extended information. The bottom right Permissions pane displays permissions for the selected object. The **Owner** box displays the user or group that owns the selected object.

- 4 Select **Show permissions** to display permissions (default) for a selected object. Clear the check box to prevent the display of permissions in all windows and dialog boxes. This setting reverts to the default each time you open Security Explorer.

Granting SQL Server permissions

i **TIP:** The Grant task provides a quick way to grant permissions. See [Using the Grant task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the **Grant SQL Permissions** dialog box, but the permissions do not.

To grant SQL Server® permissions

- 1 Open the **SQL Server Security** module.
 - 2 Open the **Browse** tab.
 - 3 Select an item in the Navigation pane, select an object in the Objects pane or a permission in the Permissions pane.
 - 4 Select **Security | Grant Permissions**.
- OR-
- Click  on the Tool Bar, click **Grant** on the Control Button Bar; or right-click the object or permission, and choose **Grant Permissions**.
- 5 Select a group or user from the list or click **User Selection** to select a group/user who is not displayed.
 - 6 From the Permission lists, select a permission to grant. To select more than one permission, select how to apply the permission, and click **Permission Selection**.
 - 7 To add the group/user to the List of users and groups to grant list, click **Add**. The selection is added to the list.
- i** **NOTE:** Only users and groups in the List of users and groups to grant list are affected by the grant action. You can sort each column by clicking the column heading. To remove a selected user or group from the list, click **Remove**.
- 8 Click **OK**. See [Completing a process](#).

Revoking SQL Server permissions


i **TIP:** The Revoke basic task provides a quick way to revoke permissions. You also can use the Revoke Unknown and Revoke Disabled advanced tasks to easily revoke permissions for those specific situations. See [Using the Revoke tasks](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the Revoke SQL Permissions dialog box, but the permissions do not.

To revoke SQL server permissions

- 9 Open the **SQL Server Security** module.
 - 10 Open the **Browse** tab.
 - 11 Select an item in the Navigation pane.
- OR-
- Type a path in the Path box, and click **Go**.
- 12 Select an object in the Objects pane or a permission in the Permissions pane.

- 13 Select **Security | Revoke Permissions**.

-OR-

Click  on the Tool Bar, click **Revoke** on the Control Button Bar; or right-click the object, and choose **Revoke Permissions**.

- 14 Select the groups and users to revoke the permission. There are a variety of ways to select groups and users. See [Using the Browse tab to revoke permissions](#).
- 15 From the Permission list, select the permissions to revoke.
- 16 Select whether or not to allow or deny all permissions for the selected user.
- 17 To add the group/user to the List of users and groups to revoke list, click **Add**.
- 18 Select options.

Table 1. Revoke options

Options	Description
Advanced Revoke Options	If you select this check box, a warning message displays and the Revoke SQL Permissions dialog box becomes inactive, so the other users/groups and permissions you selected are not included in this action. To continue, click Yes .
Revoke all unknown and deleted accounts	<i>Active only when the Advanced Revoke Options check box is selected.</i> Select to revoke permissions on unknown or deleted accounts.
Revoke all disabled accounts	<i>Active only when the Advanced Revoke Options check box is selected.</i> Select to revoke permissions on all disabled accounts.
Log Actions	<i>Active only when the Advanced Revoke Options check box is selected.</i> Select to create a log file. Browse to name the file.

- 19 Click **OK**. See [Completing a process](#).


Cloning SQL Server permissions

i **TIP:** The Clone task provides a quick way to clone permissions. For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the **Clone SQL Permissions** dialog box, but the permissions do not.

To clone SQL Server® permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 Select an object in the Objects pane or a permission in the Permissions pane.
- 4 Select **Security | Clone Group or User**.

-OR-

Click  on the Tool Bar, click **Clone** on the Control Button Bar; or right-click the object, and choose **Clone Group or User**.

- 5 In the **Source Group or User** area, click **User Selection** to select the domain or object from which to pull the permissions.
- 6 In the **Destination Group or User** area, click **User Selection** to select the domain or object to receive the cloned permissions.

i | IMPORTANT: Do not select a pair of accounts where the source is the same as the target. The permissions for the accounts will be deleted as a result of the cloning process.

- 7 Click **Add**. The selected pair displays in the List of users and groups to clone list.
 - To clear all pairs from the list, click **Clear**.
 - To remove selected user(s) or groups(s) from the list, click **Remove**.

8 **Select options.**

Table 2. Clone options

Options	Description
Clone Permissions	By default, permissions are cloned.
Clone group memberships	Select to add the destination account to the groups of which the source user is a member.


- 9 Click **OK**. See [Completing a process](#).

Modifying SQL Server permissions

To modify SQL Server® permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 In the Permissions pane, select a permission.
- 4 Select **Security | Modify Permissions**.

-OR-

Click  on the Tool Bar, click **Modify** on the Control Button Bar; or right-click the permission, and choose **Modify Permissions**.

i | NOTE: The available permission types vary according to the type of object that is selected.
NOTE: If you want to change to another Principal name, click **Change**. The **Select objects** box lists the available objects. Select another name, and click **OK**.

- 5 Select the permissions.
- 6 Click **OK**.

Searching for SQL Server objects and permissions

i | TIP: The Search basic task provides a quick way to search for permissions. You also can use the Find Unknown, Find Disabled, and Insecure Passwords advanced tasks to easily search for those specific situations. See [Using the Search tasks](#).

To search for SQL Server® objects and permissions

- 1 Open the **SQL Server Security** module.

- 2 Open the **Browse** tab.
- 3 Select an object in the Navigation or Objects pane.
- 4 Select **Search | Search in a New Window (Empty)**.

-OR-

Click  on the Tool Bar, or right-click an object, and choose **Search in a New Window**.

The object you select is added as a Search Scope so you can just set the criteria for the search. See [Setting SQL Server search criteria](#).

If you open the **Search** tab in the Navigation pane without selecting an object, you need to add a Search Scope before you set criteria. See [Adding a search scope](#).

i | **NOTE:** If you want to search for passwords, the search scope must be an SQL Server instance and not a database.

- 5 Click **Start Search**.

Setting SQL Server search criteria

Each module has a set of search criteria grouped into tabs. As you set criteria, you can update the results by clicking **Start Search** at any time.

- To return to the default selections on all tabs, click **Defaults**.

Search Mode

Table 3. Search Mode options

Option	Description
Search for permissions	By default, a search returns permissions based on the specified search criteria.
Search for passwords which are blank or fail a strong password test	Select to search for SQL Server® logins with blank passwords or those where the password is the same as the user name.
Search for a user	Select to search for user logins and database/server role memberships. Type the user names in the box. Separate names with semicolons.
Search for all users	Select to include all accounts in Active Directory®.
Search for unknown accounts	Select to include accounts deleted from Active Directory.
Search for disabled accounts	Select to include accounts that are disabled.

Permission Search Criteria

By default, all Grant, Deny, Inherited, and Explicit permissions are included in the search results. To remove a permissions type from the search, clear the corresponding check box.

You can search for the names of the Grantee and/or Grantor, or Permission types.

- To include all role memberships, select the check box.
- To search for Permissions, type the permissions in the box separated by commas, or browse to select permissions from a list.

Permission Search Objects

By default, all permissions are included in the search. To remove a permission from the list, clear the corresponding check box. To remove all permissions, click **None**. To select all permissions, click **All**.

Backing up and restoring SQL Server security

Table 4. Backup and restore SQL Server® security

Task	Description
Backup	See Backing up security .
Restore	See Restoring security .
Scheduled Backups	See Scheduling a backup .

Exporting SQL Server database permissions

By default, permissions are exported to a report, which you can save, print, or export. You can generate a report or export permissions on an SQL Server® database to a delimited file for use with Microsoft® Excel®.

TIP: The Export task provides a quick way to export permissions to a report that you can save, print, or export. See [Using the Export task](#). For more options, click **Switch to Security Explorer Classic (Advanced)**.

To export SQL Server database permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation pane, select the database.
- 4 Select **Security | Export**.

–OR–

Click  on the Tool Bar; or right-click a database, and choose **Export**.

- 5 Select the output option.

Table 5. Output options

Option	Description
Generate Report	By default, permissions are exported to a report, which you can save, print, or export.
Save to Microsoft Excel(R) Spreadsheet	Permissions can be saved only to a delimited file for use with Microsoft Excel. Select either Comma-delimited file (.CSV) or Tab-delimited file (.TXT) .

- 6 Browse to locate a destination for the file.
- 7 Click **OK**.

Managing SQL Server objects

In the SQL Security module, you can manage SQL Server® Databases, Logins, and Server roles.

Topics:

- [Copying SQL Server objects](#)
- [Copying SQL Server permissions](#)
- [Managing SQL Server databases](#)
- [Managing logins](#)
- [Managing server roles](#)

Copying SQL Server objects

You can copy database users from one database to another, and logins from one SQL Server® instance to another.

To copy SQL Server objects


- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 Right-click a login or a database user in the Navigation or Objects pane, and choose **Copy Object**.
- 4 Select a new location, such as another database, right-click, and choose **Paste Object**.

Copying SQL Server permissions

To copy SQL Server® permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 Select one or more permissions in the Permissions pane.
- 4 Select **Security | Copy Permission**.

-OR-

Click  on the Tool Bar; or right-click a permission, and choose **Copy Permission**.

i | **NOTE:** To select all permissions in the list, select **Security | Select All Permissions**, or right-click in the Permissions pane, and choose **Select All Permissions**.

- 5 Select a new location, such as another database.
- 6 Select **Security | Paste Permissions**.

-OR-

Click  on the Tool Bar; or right-click, and choose **Paste Permissions**.

Managing SQL Server databases

You can view the assemblies, functions, stored procedures, synonyms, tables, and views for SQL Server® databases by expanding the category in the Navigation pane. You also can add, edit, and delete database roles and users, and add or delete schemas.

Topics:

- [Adding a new database role](#)
- [Removing a database role](#)
- [Modifying a database role](#)
- [Adding a new database user](#)
- [Removing a database user](#)
- [Modifying a database user](#)
- [Adding a new schema](#)
- [Removing a schema](#)
- [Modifying a schema](#)

Adding a new database role

To add a new database role

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and expand a database.
- 3 Select **Database Roles**, and select **Tools | New**.
–OR–
Right-click **Database Roles**, and choose **New**.
- 4 Type a name for the database role.
- 5 To assign members to the role, open the Role Members tab, and click **Add**.
- 6 Select the members to add, and click **OK**.
- 7 To assign permissions to the role, open the **Permissions** tab. Use the scroll bar or adjust the panes as necessary to view the contents.

Removing a database role

To remove a database role

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and expand a database,
- 3 Select a database role, and select **Tools | Delete**.
–OR–
Right-click a database role, and choose **Delete**.
- 4 Click **Yes**. See [Completing a process](#).


Modifying a database role

You can change the members of a role and its permission.

To modify a database role

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and expand a database.
- 3 Select a database role, and select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click a database role, and choose **Properties**. See [Adding a new database role](#)

Adding a new database user

To add a new database user

- 1 Open the **SQL Server Security** module.
 - 2 In the Navigation pane, select a server, and expand a database,
 - 3 Select **Users**, and select **Tools | New**.
- OR-
- Right-click **Users**, and choose **New**.
- 4 Type the username.
 - 5 Select how to map the user.
 - 6 If you select Login, browse to select a login.
 - 7 Open the **Roles membership** tab to select database roles.
 - 8 To assign permissions to the user, open the **Permissions** tab. Use the scroll bar or adjust the panes as necessary to view the contents.

Removing a database user

To remove a database user

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and expand a database.
- 3 Select a user, and select **Tools | Delete**.

-OR-

Right-click a user, and choose **Delete**.

- 4 Click **Yes**. See [Completing a process](#).

Modifying a database user


Once a user is created, you can modify the roles in which the user is a member and the user's permissions.


To modify a database user

- 1 Open the **SQL Server Security** module.

- 2 In the Navigation pane, select a server, and expand a database.
- 3 Select a database user, and select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click one or more users in the Objects pane, and choose **Properties**.

 **NOTE:** If you select more than one user, the actions apply to all the users in the selection, not just the one user displayed in the **Role Name** box.

See [Adding a new database user](#).

Adding a new schema

To add a new schema

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and expand a database.
- 3 Select **Schemas**, and select **Tools | New**. Alternatively, right-click **Schemas**, and choose **New**.
- 4 Type the name of the schema to add.
- 5 Browse to select the name of a database user or role to own the schema.

Removing a schema

To remove a schema

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and expand a database.
- 3 Select a schema, and select **Tools | Delete**. Alternatively, right-click a schema, and choose **Delete**.
- 4 Click **Yes**. See [Completing a process](#).

Modifying a schema

You can change the owner of a schema.

To modify a schema

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and expand a database.
- 3 Select a schema, and select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click a schema, and choose **Properties**.

Managing logins

You can add, edit, or delete logins.

Adding a new login

To add a new login

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server.
- 3 Select **Logins**, and select **Tools | New**. Alternatively, right-click **Logins**, and choose **New**.
- 4 Type a name, or click **Search** to locate a name.
- 5 Select whether to use Windows® or SQL Server® Authentication. If you select **SQL Server Authentication**, assign a password.
- 6 Choose the default database from the list.
- 7 To assign server roles, open the **Server Roles** tab.
- 8 To assign user mappings, open the **User Mappings** tab.

Removing a login

To remove a login

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server.
- 3 Select a login, and select **Tools | Delete**. Alternatively, right-click a login, and choose **Delete**.
- 4 Click **Yes**. See [Completing a process](#).

Modifying a login

You can change the default database, server role, and user mapping.

To modify a login

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server.
- 3 Select a login, and select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click a login, and choose **Properties**.

Managing server roles

If you are using Microsoft® SQL Server® 2012, 2014, 2016, or 2019, you can manage SRS roles and permissions.

Adding a server role

To add a server role

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server.
- 3 Select **Server Roles**, and select **Tools | New**. Alternatively, right-click **Server Roles**, and choose **New**.

- 4 Type the name of the new server role.
- 5 Browse to select an owner.
- 6 Click **Add** to add logins to the selected server role.
- 7 Select the server role, open the **Memberships** tab, and select the database roles to assign to the server role.
- 8 Open the **Permissions** tab, expand the **Securables**, and modify permissions as necessary.

Removing a server role

To remove a server role


- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server.
- 3 Select a server role, and select **Tools | Delete**. Alternatively, right-click a server role, and choose **Delete**.
- 4 Click **Yes**. See [Completing a process](#).

Modifying server roles

To modify server roles

- 5 Open the **SQL Server Security** module.
- 6 In the Navigation pane, select a server.
- 7 Select a server role, and select **Tools | Properties**.


-OR-

Click  on the Tool Bar; or right-click a server role, and choose **Properties**.

Managing Security SQL Reporting Services

Security Explorer allows to manage Security SQL Reporting Services (SSRS) in the following ways:

- Create, edit, and delete system roles. Each system role is a set of special permissions, similar to permission levels in SharePoint®. System roles can be granted only on SSRS instances.
- Create, edit, and delete catalog roles. Each catalog role is also a set of special permissions. Catalog roles apply to SSRS catalog items.
- Manage security of catalog items. Catalog items can be models, data sources, reports, folders and files. You can grant, revoke, clone, modify, copy, delete, export, back up, and restore SSRS permissions.


 | **NOTE:** SSRS is visible only when browsing in the Network Node.

Topics:

- [Managing system roles](#)
- [Managing catalog roles](#)
- [Managing catalog items](#)

Managing system roles

You can add, delete, and modify system roles.

 | **NOTE:** Security SQL Reporting Services (SSRS) is visible only when browsing in the Network Node.

Creating a new system role

To create a new system role

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, expand the **Network** node, and select a server.
- 3 Select **System Roles**, and select **Tools | New**. Alternatively, right-click **System Roles**, and choose **New**.

Deleting system roles

To delete system roles

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, expand the **Network** node, select a server, and expand **System Roles**.
- 3 Select a system role, and select **Tools | Delete**. Alternatively, right-click a system role, and choose **Delete**.
- 4 Click **Yes**. See [Completing a process](#).


Modifying a system role

You can modify the description and tasks assigned to the role.

To modify a system role


- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, expand the **Network** node, select a server, and expand **System Roles**.
- 3 Select a server role, and select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click a system role, and choose **Properties**.

Managing catalog roles

You can add, delete, and modify catalog roles.

 | **NOTE:** Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

Creating a new catalog role

To create a new catalog role

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, expand the Network node, and select a server.

- 3 Select **Catalog Roles**, and select **Tools | New**. Alternatively, right-click **Catalog Roles**, and choose **New**.

Deleting catalog roles

To delete catalog roles

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, expand the Network node, select a server, and expand **Catalog Roles**.
- 3 Select a catalog role, and select **Tools | Delete**. Alternatively, right-click a catalog role, and choose **Delete**.
- 4 Click **Yes**. See [Completing a process](#).


Modifying a catalog role

You can modify the description and tasks assigned to the role.

To modify a catalog role

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, expand the Network node, select a server, and expand **Catalog Roles**.
- 3 Select a catalog role, and select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click a catalog role, and choose **Properties**.

Managing catalog items

Catalog items can be models, data sources, reports, folders and files. You can grant, revoke, clone, copy, delete, export, back up, and restore SSRS roles and permissions.

Topics:

- [Granting SSRS permissions](#)
- [Revoking SSRS permissions](#)
- [Cloning SSRS permissions](#)
- [Searching for SSRS permissions](#)
- [Modifying SSRS permissions](#)
- [Copying SSRS permissions](#)
- [Deleting SSRS permissions](#)
- [Exporting SSRS permissions](#)
- [Backing up and restoring SSRS permissions](#)

Granting SSRS permissions


i **TIP:** The Grant task provides a quick way to grant permissions. See [Using the Grant task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the Grant SSRS Permissions dialog boxes, but the permissions do not.

NOTE: Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

To grant SSRS permissions

- 4 Open the **SQL Server Security** module.
- 5 Open the **Browse** tab.
- 6 Select an item in the Navigation pane, select an object in the Objects pane, or a permission in the Permissions pane.
- 7 Select **Security | Grant**.

-OR-

Click  on the Tool Bar, click **Grant** on the Control Button Bar; or right-click the object or permission, and choose **Grant Permissions**.

- 8 Click **Advanced User Selection** to select a group/user.
- 9 From the **Role** list, select a role to grant. To select more than one role, click **Advanced Permission Selection**.
- 10 To add the group/user to the **List of users and groups to grant** list, click **Add**.

i **NOTE:** Only users and groups in the **List of users and groups to grant** list are affected by the grant action. You can sort each column by clicking the column heading. To remove a selected user or group from the list, click **Remove**.

- 11 Click **OK**. See [Completing a process](#).

Revoking SSRS permissions


i **TIP:** The Revoke basic task provides a quick way to revoke permissions. See [Using the Revoke tasks](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the Revoke SQL Permissions dialog box, but the permissions do not.

NOTE: Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

To revoke SSRS permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane, select an object in the Objects pane, or a permission in the Permissions pane.
- 4 Select **Security | Revoke Permissions**.

-OR-

Click  on the Tool Bar, click **Revoke** on the Control Button Bar; or right-click the object, and choose **Revoke Permissions**.

- 5 Click **Advanced User Selection** to select a group/user.
- 6 Select a role to revoke. To select more than one role, click **Advanced Permission Selection**.
- 7 To add the group/user to the List of users and groups to revoke list, click **Add**.
- 8 Click **OK**. See [Completing a process](#).

Cloning SSRS permissions


i **TIP:** The Clone task provides a quick way to clone permissions. See [Using the Clone task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the Clone SSRS Permissions dialog box, but the permissions do not.

NOTE: Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

To clone SSRS permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 Select an object in the Objects pane, or a permission in the Permissions pane.
- 4 Select **Security | Clone Group or User**.

-OR-

Click  on the Tool Bar, click **Clone** on the Control Button Bar; or right-click the object, and choose **Clone Group or User**.

- 5 In the Source Group or User area, click **User Selection** to select the domain or object from which to pull the permissions.
- 6 In the Destination Group or User area, click **User Selection** to select the domain or object to receive the cloned permissions.

i **IMPORTANT:** Do not select a pair of accounts where the source is the same as the target. The permissions for the accounts will be deleted as a result of the cloning process.

- 7 Click **Add**.
- 8 Click **OK**. See [Completing a process](#).

Searching for SSRS permissions

i **TIP:** The Search basic task provides a quick way to search for permissions. See [Using the Search tasks](#).

NOTE: Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

To search for SSRS permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 Select an object in the Navigation or Objects pane.
- 4 Select **Search | Search in a New Window (Empty)**.

-OR-

Click  on the Tool Bar, or right-click an object, and choose **Search in a New Window**.

The object you select is added as a Search Scope so you can just set the criteria for the search, and start the search. See [Setting SQL Server search criteria](#).

If you open the Search tab in the Navigation pane without selecting an object, you need to add a Search Scope before you set criteria. See [Adding a search scope](#).

- 5 Set options.

Table 6. Search for permission options

Option	Description
Search for permissions	By default, a search returns permissions based on the specified search criteria.
Permission Search Criteria	By default Inherited, and Explicit permissions are included in the search results. To remove a permissions type from the search, clear the corresponding check box. To search for Permissions, type the permissions in the box separated by commas. Alternatively, browse to select permissions from a list.
Permission Search Objects	By default, all permissions are included in the search. To remove a permission from the list, clear the corresponding check box. To remove all permissions, click None . To select all permissions, click All .

- 6 Click **Start Search**.


Modifying SSRS permissions

i | **NOTE:** Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

To modify SSRS permissions

- 1 Open the **SQL Server Security** module.
- 2 Open the **Browse** tab.
- 3 In the Permissions pane, select a permission.
- 4 Select **Security | Modify Permissions**.

-OR-

Click  on the Tool Bar, click **Modify** on the Control Button Bar; or right-click the permission, and choose **Modify Permissions**.

i | **NOTE:** If you want to change to another Principal name, click **Change**. The Select objects box lists the available objects. Select another name, and click **OK**.

- 5 Select the roles.
- 6 Click **OK**.

Copying SSRS permissions

i | **NOTE:** Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

See [Copying permissions](#).

Deleting SSRS permissions

i | **NOTE:** Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

See [Deleting permissions](#).

Exporting SSRS permissions

By default, permissions are exported to a report, which you can save, print, or export. You can generate a report or export permissions on a database to a delimited file for use with Microsoft® Excel®.

TIP: The Export task provides a quick way to export permissions to a report that you can save, print, or export. See [Using the Export task](#). For more options, click **Switch to Security Explorer Classic (Advanced)**.

NOTE: Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

See [Exporting SQL Server database permissions](#).

Backing up and restoring SSRS permissions

NOTE: Security SQL Reporting Services (SSRS) roles and permissions are visible only when browsing in the Network node.

See [Backing up security](#).

Setting options for SQL Server

To set options for SQL Server®

- 1 Select **Tools | Options**.
- 2 Open the **SQL** tab.
- 3 Set options for SQL Server.

Table 7. SQL Server options

Option	Description
Display separate domain column in permissions list	By default, the domain for each object is listed in the Permissions pane. Clear the check box to remove the Domain column from the Permissions pane.
Display SQL Server version	By default, SQL Server displays in the Type column in the Objects pane when you select the SQL Server Security module. Select to display the version and service pack level in the Type column. NOTE: Security Explorer must be able to connect to the server to display the version and service level.

- 4 Set default SQL Server credentials.

Table 8. Default SQL Server credentials options

Option	Description
Use Windows Authentication	By default, Security Explorer uses Windows® Authentication when connecting to SQL Server.

Table 8. Default SQL Server credentials options

Option	Description
Always open authentication dialog	Select to display the Open Authentication dialog box when connecting to SQL Server.
Use alternate credentials list	Select to use the alternate credentials list when connecting to SQL Server. Security Explorer tries each account in the order they appear in the list until an account is found with sufficient privileges. If no account is found, Access Denied is displayed. NOTE: You can use only an SQL account for SQL alternate credentials. You cannot use a Windows account.


Table 9. SQL Server alternate credentials options

Button	Description
Add	Add an alternate credential. <ol style="list-style-type: none"> 1 Type an account name, or browse to select an account. 2 Type the password. 3 Type a computer name (<i>optional</i>). NOTE: If you do not enter a computer name, each account is tried in the order listed until an account is found with sufficient privileges. 4 Click OK.
Edit	Edit a selected alternate credential.
Del	Delete a name from the list.
Clear	Clear all names from the list.

Modifying SQL Server security settings

i | **TIP:** You can use the Security Settings advanced task to modify SQL Server® security settings. Click **Security Settings**, add a path, and click **OK**.

To modify SQL Server security settings

- 1 Open the **SQL Server Security** module.
- 2 In the Navigation pane, select a server, and select **Tools | SQL Server Security Settings**.
-OR-
Click  on the Tool Bar; or right-click a server, and choose **SQL Server Security Settings**.
- 3 Set the Server Authentication and the type of logins to audit: None, Failed logins only, Successful logins only, or Both failed and successful logins.

Managing SQL Server network settings


i | **TIP:** You can use the Network Settings advanced task to modify SQL Server® security settings. Click **Network Settings**, add a path, and click **OK**.

To manage SQL Server network settings

- 1 Open the **SQL Server Security** module.

- 2 In the Navigation pane, select a server, and select **Tools | SQL Network Settings**.

-OR-

Click  on the Tool Bar; or right-click a server, and choose **SQL Network Settings**.

- 3 Open the **Network Settings** tab to view network protocol properties.

Working with Microsoft Exchange

With the Exchange Security module, you can view permissions on Administrative Groups, Exchange Administrators, Exchange Distribution Groups, Mailboxes, and Public Folders. For Microsoft® Exchange 2010, 2013, 2016, and 2019, you can manage entities in Role-Based Access Control (RBAC).

i | **NOTE:** Public folders created in Exchange native tools are mail disabled by default. Public Folders created with Security Explorer are mail-enabled for all Exchange versions.

Topics:

- [Checking minimum requirements](#)
- [Viewing Exchange permissions](#)
- [Granting Exchange permissions](#)
- [Revoking Exchange permissions](#)
- [Cloning Exchange permissions](#)
- [Searching for Exchange server objects and permissions](#)
- [Backing up and restoring Exchange server security](#)
- [Modifying Exchange permissions](#)
- [Managing Exchange group memberships](#)
- [Exporting Exchange security permissions](#)
- [Creating Exchange databases](#)
- [Creating public folder mailboxes](#)
- [Managing Exchange administrators](#)
- [Managing Exchange distribution groups](#)
- [Managing mail contacts](#)
- [Managing mail users](#)
- [Managing mailboxes](#)
- [Managing mailbox folders](#)
- [Managing public folders](#)
- [Using role based access control](#)
- [Setting options for Exchange security](#)

Checking minimum requirements

The first time you expand an Exchange server in the Navigation pane of the Exchange Security module, an information message displays the minimum requirements for managing Exchange security.

For more detailed information about minimum requirements, see the *Security Explorer Installation Guide*.

To check minimum requirements

- 1 Open the **Exchange Security** module for the first time.
 - To view the minimum requirements, click the version of Exchange.
 - To view a list of prerequisites for the current account, click **Pre-Requisites**.
- 2 If you click **Yes** to proceed, you are asked to enable Exchange Impersonation for the selected organization. Exchange Impersonation must be enabled for the currently logged on user.

i | **IMPORTANT:** If you are using Exchange Server 2013, 2016, or 2019, you do not have the opportunity to enable Exchange Impersonation at this point. You must enable Exchange impersonation prior to accessing the Exchange Server in Security Explorer.

Viewing Exchange permissions

i | **IMPORTANT:** If Exchange Server 2013, 2016, or 2019 is installed in a child domain, you cannot manage directory permissions nor disable the mail-enable property for public folders.

To view Exchange permissions

- 1 Open the **Exchange Security** module.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane. Alternatively, type a path, in either drive letter notation or UNC pathname format, in the Path box, and click **Go**.

The Objects pane displays objects along with the extended information. The Permissions pane displays permissions for the selected object.

i | **NOTE:** If user has a different login name and display name, the login name is used to display directory permissions, and the display name (from Address book) is used to display Mailbox/Public Folder permissions.

Granting Exchange permissions


i | **IMPORTANT:** If Exchange Server 2013, 2016, or 2019 is installed in a child domain, you cannot grant directory permissions to mail-enabled public folders.

TIP: The Grant task provides a quick way to grant permissions. See [Using the Grant task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the Grant Exchange Permissions dialog box, but permissions do not.

To grant Exchange permissions using the Browse tab

- 1 Open the **Exchange Security** module.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane, or type a path in the Path box, and click **Go**.
- 4 Select an object in the Objects pane or a permission in the Permissions pane.
- 5 Select **Security | Grant Permissions**.

-OR-

Click , click **Grant** on the Control Button Bar; or right-click the object or permission, and choose **Grant Permissions**.

- 6 Select the groups and users to grant the permission. There are a variety of ways to select groups and users. See [Using the Browse tab to grant permissions](#).
- 7 Select a permission type, a permission to grant and how to apply it.
 - To select more than one permission, select how to apply the permission, and click **Advanced Permission Selection**.
 - To propagate the permission to subfolders, select the check box.
- 8 To add the group/user to the List of users and groups to grant list, click **Add**.
- 9 Click **OK**. See [Completing a process](#).

Revoking Exchange permissions

i **TIP:** The Revoke basic task provides a quick way to revoke permissions. You also can use the Revoke Unknown and Revoke Disabled advanced tasks to easily revoke permissions for those specific situations. See [Using the Revoke tasks](#).
For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the Revoke Exchange Permissions dialog box, but the permissions do not.

To revoke Exchange permissions using the Browse tab


- 1 Open the **Exchange Security** module.
 - 2 Open the **Browse** tab.
 - 3 Select an item in the Navigation pane, or type a path in the Path box, and click **Go**.
 - 4 Select an object in the Objects pane or a permission in the Permissions pane.
 - 5 Select **Security | Revoke Permissions**.
- OR-
- Click , click **Revoke** in the Control Button Bar; or right-click the object, and choose **Revoke Permissions**.
- 6 Select the groups and users to revoke the permission. There are a variety of ways to select groups and users. See [Using the Browse tab to revoke permissions](#).
 - 7 From the Permission list, select the permissions to revoke, and whether or not to Allow or Deny. If the choice is not available in the list, click **Advanced Permission Selection** to create a custom choice.
 - 8 To add the group/user to the List of users and groups to revoke list, click **Add**.
 - 9 Select options.

Table 1. Revoke options

Option	Description
Revoke all permissions (Allow and Deny) for the selected user	Select to revoke all permissions (Allow and Deny) for the selected user.
Propagate permissions down to subfolders	Select to revoke permissions in any subfolders for the selected user.
Advanced Revoke Options	If you select this check box, a warning message displays and the Revoke Folder Permissions dialog box becomes inactive, so the other users/groups and permissions you selected are not included in this action. To continue, click Yes .

Table 1. Revoke options

Option	Description
Revoke all unknown and deleted accounts	<i>Active only when the Advanced Revoke Options check box is selected.</i> Select to revoke permissions on unknown or deleted accounts.
Revoke all disabled accounts	<i>Active only when the Advanced Revoke Options check box is selected.</i> Select to revoke permissions on all disabled accounts. NOTE: For Exchange 2010, mailbox folder disabled permissions do not display in Security Explorer, therefore the Revoke Disabled Accounts function will not be able to revoke those permissions. NOTE: For Exchange 2010, public folder disabled permissions display with NT User: within the account name and cannot be revoked.

10 Click **OK**. See [Completing a process](#).

Cloning Exchange permissions

- i** | **IMPORTANT:** If Exchange Server 2013, 2016, or 2019 is installed in a child domain, you cannot manage directory permissions nor disable the mail-enabled property for public folders.
- TIP:** The Clone task provides a quick way to clone permissions. See [Using the Clone task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**. The path carries to the Clone Exchange Permissions dialog box, but the permissions do not.

To clone Exchange permissions using the Browse tab


- 1 Open the **Exchange Security** module.
 - 2 Open the **Browse** tab.
 - 3 Select an object in the Objects pane or a permission in the Permissions pane.
 - 4 Select **Security | Clone Group or User**.
- OR-
- Click  on the Tool Bar; or right-click the object, and choose **Clone Group or User**.
- 5 In the Source Group or User area, click **Advanced User Selection** to select the domain or object from which to pull the permissions.
 - 6 In the Destination Group or User area, click **Advanced User Selection** to select the domain or object to receive the cloned permissions.
- i** | **IMPORTANT:** Do not select a pair of accounts where the source is the same as the target. The permissions for the accounts will be deleted as a result of the cloning process.
- 7 Click **Add**. The selected pair displays in the List of users and groups to clone list.
 - To clear all pairs from the list, click **Clear**.
 - To remove selected users from the list, click **Remove**.
 - 8 **Select options.**

Table 2. Clone options


Option	Description
Clone Permissions	By default, permissions are cloned.
Clone group memberships	Select to add the destination account to the groups of which the source user is a member.

- 9 Click **OK**. See [Completing a process](#).

Searching for Exchange server objects and permissions

i **TIP:** The Search basic task provides a quick way to search for permissions. You also can use the Find Unknown and Find Disabled advanced tasks to easily search for those specific situations. See [Using the Search tasks](#).

To search for Exchange server objects and permissions using the Browse tab

- 1 Open the **Exchange Security** module.
 - 2 Open the **Browse** tab.
 - 3 Select an object in the Navigation or Objects pane.
 - 4 Select **Search | Search in a New Window (Empty)**.
 - OR-
 - Click  on the Tool Bar, or right-click an object, and choose **Search in a New Window**.
 - 5 The object you select is added as a Search Scope so you can just set the criteria for the search. See [Setting Exchange security search criteria](#).
- If you open the Search tab in the Navigation pane without selecting an object, you need to add a Search Scope before you set criteria. See [Adding a search scope](#).
- 6 Click **Start Search**. See [Using the Browse tab to search](#).

Setting Exchange security search criteria

Each module has a set of search criteria grouped into tabs. As you set criteria, you can update the results by clicking **Start Search** at any time.

- To return to the default selections on all tabs, click **Defaults**.

Permission search criteria

Table 3. Permission search criteria

Option	Description
Name	Type the names of the principals you want to find. Separate names with semicolons. You can use the * and ? wildcards.
Include all group memberships	Select to find all locations that a user has access throughout the Exchange Organization, both directly and indirectly assigned. The drop-down list populates with the group names.

Table 3. Permission search criteria

Option	Description
Directory Permissions	By default, all Directory, Mailbox, Mailbox Folder, and Public-Folder permissions are included in the search results. To remove a permissions type from the search, clear the corresponding check box.
Mailbox Permissions	
Mailbox Folder Permissions	
Public Folder Permissions	
Permissions	You can search for a name or a permission type. If you want to search for permissions, type the permissions in the box separated by commas. Alternatively, browse to select permissions from a list.
Allow Permissions	By default, Allow, Deny, Inherited, and Explicit permissions are included in the search results. To remove a permissions type from the search, clear the corresponding check box.
Deny Permissions	
Inherited Permissions	
Explicit Permissions	
Search for unknown accounts	Select to include accounts deleted from Active Directory®. TIP: You also can use the Find Unknown advanced task to search easily for unknown accounts.
Search for disabled accounts	Select to include accounts that are disabled. TIP: You also can use the Find Disabled advanced task to search easily for disabled accounts.

Permission search objects

By default, all permissions are included in the search. To remove a permission from the list, clear the corresponding check box. To remove all permissions, click **None**. To select all permissions, click **All**.

Backing up and restoring Exchange server security

Table 4. Exchange Security backup and restore tasks

Task	Description
Backup	See Backing up security .
Restore	See Restoring security .
Scheduled Backups	See Scheduling a backup .

Modifying Exchange permissions


NOTE: If you are using Exchange Server 2010, you cannot delete Default empty permission from public folders.
If you are using Exchange Server 2013, 2016, or 2019, you cannot delete Default empty permission for Default and Anonymous from public folders.

To modify Exchange permissions

- 1 Open the **Exchange Security** module.
- 2 Open the **Browse** tab.

- 3 Select an object in the Navigation or Objects pane.
- 4 Select a permission in the Permissions pane.
- 5 Select **Security | Modify Permissions**.

-OR-

Click  on the Tool Bar; click **Modify** on the Control Button Bar; or right-click the permission, and choose **Modify Permissions**.

- 6 Modify the permissions.
- 7 Click **OK**.

Managing Exchange group memberships

To manage Exchange group memberships

- 1 Open the **Exchange Security** module.
- 2 Open the **Browse** tab.
- 3 Select an object in the Navigation or Objects pane.
- 4 Select a single permission in the Permissions pane.
- 5 Select **Tools | Display Group Contents** or **Tools | Display Group Membership**.
- 6 Select a member, and click a button corresponding to the action you want to perform.

Table 5. Managing Exchange group memberships

Button	Description
Add	Add members to the selected group. See Modifying group memberships .
Remove	Remove selected members from the selected group.
Refresh	Refresh the list after adding or removing a member.
Print	Print the list.
Save	Save the list as a .txt file.
Show Group Contents	View the members of a selected group.
Show Memberships	Show the groups of which the selected group or user is a member. NOTE: You also can view memberships by right-clicking a selected group or user in the Permission pane, and choosing Display Memberships .
Close	Close the Group contents box.

Exporting Exchange security permissions


By default, permissions are exported to a report, which you can save, print, or export. You can generate a report or export permissions to a delimited file for use with Microsoft® Excel®.

- TIP:** The Export task provides a quick way to export permissions to a report that you can save, print, or export. See [Using the Export task](#). For more options, click **Switch to Security Explorer Classic (Advanced)**.

To export Exchange security permissions

- 1 Open the **Exchange Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select one or more items.
- 4 Select **Security | Export**.

-OR-

Click  on the Tool Bar; or right-click a selection of objects, and choose **Export**.

- 5 Select options.

Table 6. Report options

Option	Description
Exchange permissions report	Select to include all the permissions for the selected path.
Exchange Non-Owner Permissions report	Select to include only the permissions for non-owners with explicit access to the Inbox folders. This option is useful to discover if a user has given someone explicit access to their inbox, or alternatively, if a rogue administrator has added himself to a user inbox. This option is available only for mailboxes.
Generate Report	By default, permissions are exported to a report, which you can save, print, or export.
Save to Microsoft Excel® Spreadsheet	SQL database permissions can be saved only to a delimited file for use with Microsoft Excel. Select either Comma-delimited file (.CSV) or Tab-delimited file (.TXT) . Browse to locate a destination for the file.

- 6 To export the data in the specified format, click **OK**.

Creating Exchange databases

You can create new mailbox and public folder databases.

To create an exchange database

- 1 Open the **Exchange Security** module.
- 2 Open the **Browse** tab.
- 3 Select the Exchange server or Exchange storage group in the Navigation pane.
- 4 Select **Tools | New**. Alternatively, right-click the Exchange Server or Storage Group, and choose **New**.
- 5 Choose the database to create, and click **Next**.
- 6 Type a name for the database. By default, the database will be mounted. If you do not want to mount the database, clear the check box.
- 7 Click **Next**.
- 8 Review the database details, and click **New**.
- 9 Click **Finish**.

Creating public folder mailboxes

In Exchange Server 2013, 2016, and 2019, public folders are considered public folder mailboxes and are managed by the Exchange Admin Center. You create public folder mailboxes in the New Database dialog box.

To create a public folder mailbox


- 1 Open the **Exchange Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation pane, expand the **Exchange Administrative Group**.
- 4 Select the Exchange server with the Mailbox Role, and select **Tools | New**. Alternatively, right-click the Exchange server with the Mailbox role, and choose **New**.
- 5 Select **Public Folder mailbox**, and click **Next**.
- 6 Type a name for the Public Folder mailbox.
- 7 Select the Mailbox Store.
- 8 Click **Next**.
- 9 Review the database details, and click **New**.
- 10 Click **Finish**.

Managing Exchange administrators

- [Adding Exchange administrators](#)
- [Modifying Exchange administrators](#)
- [Deleting Exchange administrators](#)

Adding Exchange administrators

To add an Exchange administrator

- 1 Open the **Exchange Security** module.
- 2 Expand **Exchange Administrators**, and select an Exchange group.
- 3 Select **Tools | Properties**.
-OR-
Click ; or right-click an Exchange group, and choose **Properties**.
- 4 Click **Add Member**, and locate one or more users or groups to add to the Exchange Group.


Modifying Exchange administrators

You can change only the role for a selected account.

To modify Exchange administrators

- 1 Open the **Exchange Security** module.
- 2 Select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click an Exchange group, and choose **Properties**.

Deleting Exchange administrators

To delete Exchange administrators

- 1 Open the **Exchange Security** module.
- 2 Expand **Exchange Administrators**.
- 3 Select an Exchange group, and select **Tools | Properties**. Alternatively, right-click an Exchange group, and choose **Properties**.
- 4 Select one or more members, and click **Delete Selected**.

Managing Exchange distribution groups

You can add, modify, or delete Universal or Dynamic distribution groups.

i **NOTE:** With Exchange 2013, 2016, and 2019, you can add text or a user attribute to the prefix and suffix of the distribution group name. For example, if you select the City attribute, the group name will include the city value for the current user. It is also possible to enter a blocked word that cannot be used to create the name of a group. If a user attempts to use the blocked word when naming a group, a warning box displays.

Adding distribution groups

To add a distribution group

- 1 Open the **Exchange Security** module.
- 2 Select **Exchange Distribution Groups**, and select **Tools | New**. Alternatively, right-click **Exchange Distribution Groups**, and choose **New**.
- 3 Select either **Universal Distribution Group** or **Dynamic Distribution Group**.

Modifying distribution groups

To modify a distribution group

- 1 Open the **Exchange Security** module.
- 2 Expand **Exchange Distribution Groups**.
- 3 Select the distribution group, and select **Tools | Properties**. Alternatively, right-click the distribution group, and choose **Properties**.

Deleting distribution groups

To delete a distribution group


- 1 Open the **Exchange Security** module.
- 2 Expand **Exchange Distribution Groups**.
- 3 Select the distribution group, and select **Tools | Delete**. Alternatively, right-click the distribution group, and choose **Delete**.

Managing mail contacts

- [Creating mail contacts](#)
- [Modifying mail contacts](#)
- [Modifying mail contacts](#)
- [Deleting mail contacts](#)


Creating mail contacts

To create mail contacts

- 1 Open the **Exchange Security** module.
- 2 Select **Mail Contacts**, and select **Tools | New**. Alternatively, right-click **Mail Contacts**, and choose **New**.
 | **NOTE:** Boxes marked with an asterisk (*) are required entries.
- 3 Enter the user's account information, and click **Next**.
- 4 Type the user's alias.
- 5 Click **Edit**.
- 6 Enter the email address of the user and the type of email, and click **OK**.
- 7 Click **New**.
- 8 Click **Finish**.

Modifying mail contacts

To modify mail contacts

- 1 Open the **Exchange Security** module.
 - 2 Expand the **Mail Contacts** category, and select the mail contact.
 - 3 Select **Tools | Properties**.
- OR-
- Click  on the Tool Bar, or right-click the mail contact, and choose **Properties**.

Deleting mail contacts

To delete mail contacts

- 1 Open the **Exchange Security** module.
- 2 Expand the **Mail Contacts** category.
- 3 Select a contact, and select **Tools | Delete**. Alternatively, right-click a mailbox contact, and choose **Delete**.


Managing mail users

- [Creating mail users](#)
- [Modifying mail users](#)
- [Deleting mail users](#)

Creating mail users

To create a mail user

- 1 Open the **Exchange Security** module.
- 2 Select **Mail Users** in the Navigation pane, and select **Tools | New**. Alternatively, right-click **Mail Users**, and choose **New**.
- 3 Choose to create a new user or select an existing user.
- 4 Click **Next**. If you selected **Existing user**, skip ahead to step 7.
- 5 Enter the account information of the user, and click **Next**.

 **NOTE:** Boxes marked with an asterisk (*) are required entries.


- 6 Enter the user's contact information, and click **Next**.
- 7 Type the alias of the user.
- 8 Click **Edit**.
- 9 Enter the email address of the user and the type of email, and click **OK**.
- 10 Click **Next**.
- 11 Click **New**.
- 12 Click **Finish**.

Modifying mail users

To modify a mail user

- 1 Open the **Exchange Security** module.
- 2 Select a mail user.
- 3 Select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click the mail user, and choose **Properties**.

Deleting mail users

To delete a mail user

- 1 Open the **Exchange Security** module.
- 2 Select a mail user, and select **Tools | Delete**. Alternatively, right-click a mail user, and choose **Delete**.

Managing mailboxes

- [Creating mailboxes](#)
- [Modifying mailbox settings](#)
- [Deleting mailboxes](#)

i | **NOTE:** In Exchange Server 2013, 2016, and 2019, public folders are considered public folder mailboxes and are managed by the Exchange Admin Center. You create public folder mailboxes in the **New Database** dialog box. See [Creating public folders](#).

Creating mailboxes

To create a mailbox

- 1 Open the **Exchange Security** module.
- 2 Select a mailbox group, and select **Tools | New**. Alternatively, right-click a mailbox group, and choose **New**.

i | **NOTE:** If you select **Mailboxes (All)**, the new mailbox is placed automatically in the correct alphabetical mailbox category.

- 3 Choose to create a new user or select an existing user.
- 4 Click **Next**. If you selected **Existing user**, skip ahead to step 6.
- 5 Enter the account information of the user, and click **Next**.

i | **NOTE:** Boxes marked with an asterisk (*) are required entries.

- 6 Enter the contact information of the user, and click **Next**.
- 7 Select the Exchange server and mailbox database, and click **Next**.
- 8 Review the details, and click **New**.
- 9 Click **Finish**.


Modifying mailbox settings

To modify mailbox settings

- 1 Open the **Exchange Security** module.
- 2 Select a mailbox.

- 3 Select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click the mailbox, and choose **Properties**.

- 4 Modify the settings for the mailbox.

Table 7. Mailbox settings

Setting	Description
Changing Role Assignment Policy	In the Mailbox Settings box, you can change the Role assignment policy and delivery options. You also can set a litigation hold on the mailbox.
Changing Delivery Options	<p>To change the delivery options, click Delivery Option.</p> <p>Send on behalf</p> <ul style="list-style-type: none">• To grant the Send on behalf permission, select accounts from the list.• To add an account to the list, click Add.• To remove a selected account from the list, click Remove. <p>Forwarding address</p> <p>To forward messages, select the Forward to check box, and click Search to select an account. To deliver the messages to the mail box also, select the Deliver messages to both forwarding address and mailbox check box.</p> <p>Recipients limits</p> <p>By default, recipients are limited to 10. To change the limit, type a number in the box. For unlimited recipients, clear the Maximum recipients check box.</p> <p>Email addresses</p> <p>A mailbox can have one primary email address, which is indicated by the checkmark in the Primary column.</p> <ul style="list-style-type: none">• To add an address to the list, click Add.• To set a selected address as the primary address, click Set as Reply.• To remove a selected address from the list, click Remove.
Propagating Permissions	To propagate permissions to subfolders, click Propagate client folder permissions .

Deleting mailboxes

To delete mailboxes

- 1 Open the **Exchange Security** module.
- 2 Select a mailbox or selection of mailboxes, and select **Tools | Delete**. Alternatively, right-click a mailbox or selection of mailboxes, and choose **Delete**.

Managing mailbox folders

- [Creating mailbox folders](#)
- [Managing permissions on mailbox folders for multiple users](#)

- [Deleting mailbox folders](#)

Creating mailbox folders

To create mailbox folders

- 1 Open the **Exchange Security** module.
- 2 Select a mailbox, and select **Tools | New**. Alternatively, right-click a mailbox, and choose **New**.
- 3 Type a name for the mailbox folder, and click **OK**.

Managing permissions on mailbox folders for multiple users

To manage permissions on mailbox folders for several users at one time

- 1 Open the **Exchange Security** module.
- 2 Select **Tools | Multi-User Mailbox Folder Management**. Alternatively, right-click in the Navigation or Objects Pane, and choose **Multi-User Mailbox Folder Management**.
- 3 In the **Select Mailboxes** area, click **Add**, and select the mailboxes to manage.
- 4 In the **Select Mailbox Folder** area, select the mailbox folder(s) to manage.
- 5 In the **Select Permissions** area, click **Add**.
- 6 Add or remove any users from the list.
- 7 Select the permissions to either grant, delete, or revoke.
- 8 Click **OK**.

Deleting mailbox folders

To delete mailbox folders

- 1 Open the **Exchange Security** module.
- 2 Select a mailbox folder, and select **Tools | Delete**. Alternatively, right-click a mailbox folder, and choose **Delete**.

Managing public folders

- [Creating public folders](#)
- [Modifying public folder settings](#)
- [Deleting public folders](#)

- i** **NOTE:** In Exchange Server 2013, 2016, and 2019, public folders are considered public folder mailboxes and are managed by the Exchange Admin Center. You create public folder mailboxes in the New Database dialog box. See [Creating public folders](#).
- If you are using Exchange Server 2010, you cannot delete Default empty permission from public folders.
- If Exchange Server 2013, 2016, or 2019 is installed in a child domain, you cannot manage directory permissions nor disable the mail-enabled property for public folders.

Creating public folders

To create public folders

- 1 Open the **Exchange Security** module.
- 2 Expand or select **Public Folders (All)** in the Navigation pane.
- 3 Select the parent folder, and select **Tools | New**. Alternatively, right-click the parent folder, and choose **New**.
- 4 Type the name of the new public folder.
- 5 By default, mail is enabled. To disable mail, clear the **Mail Enabled** check box.

Modifying public folder settings

You can propagate the contents of one Public Folder database to another, and set delivery options for mail-enabled Public Folders.

To modify public folder settings

- 1 Open the **Exchange Security** module.
 - 2 Select a Public Folder.
 - 3 Select **Tools | Properties**.
- OR-
- Click **i** on the Tool Bar; or right-click the public folder, and choose **Properties**.
- 4 Set options for the public folder.

Table 8. Public folder options

Option	Description
Replicating Contents	To replicate the contents of the public folder displayed in the Public Folder Path box to Public Folder databases, select the databases from the list, and click OK . <ul style="list-style-type: none">• To add a database to the list, click Add.• To remove a database from the list, click Remove.
Mail enabled	By default, public folders are mail-enabled.
Setting Delivery Options	To change the delivery options of a mail-enabled Public Folder, click Delivery Option . <p>NOTE: The Mail Enabled check box must be selected to activate Delivery Options. If you select the Mail Enabled check box, the button does not automatically activate. You must click OK, and choose Properties again.</p>

Table 8. Public folder options

Option	Description
Send on behalf	To grant the Send on behalf permission, select accounts from the list. <ul style="list-style-type: none">To add an account to the list, click Add.To remove an account from the list, click Remove.
Forwarding address	To forward messages, select the Forward to check box, and click Search to select an account. To deliver the messages to the mail box also, select the Deliver messages to both forwarding address and mailbox check box.
Propagating Client Permissions	To propagate permissions to subfolders, click Propagate client permissions .

- 5 Select the accounts whose permissions you want to propagate to all subfolders. By default, the permissions are added or replaced. To remove the permissions, select **Remove**.

Deleting public folders

To delete public folders

- 1 Open the **Exchange Security** module.
- 2 Expand or select **Public Folders (All)** in the Navigation pane.
- 3 Select a folder or selection of folders, and select **Tools | Delete**. Alternatively, right-click a folder or selection of folders, and choose **Delete**.
- 4 Click **Yes**.

Using role based access control

Role Based Access Control (RBAC) is the new permissions model introduced in Microsoft Exchange Server 2010. With Security Explorer, you can manage RBAC Roles, Role Groups, User Roles, and Custom Scopes.

Topics:

- [Managing user roles](#)
- [Managing role groups](#)
- [Managing roles](#)
- [Managing custom scopes](#)

Managing user roles

- [Adding a user role](#)
- [Modifying user roles](#)
- [Deleting user roles](#)

Adding a user role

To add a user role

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**.
- 3 Select **User Roles**, and select **Tools | New**. Alternatively, right-click **User Roles**, and choose **New**.
- 4 Type a name for the user role.
- 5 Type an optional description of the user role.
- 6 Click **Add**.
- 7 Select the roles to assign, and click **OK**.
 - To make this the default user role, select the **Is Default** check box.
 - To remove selected roles, click **Remove**.

Modifying user roles

To modify user roles

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **User Roles**.
- 3 Select a user role, and select **Tools | Properties**. Alternatively, right-click a user role, and choose **Properties**.

i | NOTE: To clear the **Is Default** check box, you must assign another user role to be the default.

Deleting user roles

To delete user roles

- 1 Open the Exchange Security module.
- 2 In the Navigation pane, expand **Role Based Access Control**, expand **User Roles**.
- 3 Select a user role, and select **Tools | Delete**. Alternatively, right-click a user role, and choose **Delete**.

Managing role groups

- [Adding role groups](#)
- [Modifying role groups](#)
- [Deleting role groups](#)

Adding role groups

To add a role group

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**.
- 3 Select **Role Groups**, and select **Tools | New**. Alternatively, right-click **Role Groups**, and choose **New**.

- 4 Type a name for the role group.
- 5 Type a description.
- 6 Select either a custom scope or an organizational unit.
- 7 To add roles and members to the group, click **Add**, and choose the roles or accounts to add. To remove selected roles or accounts, click **Remove**.
- 8 To assign managers, click **Add**, and choose the accounts to add. To remove selected managers, click **Remove**.

Modifying role groups

To modify role groups

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and select **Role Groups**.
- 3 In the Objects pane, select a Role Group, and select **Tools | Properties**. Alternatively, right-click a Role Group, and choose **Properties**.
- 4 You can change the description and write scope. You also can add or remove assigned roles, members, and managed by settings.

Deleting role groups

To delete role groups

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and select **Role Groups**.
- 3 In the Objects pane, select one or more Role Groups, and select **Tools | Delete**. Alternatively, right-click one or more Role Groups, and choose **Delete**.

Managing roles

- [Creating assignments](#)
- [Modifying assignments](#)
- [Deleting assignments](#)
- [Creating child roles](#)
- [Deleting child roles](#)
- [Adding entities](#)
- [Modifying entities](#)
- [Deleting entities](#)

Creating assignments

To create a new assignment

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Select a role.

- 4 Select **Assignments**, and select **Tools | New**. Alternatively, right-click **Assignments**, and choose **New**.

i | **NOTE:** Once you have applied a Configuration or Recipient Scope, the only way to clear the selection is to apply an Exclusive Scope of the same type.
For example, if you select to apply a CustomRecipientWriteScope, the only way to clear selection is to apply an ExclusiveConfigWriteScope.

Modifying assignments

To modify an assignment

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Select a role, and expand **Assignments**.
- 4 Select an assignment, and select **Tools | Properties**. Alternatively, right-click an assignment, and choose **Properties**.

Deleting assignments

To delete assignments

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Select a role, and expand **Assignments**.
- 4 Select one or more assignments, and select **Tools | Delete**. Alternatively, right-click one or more assignments, and choose **Delete**.

Creating child roles

To create child roles

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Expand a parent role.
- 4 Select **Child Roles**, and select **Tools | New**. Alternatively, right-click **Child Roles**, and choose **New**.

Modifying child roles

To modify a child role, you can add, modify or delete the child role's assignments and entities. You cannot directly modify the child role itself.

Deleting child roles

To delete child roles

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Expand the parent role, and expand **Child Roles**.
- 4 Select a child role, and select **Tools | Delete**. Alternatively, right-click a child role, and choose **Delete**.

Adding entities

You can add, modify, and delete entities only for child roles. Because the set of entities is constant and inherited from the parent role, the only way to add an entity to a child role is to delete the entities and add the selected entities back.

To add entities

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Expand the parent role, and expand the child role.
- 4 Right-click **Entities**, and choose **New**. Any entities that were deleted display.
- 5 Select the entities to add back to the list.

Modifying entities

To modify entities

- 1 Open the Exchange Security module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Expand the parent role, expand the child role, and expand **Entities**.
- 4 Select the entity, and select **Tools | Properties**. Alternatively, right-click the entity, and choose **Properties**.
The list of parameters is constant. You can remove parameters from the entity and add only removed parameters.

Deleting entities

To delete entities

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and expand **Roles**.
- 3 Expand the parent role, expand the child role, and expand **Entities**.
- 4 Select an entity, and select **Tools | Delete**. Alternatively, right-click an entity, and choose **Delete**.

Managing custom scopes

- [Creating a custom scope](#)
- [Editing a custom scope](#)
- [Deleting custom scopes](#)

Creating a custom scope

To create a custom scope

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**.
- 3 Select **Custom Scopes**, and select **Tools | New**.

-OR-

Right-click **Custom Scopes** or right-click in the Objects pane, and choose **New**.

- 4 Type a name for the scope.
- 5 Select a filter type. Each filter type has a corresponding example to aid in completing the Filter Value box.
- 6 To make an Exclusive Scope, select the **Exclusive** check box.

Editing a custom scope

You can change the name of the scope and the filter value.

To edit a custom scope

- 1 Open the Exchange Security module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and select **Custom Scopes**.
- 3 In the Objects pane, select a scope, and select **Tools | Properties**. Alternatively, right-click a scope, and choose **Properties**.

Deleting custom scopes

To delete a custom scope

- 1 Open the **Exchange Security** module.
- 2 In the Navigation pane, expand **Role Based Access Control**, and select **Custom Scopes**.
- 3 In the Objects pane, select one or more scopes, and select **Tools | Delete**. Alternatively, right-click one or more scopes, and choose **Delete**.

i **NOTE:** You cannot delete a scope that is used by a role assignment. If a scope is used by a role assignment, a message box displays asking if you want to delete the assignment. Click **Yes** to delete the assignment.

Setting options for Exchange security

To set options for Exchange security

- 1 Select **Tools | Options**.
- 2 Open the **Exchange** tab.
- 3 Set Exchange options.

Table 9. Exchange options

Option	Description
Use separate tabs for directory and mailbox/public-folder permissions tabs	Select to display directory, mailbox, and public folder permissions on separate tabs. By default, the permissions display on the same tab.
Show only "Active" mailboxes	By default, only Active mailboxes display. To display all mailboxes, Active and Inactive, select the check box.

Table 9. Exchange options

Option	Description
Show parent alphabetic mailbox categories	By default, the parent mailboxes are separated alphabetically into categories, such as [A-C], [D-F], and so on. To hide the category labels, clear the check box.
Show Exchange information message	The first time you expand an Exchange server in the Navigation pane of the Exchange Security module, an information message displays the minimum requirements for managing Exchange security. If you choose to hide this message, you can restore it by selecting the Show Exchange information message check box.

4 Set the default Exchange credentials.

- i NOTE:** To connect to an Exchange Server, a user must:
- Have Administrator access on the client computer
 - Have a mailbox
 - Be a Local Administrator on the computer where Exchange is installed
 - Have Exchange view-only permissions as a minimum

Table 10. Default Exchange credentials options

Option	Description
Use Windows Authentication	By default, Security Explorer uses Windows® Authentication when connecting to an Exchange server.
Always open authentication dialog	Select to display the Open Authentication dialog box when connecting to an Exchange server.
Use alternate credentials list	Select to use the alternate credentials list when connecting to an Exchange server. Security Explorer tries each account in the order they appear in the list until an account is found with sufficient privileges. If no account is found, Access Denied is displayed.

Table 11. Alternate credentials options

Button	Description
Add	<p>Add alternate credentials.</p> <ol style="list-style-type: none"> 1 Type an account name, or browse to select an account. The format is domain\account (for example, Acme\Administrator.local). Do not include the @ symbol. 2 Type the password. 3 Type a domain name (<i>optional</i>). If you do not enter a domain name, each account is tried in the order listed until an account is found with sufficient privileges. 4 Click OK.
Edit	Edit the selected alternate credential.
Del	Delete a name from the list.
Clear	Clear all names from the list.

5 Click **Specify** to select a port number to use to communicate with Exchange servers.

Table 12. Exchange server port mapping options

Button	Description
Add	Add a port number for communication with an Exchange server. You specify the domain, Exchange server, and the port number to use.
Edit	Edit a selected port mapping.
Del	Remove selected port mappings from the list.
Clear	Clear all port mappings from the list.

- 6 Select how to sort mailboxes. When you exit options, refresh the display to see the results of your selection.
- 7 Click **OK**.

Working with Microsoft SharePoint

Once you deploy the SharePoint web service, you can use the SharePoint® module to manage permissions on SharePoint objects, manage SharePoint groups, and manage SharePoint security.

Topics:

- [Using the SharePoint menu](#)
- [Adding SharePoint farms or sites](#)
- [Managing SharePoint farms or sites](#)
- [Previewing SharePoint objects](#)
- [Deploying the SharePoint web service](#)
- [Deploying the SharePoint web service manually](#)
- [Managing SharePoint permissions](#)
- [Managing SharePoint groups](#)
- [Removing accounts from SharePoint groups](#)
- [Searching for SharePoint objects](#)
- [Modifying SharePoint properties](#)
- [Backing up and restoring SharePoint security](#)
- [Exporting SharePoint permissions](#)
- [Setting SharePoint options](#)
- [Removing the SharePoint web service](#)
- [Removing the SharePoint web service manually](#)

Using the SharePoint menu

If you apply a license with SharePoint® functionality enabled, a menu is added to the menu bar.

Table 1. SharePoint menu options

Option	Description
Add SharePoint Farm or Site	Identify SharePoint farms or sites to display in the Navigation pane. See Adding SharePoint farms or sites .
View Required Web Service Version	Displays the version of the Security Explorer SharePoint Web Service required for the current version of Security Explorer.
Manage SharePoint Farms and Sites	Edit the list of SharePoint farms and sites that appear under the SharePoint node in the Navigation pane. See Managing SharePoint farms or sites .
Change credentials	Choose custom or current Windows® credentials for SharePoint Authentication.

Adding SharePoint farms or sites

Identify SharePoint® farms or sites to display in the Navigation pane.

i | **NOTE:** The **Add Farm/Site** task opens the **Add SharePoint Farm or Site** dialog box.

To add SharePoint farms or sites

- 1 Open the SharePoint module.
- 2 Select **SharePoint | Add SharePoint Farm or Site**. Alternatively, right-click in the Navigation or Objects panes, and choose **Add SharePoint Farm or Site**.
- 3 Type a name and a valid URL for the farm or site, and click **OK**.

i | **NOTE:** The first time you select the farm or site, you see a message that indicates you need to install the SharePoint Web Service. See [Deploying the SharePoint web service](#).

Managing SharePoint farms or sites

You can easily edit the list of SharePoint® farms and sites that appear under the SharePoint node in the Navigation pane. All parent Web applications for the farm and site appear in the list as well.

i | **NOTE:** The **Manage Farms/Sites and Server Search** tasks open the **Manage SharePoint Farms or Sites** dialog box.

To manage SharePoint farms or sites

- 1 Open the SharePoint module.
- 2 Select **SharePoint | Manage SharePoint Farms and Sites**. Alternatively, right-click in the Navigation or Objects panes, and choose **Manage SharePoint Farms and Sites** from the shortcut menu.


Table 2. Manage SharePoint farms and sites options


Options	Description
Editor	Display SharePoint URLs in a list, where you can add, remove, or edit the entries. Type or paste SharePoint URLs in this format: http://siteURL (name). Each URL must be on a separate line. There must be a space between the URL and the name, which must be in brackets.
Import	Import a SharePoint Sites Export (*.xml) file.
Export	Export the list of SharePoint URLs to a SharePoint Sites Export (*.xml) file.
Delete	Delete the selected SharePoint URLs from the list.
Clear	Clear the entire list of SharePoint URLs.
Add	Add the name and URL entered in the boxes.
Automatically Search for SharePoint Sites	Search for SharePoint sites on all target SharePoint servers. To narrow the search, enter a few characters of a computer name in the wildcard box. IMPORTANT: The logged-on user must be a local administrator on all of the target SharePoint servers.
Manual Web Service Deployment/Removal	Manually install or remove the SharePoint web service. See Deploying the SharePoint web service manually or Removing the SharePoint web service manually .

Previewing SharePoint objects

For SharePoint® sites/webs and lists, you can display a web browser in place of the Objects pane.

To preview SharePoint objects

- 1 Open the SharePoint Security module.
- 2 Select a SharePoint site/web or list in the Navigation pane.
- 3 Click . The Objects pane is replaced by a web browser and the SharePoint page for the selected object displays.

To hide the preview and redisplay the Objects pane, click  again.

Deploying the SharePoint web service

To access the security for a selected SharePoint® site, you must install the SharePoint Web Service. The first time you select a SharePoint server in the Navigation pane, you are prompted to install a web service.

The SharePoint Web Service Deployment Wizard guides you through installing the SharePoint Web Service on web front end servers in your farm or site.

- i** **NOTE:** To ensure the deployment succeeds, be sure that all web front end servers in the farm or site are running two required SharePoint services.
- For SharePoint 2010, SharePoint 2010 Administration and SharePoint 2010 Timer must be running.
 - For SharePoint 2013, SharePoint 2016, and SharePoint 2019, SharePoint Administration and SharePoint Timer Service must be running.

To deploy the SharePoint web service

- 1 Select a SharePoint server in the Navigation pane. If the SharePoint Web Service is not present, you see a message indicating that you should run the Deployment Wizard.

- i** **NOTE:** If you ran the SharePoint Web Service Wizard and still see the SharePoint Web Service Error message, the deployment may not be completely finished. To check on the current state of the deployment, we provide a command that you can copy. Click **More Details**, and click **Advanced**. See step four in [Deploying the SharePoint web service manually](#).

NOTE: To view more information, click **More Details**. You can view and save the error message received from SharePoint. If you prefer to install SharePoint Web Service manually, click **Manual Web Service Deployment**. See [Deploying the SharePoint web service manually](#).

- 2 Click **Deployment Wizard**.
 - To display more details, click **More Details**. See step 1.
 - To display the commands to install the SharePoint Web Service manually, click **Manual Web Service Deployment**. See [Deploying the SharePoint web service manually](#).
- 3 Click **Next**.
- 4 Choose the version of SharePoint you are using, and click **Next**. The SharePoint URL page displays the name of the selected server in the URL box.
- 5 If necessary, type the site root URL in the URL box.

- i** **NOTE:** If the SharePoint site is not using port 80, then include the port number in the URL (<http://siteroot:portnumber>). Do not include any page information in the URL.

- 6 Click **Next**.
- 7 If necessary, type a server name in the **Server name** box. Alternatively, click **Browse** and locate a server. To test communication with the server, click **Test**.

i | **NOTE:** The server name must be one of the web front end servers in your farm or site. You need to include only one server name. All other web front end servers in your farm or site currently running are included automatically in the deployment process.

- 8 Click **Next**.

For farms and sites with multiple web front end servers, it is recommended that you supply specific account credentials to run the deployment. The account must be a member of the local administrators group on the target sever and must have sufficient access rights to the SharePoint databases. Click **Advanced User Selection** to locate an account name.

For single-server SharePoint sites, leave the boxes blank to run the deployment using the local system account for the target server. The target server must contain the SharePoint database.

- 9 Click **Next**.

i | **NOTE:** To view the commands applied during deployment, click **Advanced**. See [Deploying the SharePoint web service manually](#).

- 10 Click **Finish**.

The deployment process checks the server you selected for two required SharePoint services. You are responsible for ensuring that these two services are running on the other web front end servers in your farm/site before continuing with the deployment.

- For SharePoint 2010, SharePoint 2010 Administration and SharePoint 2010 Timer must be running.
- For SharePoint 2013, SharePoint 2016, and SharePoint 2019, SharePoint Administration and SharePoint Timer Service must be running.

- 11 Click **Yes**.

- 12 Click **Close**.

Deploying the SharePoint web service manually

You can deploy the SharePoint® Web Service manually.

i | **NOTE:** If you ran the automatic removal process and it failed, when you run the manual process there may be a timer job running that will prevent the manual process from completing successfully. If this scenario occurs, you need to delete the timer job and retry the manual process. See [SharePoint web service removal fails](#).

To deploy the SharePoint web service manually

- 1 Open the SharePoint module.
- 2 Select **SharePoint | Manage SharePoint Farms and Sites**. Alternatively, right-click in the Navigation or Objects panes, and choose **Manage SharePoint Farms and Sites** from the shortcut menu.
- 3 Click **Manual Web Service Deployment/Removal**.
- 4 Click **Manual Web Service Deployment**.
- 5 Check that these two required SharePoint services are running on all of the web front end servers in your farm or site.
 - For SharePoint 2010, SharePoint 2010 Administration and SharePoint 2010 Timer must be running.

- For SharePoint 2013, SharePoint 2016, and SharePoint 2019, SharePoint Administration and SharePoint Timer Service must be running
- 6 Open the Security Explorer install folder (C:\Program Files (x86)\Quest\Security Explorer), and copy SLWebServices_1.00.0009.wsp to a new folder (SLWebServiceSetup) in the ADMIN\$ share on one of the target web front end servers in your farm or site.
 - 7 On the target web server where you copied the file in step two, open a command prompt, and execute two STSADM.exe commands: execute the addsolution command, and execute the deploysolution command.
 - i** **NOTE:** To run STSADM.exe commands, you must be logged in as a member of the local administrators group and have sufficient rights to the various SharePoint databases.
 - NOTE:** Click **Deploy Commands** to open the SharePoint Web Service Commands page where you can copy and paste the commands. Click **More Information** for a command that lists all of the SharePoint web service solutions present on your farm or site.
 - 8 To verify that the deployment succeeded, you can run one more STSADM.exe command: enumsolutions. The output of the command indicates if the web service has deployed.
 - i** **NOTE:** Click **Verify Command** to open the SharePoint Web Service Commands page where you can copy and paste the command.

Managing SharePoint permissions

- [Viewing SharePoint permissions](#)
- [Granting SharePoint permissions](#)
- [Revoking SharePoint permissions](#)
- [Cloning SharePoint permissions](#)
- [Modifying SharePoint permissions](#)
- [Modifying SharePoint permissions levels](#)
- [Repairing limited access permissions](#)
- [Removing permissions on deleted accounts](#)
- [Removing permissions on disabled accounts](#)

Viewing SharePoint permissions

- i** **NOTE:** The **View Permissions** task opens the **Browse** tab.
- NOTE:** The first time you select a SharePoint® server, you are prompted to install the SharePoint Web Services. See [Deploying the SharePoint web service](#).
- NOTE:** If the **Always open authentication dialog** check box is selected on the **SharePoint** tab of the **Options** dialog box, the **SharePoint Authentication** box appears. Enter the necessary credentials, and click **OK**. See [Setting SharePoint options](#).
- NOTE:** If the path you enter includes page information, such as default.aspx, you see a warning box. Click **Yes** to remove page information from the path.

There are three ways to select a SharePoint server. See [Using the Navigation pane](#).

- Expand **Network Neighborhood** in the Navigation pane to view a list of all sites for a selected server, including the Central Administration site.
- Type a URL in the **Path** box, and click **Set**. A new root node is created in the Navigation pane.

- Type a URL in the **Path** box, and click **Go**. The site is added automatically to the Favorites list.

i | **NOTE:** Only root SharePoint sites can be added to the Favorites list. If you want to display sub-sites, lists, or other items, use one of the other two methods.

The Objects pane displays the sites, subsites, lists, and items, such as documents, calendar items, and events, for the selected server. See [Using the Objects pane](#). Select an object to view its permissions in the Permissions pane. See [Using the Permissions pane](#).


Granting SharePoint permissions

i | **TIP:** The Grant task provides a quick way to grant permissions. See [Using the Grant task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**.

To grant SharePoint® permissions

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane, or type a path in the Path box, and click **Go**.
- 4 Select an object in the Objects pane or a permission in the Permissions pane.
- 5 Select **Security | Grant Permissions**.

-OR-

Click  on the Tool Bar; click **Grant** on the Control Button Bar; or right-click the object or permission, and choose **Grant Permissions**.

The **Grant SharePoint Permissions** dialog box displays the object, and the associated groups and users for the current object.

- 6 Select the groups and users to grant the permission. There are a variety of ways to select groups and users. See [Using the Browse tab to grant permissions](#).
- 7 Select a permission type, a permission to grant and how to apply it. To select more than one permission, select how to apply the permission, and click **Advanced Permission Selection**.
- 8 To add the group/user to the List of users and groups to grant list, click **Add**.
- 9 Click **OK**. See [Completing a process](#).

Revoking SharePoint permissions

i | **TIP:** The Revoke basic task provides a quick way to revoke permissions. See [Using the Revoke tasks](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**.

TIP: You also can use the Revoke Unknown and Revoke Disabled advanced tasks to easily revoke permissions for those specific situations.

To revoke SharePoint® permissions

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select an item in the Navigation pane, or type a path in the Path box, and click **Go**.
- 4 Select an object in the Objects pane or a permission in the Permissions pane.
- 5 Select **Security | Revoke Permissions**.

-OR-

Click  on the Tool Bar; click **Revoke** on the Control Button Bar; or right-click the object, and choose **Revoke Permissions**.


- 6 Select the groups and users to revoke the permission. There are a variety of ways to select groups and users. See [Using the Browse tab to revoke permissions](#).
- 7 Select the permissions to revoke, and whether or not to Allow or Deny. If the choice is not available in the list, click **Advanced Permission Selection** to create a custom choice.
- 8 To add the group/user to the **List of users and groups to revoke** list, click **Add**.
- 9 Select options.

Table 3. Revoke options

Option	Description
Revoke all permissions for the selected user	Select to revoke all permissions for the selected user.
Verify SharePoint accounts when adding to the list below	Select to verify the selected account when you click Add .
Advanced Revoke Options	<i>Available only for SharePoint sites.</i> If you select this check box, a warning message displays and the Revoke Folder Permissions dialog box becomes inactive, so the other users/groups and permissions you selected are not included in this action. To continue, click Yes .
Revoke all unknown and deleted accounts	<i>Active only when the Advanced Revoke Options check box is selected.</i> Select to revoke permissions on unknown or deleted accounts. The Remove Permissions for Deleted Accounts dialog box opens. See Revoking permissions on unknown accounts .
Revoke all disabled accounts	<i>Active only when the Advanced Revoke Options check box is selected.</i> Select to revoke permissions on all disabled accounts. The Remove Permissions for Disabled Accounts dialog box opens. See Revoking permissions on disabled accounts .
Include protected objects (objects with 'Inherit Permissions from Parent' disabled)	Select to revoke permissions on protected objects. If you select the Advanced Revoke Options check box, the Include protected objects check box is selected automatically.

- 10 Click **OK**. See [Completing a process](#).


Cloning SharePoint permissions

 **TIP:** The Clone task provides a quick way to clone permissions. See [Using the Clone task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**.

To clone SharePoint® permissions

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select an object in the Objects pane or a permission in the Permissions pane.
- 4 Select **Security | Clone Group or User**.


-OR-

Click  on the Tool Bar; click **Clone** on the Control Button Bar; or right-click the object, and choose **Clone Group or User**.

- 5 Select the groups or users to clone. You can select the groups and users manually or import a list of groups and users from a CSV file. The CSV file must contain a list of source and destination accounts where each pair is separated by a new line and the source and destination are separated by a comma. For example: ACME\BSmith,ACME\JAdams.

To select groups or users manually

- a In the Source Group or User area, click **Advanced User Selection** to select the domain or object from which to pull the permissions.
- b In the Destination Group or User area, click **Advanced User Selection** to select the domain or object to receive the cloned permissions.

 **IMPORTANT:** Do not select a pair of accounts where the source is the same as the destination. The permissions for the accounts are deleted in the cloning process.

- c Click **Add**.

- 6 You also can specify optional domain controllers for both the source account and the destination account. The domain controller is used to perform a SID lookup during the import operation.
- 7 Set the options for the clone process.

Table 4. Clone options

Option	Description
Clone Permissions	By default, permissions are cloned.
Clone group memberships	Select to add the destination account to the groups of which the source user is a member. If you choose this check box, a warning message displays. The destination is cloned into the same parent groups as the source. The contents of the groups selected as the source are not cloned. SharePoint groups cannot have their group memberships cloned.
Replace source permissions with destination permissions	Select to change the source permissions to match the destination permissions.
Include protected objects when cloning (objects with 'Inherit Permissions from Parent' disabled)	Select to include those objects for which the Allow inheritable permissions from parent to propagate to this object check box is unavailable. See Viewing SharePoint permissions .


- 8 Click **OK**. See [Completing a process](#).

Modifying SharePoint permissions

To modify SharePoint® permissions

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select an object in the Navigation or Objects pane.
- 4 In the Permissions pane, select a permission.
- 5 Select **Security | Modify Permissions**.

-OR-

Click  on the Tool Bar; click **Modify** on the Control Button Bar; or right-click the permission, and choose **Modify Permissions**.

- 6 From the Permissions lists, select the permission. Permissions in bold cannot be modified.

i | **NOTE:** To modify the permission levels, click **Permissions Levels**. See [Modifying SharePoint permissions levels](#).

Modifying SharePoint permissions levels

i | **NOTE:** *Applies to parent SharePoint® sites only.* The Permissions Levels advanced task opens the SharePoint Permission Levels dialog box. Add a path, and click **OK**.

To modify SharePoint permissions levels

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 In the Objects pane, select a SharePoint object,
- 4 Click **Levels**.
- 5 Select the permission levels.
 - To create a new permission level, click **New**.
 - To delete selected permission levels, click **Delete**.
 - To select all displayed check boxes, click **Select All**.
 - To clear all displayed check boxes, click **Clear All**.
- 6 Click **Apply**.

Repairing limited access permissions

SharePoint® automatically creates Limited Access permissions on a parent object when a new permission is created on a child item. For example, if you create a new Full Control permission on a subobject for AccountX, then SharePoint®, if necessary, automatically creates a Limited Access permission for AccountX on the parent object. If you delete the Full Control permission, the parent Limited Access permission is not automatically deleted. The Repair Limited Access Permissions function cleans up all orphaned Limited Access permissions that should no longer exist.

i | **NOTE:** *Applies to parent SharePoint sites only.* The Repair task opens the Repair Limited Access Permissions dialog box.

IMPORTANT: Back up your permissions before running this function. You may want to create a report that shows only the items that would change.

To repair limited access permissions


- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select a SharePoint server in the Navigation pane.
- 4 Select an item in the Objects pane, and select **Security | Repair Limited Access Permissions**.
-OR-
Click  on the Tool Bar; or right-click the item, and choose **Repair Limited Access Permissions**.
- 5 Select options.

Table 5. Report options

Option	Description
Create report (will list changed items)	Select to create a report that lists changed items. Type a file path or browse to locate a path.
Produce report only (i.e. no changes will be made)	Select to create only a report that shows what items would be changed if you ran the Repair Limited Access Permissions process.

Removing permissions on deleted accounts

If you remove an Active Directory® account, the permissions are still retained on the SharePoint® server. Use this feature to remove all permissions associated with deleted Active Directory accounts on a SharePoint site.


i **NOTE:** *Applies to parent SharePoint sites only.* The Revoke Unknown task opens the **Remove Permissions for Deleted Accounts** dialog box. Add at least one path, and click **OK**.

IMPORTANT: Back up your permissions before running this function. You may want to create a report that shows only the items that would change.

To remove permissions on deleted accounts

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select a SharePoint server in the Navigation pane.
- 4 Select an item in the Objects pane, and select **Security | Remove Permissions for Deleted Accounts**.

-OR-

Click  on the Tool Bar; or right-click the item, and choose **Remove Permissions for Deleted Accounts**.

- 5 Select options.

Table 6. Remove permissions options

Option	Description
Remove deleted accounts from SharePoint groups	Select to remove permissions for deleted accounts on the selected SharePoint site.
Create report (will list changed items)	Select to create a report that lists changed items. Type a file path or browse to locate a path.
Produce report only (i.e. no changes will be made)	Select to create only a report that shows what items would be changed if you ran the Remove Permissions for Deleted Accounts process.

Removing permissions on disabled accounts

Removes all permissions associated with disabled Active Directory® accounts on a SharePoint® site.

i **NOTE:** *Applies to parent SharePoint sites only.* The Revoke Disabled task opens the Remove Permissions for Disabled Accounts dialog box. Add at least one path, and click **OK**.

IMPORTANT: Back up your permissions before running this function. You may want to create a report that shows the items that would change.

To remove permissions on disabled accounts

- 1 Open the SharePoint Security module, and open the **Browse** tab.
- 2 Select a SharePoint server in the Navigation pane.
- 3 Select an item in the Objects pane, and select **Security | Remove Permissions for Disabled Accounts**.

-OR-

Right-click the item, and choose **Remove Permissions for Disabled Accounts**.

- 4 Select options.

i | **NOTE:** If you came to the Remove Permissions For Disabled Accounts dialog box from the Revoke SharePoint Permissions dialog box, the Include protected objects (objects with 'Inherit Permissions from Parent' disabled) check box is selected automatically (see [Revoking SharePoint permissions](#)).

Table 7. Remove permissions options

Option	Description
Remove disabled accounts from SharePoint groups	Select to remove permissions for disabled accounts from SharePoint groups.
Remove disabled accounts from AD groups (except primary groups)	Select to remove permissions for disabled accounts that were added to SharePoint from their Active Directory groups, except primary groups. NOTE: The currently logged on user must have the Read Members and Write Members permissions applied to the Descendant Group on the target domains.
Create report (will list changed items)	Select to create a report that lists changed items. Type a file path or browse to locate a path. NOTE: If you select the Create Report check box, only the parent container is examined and appears on the report because the child objects are included in the revoke process automatically.
Produce report only (i.e. no changes will be made)	Select to create only a report that shows what items would be changed if you ran the Remove Permissions for Disabled Accounts process. NOTE: If you select the Produce report only check box, all objects appear on the report.

Managing SharePoint groups

You can manage group membership for SharePoint® groups, including the Site Collection Administrators group for each site collection.

i | **NOTE:** Applies to parent SharePoint sites only. The SharePoint Groups advanced task opens the **SharePoint Groups** dialog box. Add a path, and click **OK**.

To manage SharePoint groups

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select a group in the Permissions pane.
- 4 Click **Groups**.

You also can select a group from the drop-down list, or browse to locate a SharePoint group.

- 5 Modify the group.

Table 8. Modify SharePoint group options

Button	Description
New Group	Create a new SharePoint group.
Delete Group	Delete the displayed SharePoint group.
New Member	Add a new member to the displayed SharePoint group.
Delete Member	Delete a member from the displayed SharePoint group.
Export	Generate a report that you can print, save, or export.
Show AD Group Contents	Look up the Active Directory® account for the selected member.

Removing accounts from SharePoint groups

Removes accounts from SharePoint® groups on a SharePoint site.

i | **NOTE:** Applies to parent SharePoint sites only. The Remove Members Advanced task opens the **Remove Accounts from SharePoint Groups** dialog box.

To remove accounts from SharePoint groups


- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select a SharePoint server in the Navigation pane.
- 4 Select an item in the Objects pane, and select **Security | Remove Accounts from SharePoint Groups**.
–OR–
Right-click the item, and choose Remove Accounts from SharePoint Groups.
- 5 Click **Add** to add SharePoint sites and Web Applications.
- 6 Click **Add** to add accounts.
- 7 Click **Remove Accounts** to remove the listed accounts from the listed SharePoint sites and Web Applications.

Searching for SharePoint objects

i | **TIP:** The Search basic task provides a quick way to search for permissions. You also can use the Find Unknown and Find Disabled advanced tasks to easily search for those specific situations. See [Using the Search tasks](#).

To search for SharePoint® objects

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 Select an object in the Navigation or Objects pane.
- 4 Select **Search | Search in a New Window (Empty)**.
–OR–

Click  on the Tool Bar; or right-click an object, and choose **Search in a New Window**.

- 5 The object you select is added as a Search Scope so you can just set the criteria for the search. See [Setting SharePoint security search criteria](#).
- 6 If you open the Search tab in the Navigation pane without selecting an object, you need to add a Search Scope before you set criteria. See [Adding a search scope](#).
- 7 Click **Start Search**.

Setting SharePoint security search criteria

Each module has a set of search criteria grouped into tabs. As you set criteria, you can update the results by clicking **Start Search** at any time. To return to the default selections on all tabs, click **Defaults**.

- [Group and user search criteria](#)
- [Permission search criteria](#)
- [SharePoint Search Criteria](#)

Group and user search criteria

Table 9. Group and user search criteria

Option	Description
Group/User	Type a group or user name, or browse for a group or user, or click Advanced User Selection .
Include Active Directory group memberships	Select to include Active Directory® group memberships in the search.
Include SharePoint group memberships	Select to include SharePoint® group memberships in the search.
Include all nested Active Directory groups	Select to include all nested Active Directory groups in the search. <i>Active only when the Include Active Directory group memberships check box and/or the Include SharePoint group memberships check box is selected.</i>
Reset Active Directory Group Member Cache	Click to clear the Active Directory group member cache. <i>Active only when the Include Active Directory group memberships check box and/or the Include SharePoint group memberships check box is selected.</i>
Include group results	By default, groups are included in the results. To show only users, clear the check box.
Include user results	By default, users are included in the results. To show only groups, clear the check box.
Search for unknown accounts	Select to include accounts that no longer exist in Active Directory in the results.
Search for disabled accounts	Select to include accounts that are disabled in Active Directory in the results.

Permission search criteria

Table 10. Permission search criteria

Option	Description
Permission Level	Choose what permissions to search. If you chose Custom , type the name of the custom permission in the Custom Search Level box.
Inherited Permissions	By default, inherited permissions are included in the search results. Inherited permissions are indicated by (I) in the Type column. To exclude inherited permissions, clear the check box.
Explicit Permissions	By default, explicit permissions are included in the search results. To exclude explicit permissions, clear the check box.
Search for exact permissions (as set above)	By default, only exact permissions as set by the Permission Level are included in the results. You can choose to include exact permissions or better, but this option is not available for the Custom permission level.
Search for exact permissions or better (not available for custom permission levels)	

SharePoint Search Criteria

By default, a search includes site, list, and item permissions for all contents.

Table 11. SharePoint search criteria


Option	Description
Search for site permissions	By default, site permissions are included in the search. To remove site permissions from the search, clear the check box.
Search for list permissions	By default, list permissions are included in the search. To remove list permissions from the search, clear the check box.
Search for item permissions	By default, item permissions are included in the search. To remove item permissions from the search, clear the check box.
Recurse all contents	By default, all contents are included in the search results.
Recurse to Depth	Select to include contents to the depth specified in the box. The default depth is 1, which is one level below the selected object.

Modifying SharePoint properties

To modify SharePoint® properties

- 1 Open the **SharePoint Security** module.
- 2 Select a SharePoint server in the Navigation pane.
- 3 Select an item in the Objects pane, and select **Tools | Properties**.

-OR-

Click  on the Tool Bar; or right-click the item, and choose **Properties** from the shortcut menu.

Backing up and restoring SharePoint security

Table 12. Backup and restore SharePoint® security

Task	Description
Backup	See Backing up security .
Restore	See Restoring security .
Scheduled Backups	See Scheduling a backup .

Exporting SharePoint permissions


You can generate a report or export permissions to a delimited file for use with Microsoft® Excel®. By default, permissions are exported to a report, which you can save, print, or export.

TIP: The Export task provides a quick way to export permissions to a report that you can save, print, or export. See [Using the Export task](#). For more options, click **Switch to Security Explorer Classic (Advanced)**.

To export SharePoint® permissions

- 1 Open the **SharePoint Security** module.
- 2 Open the **Browse** tab.
- 3 In the Navigation or Objects pane, select one or more items.
- 4 Select **Security | Export**.

-OR-

Click  on the Tool Bar; or right-click an item in the Navigation pane or anywhere in the Objects pane, and choose **Export**.

- 5 Select output options.

Table 13. Output options


Option	Description
Generate Report	By default, permissions are exported to a report, which you can save, print, or export.
Save to Microsoft Excel® Spreadsheet	SharePoint information can be saved only to a delimited file for use with Microsoft Excel. Select either Comma-delimited file (.CSV) or Tab-delimited file (.TXT) . Browse to locate a destination for the file.
Export explicit permissions only	Select to include only explicit permissions in the export file. Because the majority of permissions on SharePoint items are inherited from the site level, exporting only explicit permissions produces a list of items where the standard inheritance is broken on the site, which highlights potential security weaknesses.

- 6 To schedule an export task:
 - a Select **Create a scheduled export task**.
 - b Type a job name.
 - c Click **Schedule**.
 - d Browse to locate an account with the appropriate permissions.

- e Click **Schedule**.
- 7 Click **OK**.

Deleting export tasks

To delete export tasks

- 1 Open the **SharePoint Security** module.
- 2 Select **Security | Export Scheduler**.
- OR–
- Click  on the Tool Bar.
- 3 Select one or more tasks, and click **Delete**.

Setting SharePoint options

To set SharePoint® options

- 1 Select **Tools | Options**.
- 2 Open the **SharePoint** tab.
- 3 Set SharePoint options.

Table 14. SharePoint options

Option	Description
Download SharePoint Icons when Browsing and Searching	By default, icons representing each SharePoint object display next to each item. These icons are downloaded automatically from the SharePoint site. To remove the icons and use simpler default icons, clear the check box.
Show web applications (when browsing to a server only)	By default, web applications display when browsing through the web server and all site collections within web applications.
Show progress information when searching	By default, the name of the objects being searched do not display in the progress bar, which is the fastest way to load objects. Select to display the name of the object currently being loaded in the progress bar.
Use Security Explorer Web Service to extract sites, lists, and items	By default, the Security Explorer SharePoint Web Service extracts sites/webs, lists and items, and, optionally, to save time, can include permissions for each item returned when backing up, exporting, and searching. To turn off this feature, clear the check box.
Suppress authentication dialogs when searching and backing up	By default, authentication dialogs do not display when searching or backing up. If you want the dialogs to display, clear the check box.

- 4 Set the default SharePoint credentials.

Table 15. SharePoint credentials options

Option	Description
Use Windows Authentication	By default, Security Explorer uses Windows® Authentication when connecting to a SharePoint server.
Always open authentication dialog	Select to display the open authentication dialog box when connecting to a SharePoint server.
Use alternate credentials list	Select to use the alternate credentials list when connecting to a SharePoint server. Security Explorer tries each account in the order they appear in the list until an account is found with sufficient privileges. If no account is found, Access Denied is displayed.

Table 16. SharePoint alternate credentials options

Button	Description
Add	Add an alternate credential. <ol style="list-style-type: none">1 Type an account name (domain\account), or browse to select an account.2 Type the password.3 Type a type a base URL (optional). If you do not enter a base URL, each account is tried in the order listed until an account is found with sufficient privileges.4 Click OK.
Edit	Edit a selected alternate credential.
Del	Delete a name from the list.
Clear	Clear all names from the list.

Removing the SharePoint web service

To remove the SharePoint® web service

- 1 Right-click the SharePoint server in the Navigation pane, and choose Remove Security Explorer Web Service.
- 2 To start the SharePoint Web Service Removal Wizard, click **Yes**.
To display the commands to remove the SharePoint Web Service manually, click **Manual Web Service Removal**.
- 3 Click **Next**.
- 4 Choose the version of SharePoint, and click **Next**.
- 5 If necessary, type a server name in the Server name box. Alternatively, click **Browse** and locate a server. To test communication with the server, click **Test**.

i **NOTE:** The server name must be one of the web front end servers in your farm or site. You need to include only one server name. All other web front end servers in your farm or site currently running are included automatically in the removal process.

- 6 Click **Next**.

For farms and sites with multiple web front end servers, it is recommended that you supply specific account credentials to run the removal. The account must be a member of the local administrators group on the target sever and must have sufficient access rights to the SharePoint databases. Click **Advanced User Selection** to locate an account name.

For single-server SharePoint sites, leave the boxes blank to run the removal using the local system account for the target server. The target server must contain the SharePoint database.

- 7 Click **Next**.

i | **NOTE:** To view the commands applied during removal, click **Advanced**. See [Removing the SharePoint web service manually](#).

- 8 Click **Finish**. A message displays.

The removal process checks the server for two services that must be running for the process to work.

- For SharePoint 2010 the process requires SharePoint 2010 Administration and SharePoint 2010 Timer.
- For SharePoint 2013, SharePoint 2016, and SharePoint 2019, SharePoint Administration and SharePoint Timer Service must be running.

You are responsible for ensuring that these services are running on the other web front end servers in your farm/site before continuing with the removal.

- 9 Click **Yes**.

- 10 Click **Close**.

i | **NOTE:** If the automatic process fails to remove the Web Service, run the manual process. See [Removing the SharePoint web service manually](#).

Removing the SharePoint web service manually

i | **IMPORTANT:** If you ran the automatic removal process and it failed, when you run the manual process there may be a timer job running that will prevent the manual process from completing successfully. If this scenario occurs, you need to delete the timer job and retry the manual process. See [SharePoint web service removal fails](#).

To remove the SharePoint® web service manually

- 1 From the **Manage SharePoint Farms and Sites** box (see [Managing SharePoint farms or sites](#)), click **Manual Web Service Deployment/Removal**, and click **Manual Web Service Removal**.
- 2 Check that the two required SharePoint services are running on all of the web front end servers in your farm or site.
 - For SharePoint 2010, SharePoint 2010 Administration and SharePoint 2010 Timer must be running.
 - For SharePoint 2013, SharePoint 2016, and SharePoint 2019, SharePoint Administration and SharePoint Timer Service must be running
- 3 On the target web server where you copied the file in step two, open a command prompt, and execute two STSADM.exe commands: execute the retractsolution command, and execute the deletesolution command.

i | **NOTE:** To run STSADM.exe commands, you must be logged in as a member of the local administrators group and must have sufficient rights to the various SharePoint databases.

NOTE: Click **Removal Commands** to open the SharePoint Web Service Commands page where you can copy and paste the commands. Be sure to select the correct version of SharePoint.

NOTE: Click **More Information** for a command that lists all of the SharePoint web service solutions present on your farm or site. See step three.

- 4 To verify that the removal process succeeded, you can run one more STSADM.exe command: enumsolutions. The output of the command indicates if the web service has been removed.

i | **NOTE:** Click **Verify Command** to open the SharePoint Web Service Commands page where you can copy and paste the command.

Working with Access Explorer

To ensure network resources are secured in a manner that meets your business needs, you must be able to easily identify who has access to those resources and manage that access appropriately. With Access Explorer, you can quickly see who has access to specific resources (files, folders, and shares) and the explicit permissions associated with those resources. At any point in the exploration of an account, you can run reports on the available information.

i **NOTE:** The User Centric Security Management features provided by Security Explorer® appear as an Access Explorer node in the navigation tree on the **Browse** tab if the Access Explorer feature is installed and the license is enabled for Access Explorer. If installed, the Access Explorer menu options are present regardless of whether the license is enabled for Access Explorer.

Topics:

- [Access Explorer components](#)
- [Setting up Access Explorer](#)
- [Updating Access Explorer configuration](#)
- [Collecting Access Explorer data](#)
- [Viewing Access Explorer objects](#)
- [Searching Access Explorer servers](#)
- [Using the Access Explorer permission wizard](#)
- [Setting options for Access Explorer](#)

Access Explorer components

This section defines all of the components that comprise an Access Explorer deployment.

- [Managed domain](#)
- [Registered forest](#)
- [Managed computer](#)
- [Access Explorer agent](#)
- [Scopes](#)
- [Database](#)
- [Service accounts](#)

Managed domain

To ensure that the Access Explorer service can install agents successfully, the Security Explorer® server needs domain user credentials with sufficient access. Access Explorer uses the concept of a managed domain, which is an association of service accounts (user credentials) to Active Directory® domains. When a new service account is

added in the configuration, it is automatically granted the required Log On as a Service local user right on the Security Explorer server. This managed domain service account is used to install the agents. Local agents run as Local System and remote agents run as the service account specified during their installation.

i | NOTE: Only domains that have a trust relationship with the Access Explorer service domain can be managed.

Once a domain is managed, the application creates a Service Connection Point (SCP) in the domain that provides server location information so that all agents and clients know where to connect.

For more information, see [Adding managed domains](#).

Registered forest

To register a forest, add the forest to Access Explorer. See [Adding forests](#). When you add a forest, you must provide a service account with sufficient permissions to perform all Access Explorer configuration tasks. If the application needs to resolve a SID or expand group membership from that forest, it will use the associated service account.

When you add a managed domain and the associated Active Directory® forest is not yet registered, the Security Explorer Server will automatically add the forest and use the domain service account credentials as the forest credentials.

For more information, see:

- [Adding forests](#)
- [Adding service accounts](#)

Managed computer

A managed computer is any network object that can host resources such as files, folders, and shares. Currently supported resources include Windows® computers, Windows® clusters, and certain network attached storage (NAS) devices. When the user adds a managed computer, Configuration Manager deploys an Access Explorer agent to scan that computer. The agent may be installed on the computer (local agent) or it may be installed on another computer (remote agent). Detailed access information is maintained on the agent computer, only sending general access information to the server.

i | NOTE: When adding a remote agent, ensure a trust exists between the agent computer and the resource domains.

For more information, see:

- [Setting up a managed computer](#)
- [Managing managed computers](#)
- [Modifying managed computer properties](#)

Access Explorer agent

When a managed computer is added, an agent is assigned to that computer. The agent may reside on the computer or it may be a remote agent that resides elsewhere. The primary focus of the agent is to index all the explicit permissions throughout its assigned scopes. The agent installs a service that allows it to perform all of the necessary functions and to report data to Security Explorer.

The indexing of only explicit permissions is done for the following reasons:

- Indexing every permission would overwhelm the indexing system.
- Indexing every permission would overwhelm the user with information that could not be reported easily.

A managed computer may be scanned by either a local agent or one or more remote agents. Only one local agent can be installed on a managed computer and a managed computer with a local agent cannot be scanned by remote agents.

A local agent does an immediate scan as soon as it is added. Remote agents only scan according to a schedule, but if you want the agent to scan as soon as it is added you can enable the **Immediately scan on agent restart or scope change** option. This option is cleared by default.

For more information, see:

- [Managing Access Explorer agents](#)
- [Adding an agent to a remotely-managed computer](#)
- [Restarting an agent](#)

Scopes

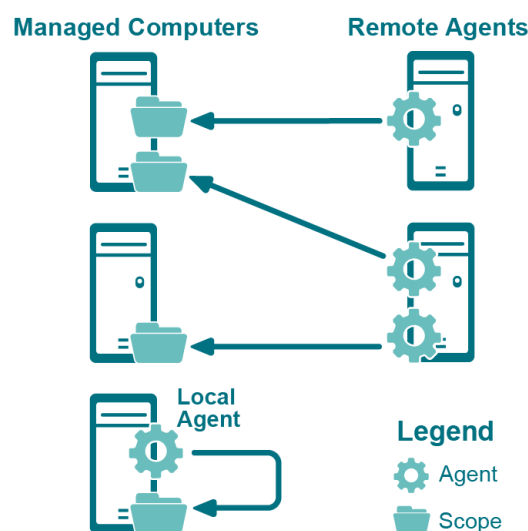
Scopes define the file system targets of the scan on the managed computer. The scopes available for scanning differ for local and remote agents.

- Local agents scan all local fixed volumes on their host computer.
- Remote agents may scan all shares available to agents as well as any user-created shares. The scopes scanned by a remote agent are chosen during the configuration of a new remote agent service. The scanned roots may also be changed through the
- **Scopes** tab of the Agent Properties.

More than one remote agent may be configured to scan a managed computer provided each agent scans different scopes. A given scope can be scanned by only one agent.

[Figure 1](#) depicts the possible deployment scenarios for Access Explorer agents and managed computers in remote and local installations.

Figure 1. Possible Access Explorer deployment scenarios



For more information, see:

- [Installing the Access Explorer agent remotely](#)
- [Modifying the scope of a scan](#)

Database

The Security Explorer server stores all data gathered in a SQL Server® database, including indexed data received from the agents. See [Setting up the Access Explorer database](#).

Service accounts

A service account is a set of credentials provided by the user and is used to perform certain deployment and query operations.

Managed domains service account

When you place a domain under management, you must provide a service account for the domain. The service account ensures computers from that domain can be added as managed computers. Each managed domain can only have one associated service account at any time, but the same service account can be used for multiple managed domains.

When a new service account is added in the configuration, it is automatically granted the required Log On as a Service local user right on the Quest Security Explorer Server.

Managed computer service account

When you deploy a remote agent to a managed computer, the agent requires a set of credentials to read information from the remote target computer. The credentials provided are referred to as the managed computer service account and are used only to read information from the remotely targeted computer.

NOTE: Local agents run as Local System.

Account usage

Various operations within Access Explorer use different credentials. The following table details when various accounts are being used.

Table 1. Account Usage in Access Explorer

Actions	Managed domain service account	Forest service account	Managed computer service account
Agent deployment and removal ¹	Yes		
Restart agent	Yes		
Take domain under management	Yes		
Register a forest and enumerate		Yes	
Read information from targets			Yes ¹

¹ The managed domain service account is used to install, upgrade, or remove the agent on the target computer. In the case where the agent is deployed locally, the agent will run as Local System. In the case where an agent is deployed remotely, the managed computer service account is used to read information from the remote computer.

Security of the service accounts

Service account credentials are maintained in the database in a secure encrypted form. In the event that someone gains access to the database, they would not be able to decrypt any of the credentials provided.

Access Explorer uses the FIPS 140-2 compliant encryption to protect the service account credentials.

For more information see:

- [Adding service accounts](#)

- [Editing service accounts](#)
- [Changing the service account](#)

Setting up Access Explorer

The initial configuration of Access Explorer involves a one-time setup of the Access Explorer database and the first managed domain.

Topics:

- [Setting up the Access Explorer database](#)
- [Setting up the first managed domain \(includes the service account\)](#)

Setting up the Access Explorer database

The Access Explorer service scans and indexes security access information on files, folders, and shares on managed computers in managed domains. The data is stored in the Access Explorer database.

To set up the Access Explorer database

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 On the **Configuration** tab, below **set up database**, click **set up now**.
- 4 Enter the target SQL Server® instance.
- 5 Enter a name for your database.
The default database name is dbAccessExplorer.
- 6 Enter database access credentials.

i | **NOTE:** These credentials must have the right to create databases on the target SQL Server® instance. They are subsequently used to access the database to store permission information collected from managed computers.

- 7 Click **OK**.

Once the Access Explorer database setup is complete, the database icon is displayed with a green check mark to show that it is configured.

Setting up the first managed domain (includes the service account)

Before you can start managing computers, you must first add a domain in which those computers reside. This domain must be associated with a service account with credentials that can perform operations on those computers.

i | **NOTE:** Only domains that have a trust relationship with the Access Explorer service domain can be managed.

To set up the first managed domain

- 1 Select **Tools | Access Explorer Configuration**.

- 2 Click **Configure Access Explorer**.
- 3 On the **Configuration** tab, below **set up managed domain**, click **set up now**.
- 4 Enter a managed domain DNS name.
- 5 Enter the service account credentials.

The service account must have administrative access to the specified domain.

- 6 Click **OK**.

Once the Access Explorer managed domain setup is complete, the domain icon is displayed with a green check mark to show that it is configured.

An option to **Click for more configuration options** is displayed. Selecting this option closes the one-time setup screen permanently and opens **Tools | Access Explorer Configuration | Configure Access Explorer | Configuration** tab. See [Updating Access Explorer configuration](#).

Updating Access Explorer configuration

Once the database and the first managed domain and service accounts are added, you can continue to add or edit additional managed domains, forests, and service accounts.

Topics:

- [Adding managed domains](#)
- [Adding forests](#)
- [Editing managed domains or forests](#)
- [Adding service accounts](#)
- [Editing service accounts](#)
- [Deleting service accounts](#)

Adding managed domains

Once you have set up the Access Explorer database and your first managed domain, you may add more managed domains.

To add managed domains

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Configuration** tab, if necessary.
- 4 Click **Configure managed domains for Access Explorer**.
- 5 Click **Add Domain**.
- 6 Enter the domain name.
- 7 Enter the service account.
 - OR -
 - Click **New** to create a service account. See [Adding service accounts](#).
- 8 Click **OK**.

Adding forests

Once you have set up the Access Explorer database and your first managed domain, you may add forests.

To add forests

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Configuration** tab, if necessary.
- 4 Click **Configure managed domains for Access Explorer**.
- 5 Click **Add Forest**.
- 6 Enter the DNS name.
- 7 Enter the service account.

- OR -

Click **New** to create a service account. See [Adding service accounts](#).

NOTE: The service account must have sufficient access required to query group membership within the forest.

The service account set on the forest will be used as the default service account on any managed domain within that forest.

- 8 Click **OK**.

Editing managed domains or forests

Once you have set up the Access Explorer database and your first managed domain, you can change the service accounts on domains or forests.

To edit domains or forests

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Configuration** tab, if necessary.
- 4 Click **Configure managed domains for Access Explorer**.
- 5 Select the domain or forest to edit.
- 6 Click **Edit**.
- 7 Enter the service account.

- OR -

Click **New** to create a service account. See [Adding service accounts](#).

- 8 Click **OK**.

Adding service accounts

Service accounts are sets of credentials used to manage computers in Access Explorer. The service accounts must be configured to access an existing Active Directory® account with sufficient rights to log onto the server.

Once you have set up the Access Explorer database and your first managed domain, you may add service accounts.

To add service accounts

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Configuration** tab, if necessary.
- 4 Click **Configure service accounts for Access Explorer**.
- 5 Click **Add**.
- 6 Enter the account name (domain\username).
- 7 Enter matching passwords.
- 8 Click **OK**.

The first service account you add is set as the default account for accessing any domains that cannot be reached through the current configuration.

To change the default service account, see [Editing service accounts](#).

To delete a service account, see [Deleting service accounts](#).

i | NOTE: When a new service account is added, it is automatically granted the required Log On as a Service local user right.

Editing service accounts

You can change the password on a service account and reassign the default account. A green check mark displays next to the service account that is used as the default account to access any domains that cannot be reached through the current configuration. See [Adding service accounts](#) and [Deleting service accounts](#).

To edit service accounts

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Configuration** tab, if necessary.
- 4 Click **Configure service accounts for Access Explorer**.
- 5 Select a service account to edit.
- 6 Click **Edit**.
- 7 Enter a new password.
- 8 Select or clear the default service account option.
- 9 Click **OK**.

Deleting service accounts

Once you have set up the Access Explorer database and your first managed domain, you may delete service accounts.

To delete service accounts

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Configuration** tab, if necessary.
- 4 Click **Add new Service Accounts**.

- 5 Select the service account to delete.
- 6 Click **Delete**.
- 7 Click **OK** to confirm deletion of the service account.
- 8 Click **Refresh** to update the display.

Collecting Access Explorer data

The Access Explorer agents collect data on only the computers you choose to manage. You can choose which folders the Access Explorer agent scans on the managed computer and you can set the schedule when the scan occurs.

i **IMPORTANT:** It is very important that the service account you choose to use for the Access Explorer agent is one that has the permissions to install the agent and the service on the selected server. Only a member of the Administrator group on the selected server has the necessary permissions to install the agent and the service.

Topics:

- [Setting up a managed computer](#)
- [Installing the Access Explorer agent locally](#)
- [Installing the Access Explorer agent remotely](#)
- [Managing managed computers](#)
- [Modifying managed computer properties](#)
- [Managing Access Explorer agents](#)

Setting up a managed computer

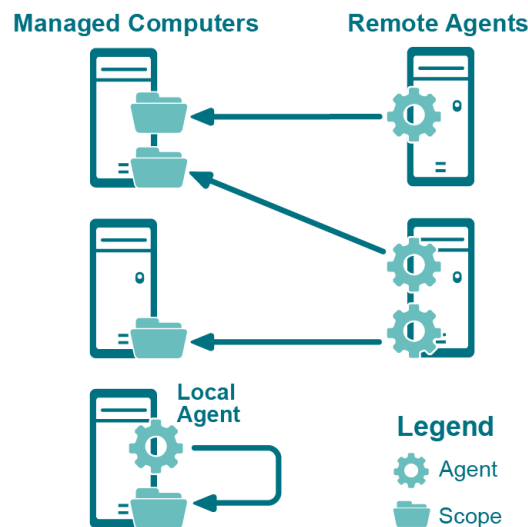
A managed computer is one that is scanned by the Access Explorer agent for security data. When you add a managed computer, you have the option of installing a local agent on the same computer or configuring a remote agent installed on another computer. If you install a locally managed computer, you can automatically install the agent with the computer, or install the agent manually later.

i **NOTE:** Only computers in domains that are managed can be added as managed computers. To add a domain, other than the domain specified during installation, see [Adding managed domains](#).
If you choose to add a remote agent to a managed computer, the first remote agent must be configured during the deployment of the managed computer. You can add more remote agents later, if needed.

TIP: More than one remote agent may be used to scan a managed computer. This is useful if the managed computer has a large set of data roots. Multiple agents may not scan the same data root.

[Figure 2](#) depicts the possible deployment scenarios for Access Explorer agents and managed computers in remote and local installations.

Figure 2. Possible Access Explorer deployment scenarios



A locally managed computer is one on which the Access Explorer agent is installed and scanning security data on the same server. Local installation is available only for Windows® Servers. With a local installation, you also can choose automatic or manual installation. See [Installing the Access Explorer agent locally](#).

A remotely managed computer is one that has its security data scanned and collected by Access Explorer agents running on different servers. Other than Windows® Servers, all other server types require remote installation. There is no option to install the agent manually. See [Installing the Access Explorer agent remotely](#).

Installing the Access Explorer agent locally

Currently, the only type of server on which you can install the Access Explorer agent locally is Windows® Server.

To install the Access Explorer agent locally

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Manage Computers** tab.
- 4 Click **New Managed Computer**, and choose **Windows Server**.
- 5 Choose **Locally Managed**, and click **Next**.
- 6 Choose **Automatic installation (recommended)**, and click **Next**.

i **NOTE:** If you choose manual installation, the managed computer is added to the list but the Access Explorer service is not installed. The status of the computer remains at **Waiting for agent first connection** until the service is installed.

To install the Access Explorer service, run the agent installer located in the Security Explorer installation folder (**Program Files\Quest\Security Explorer\Access Explorer\Agent Management\Agent**).

- 7 Choose the domain that contains the computers you want to manage.

If the domain is not listed, you need to add it as a managed domain. For more information, see [Adding managed domains](#).

If the list of computers is long, you can type in the blank row at the top to sort the list.

i **NOTE:** To quickly add computers to the list, click **Import** to import a .txt file that contains the fully qualified domain names listed one per line or in a string separated by commas.

- 8 Select the computers you want to manage and click **Add**.

To remove a selected computer from the list, click **Remove**.

- 9 Click **Finish**.

The agent will now be installed on the selected computers.

As the agent is installed, the status changes to reflect the progress of the installation. When the Status column is OK the agent is installed. When the initial scan is complete, the Data State column displays Data Available.

By default, the Access Explorer agent scans the entire root drive of the managed computer. To select specific folders to scan, see [Modifying the scope of a scan](#).

Installing the Access Explorer agent remotely

Install the Access Explorer agent remotely when you cannot install the agent on the computer you want to manage. You can install the agent on more than one remote server, so you can have several different servers collecting security information on the same computer.

i **NOTE:** You can install the Access Explorer agent remotely on only one managed computer at a time. You can, however, install the agent on multiple remote servers to scan a single managed computer. See [Adding an agent to a remotely-managed computer](#).

Remote installation of the Access Explorer Agent is available for:

- [Windows Servers](#)
- [NAS Servers](#)
- [Clusters](#)

Windows Servers

To install the Access Explorer agent remotely for a Windows® Server

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Click **New Managed Computer** and choose **Windows Server**.
- 3 Choose **Remotely Managed** and click **Next**.
- 4 Choose the domain that contains the computers you want to manage.
- 5 Select the computer to manage and click **Next**.

If the list of computers is long, you can type in the blank row at the top to filter the list.

You cannot select multiple computers to manage. You must install the agent on one computer at a time.

- 6 Select the root folders for the Access Explorer service to scan for data and click **Next**.

Only the root folder is marked as selected, but all folders and files beneath the root are included in the selection.

- 7 Click **Browse** to select a server (Agent Computer) on which to install the Access Explorer agent.
- 8 Select a service account that has the necessary permissions to install the Access Explorer agent on the designated Agent Computer.
- 9 Create a schedule for when the Access Explorer agent scans the managed computer for data.

i **NOTE:** When selecting to **Run On An Interval**, it is possible to choose a frequency such that the agent is still busy completing the last scan when the next scan should start. In this case, the scan that could not start on time will be skipped and the next scan will be started as normal.

- 10 For remote agents, you must enable the **Immediately scan on agent restart or scope change** option if you want the agent to scan immediately when it is added. This option is cleared by default.
- 11 Click **Finish**.

As the agent is installed, the status changes to reflect the progress of the installation. When the **Status** column is **OK** the agent is installed. When the initial scan is complete, the **Data State** column displays **Data Available**.

NAS Servers

To install the Access Explorer agent remotely for a NAS Server

- 1 Select **Access Explorer Management | Manage Computers**.
- 2 Click **New Managed Computer**, and choose **NAS Server**.
- 3 Choose the domain that contains the computers you want to manage.
- 4 Select the computer to manage and click **Next**.

If the list of computers is long, you can type in the blank row at the top to filter the list.

i | **NOTE:** You cannot select multiple computers to manage. You must install the agent service on one computer at a time.

- 5 Select the root folders for the Access Explorer agent to scan for data and click **Next**.
Only the root folder is marked as selected, but all folders and files beneath the root are included in the selection.
- 6 Click **Browse** to select a server (Agent Computer) on which to install the Access Explorer agent.
- 7 Select a service account that has the necessary permissions to install the Access Explorer agent on the designated Agent Computer.
- 8 Create a schedule for when the Access Explorer agent scans the managed computer for data.

i | **NOTE:** When selecting to **Run On An Interval**, it is possible to choose a frequency such that the agent is still busy completing the last scan when the next scan should start. In this case, the scan that could not start on time will be skipped and the next scan will be started as normal.

For remote agents, you must enable the **Immediately scan on agent restart or scope change** option if you want the agent service to scan immediately when it is added. This option is cleared by default.

- 9 Click **Finish**.

As the agent is installed, the status changes to reflect the progress of the installation. When the **Status** column is **OK** the agent is installed. When the initial scan is complete, the **Data State** column displays **Data Available**.

Clusters

To install the Access Explorer agent remotely for a cluster

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Manage Computers** tab.
- 4 Click **New Managed Computer**, and select **Cluster**.
- 5 Select the domain containing the cluster from the list.

Once the domain has been selected, the wizard numerates the clusters available in the domain.

i | **NOTE:** If the selected cluster name is not correct, click Edit Cluster Name to assign the correct name for the rest of the process.

- 6 Select the cluster to be added to the managed domain and click Next.

The managed cluster has been added to the domain.

- 7 Select the root folders for the Access Explorer agent to scan for data and click **Next**.

Only the root folder is marked as selected, but all folders and files beneath the root are included in the selection.

- 8 Click **Browse** to select a server (Agent Computer) on which to install the Access Explorer agent.
- 9 Select a service account that has the necessary permissions to install the Access Explorer agent on the designated Agent Computer.
- 10 Create a schedule for when the Access Explorer agent scans the managed computer for data.

i | **NOTE:** When selecting to **Run On An Interval**, it is possible to choose a frequency such that the agent is still busy completing the last scan when the next scan should start. In this case, the scan that could not start on time will be skipped and the next scan will be started as normal.

For remote agents, you must enable the **Immediately scan on agent restart or scope change** option if you want the agent service to scan immediately when it is added. This option is cleared by default.

- 11 Click **Finish**.

As the agent is installed, the status changes to reflect the progress of the installation. When the **Status** column is **OK**, the agent is installed. When the initial scan is complete, the **Data State** column displays **Data Available**. For information on adding an agent to the cluster, see [Adding an agent to a remotely-managed computer](#).

Managing managed computers

You can monitor your list of managed computers easily on the **Managed Computers** tab.

The **Managed Computer** tab is organized by domain name. Next to the domain name, you can quickly see how many of the managed computers are healthy or unhealthy. An unhealthy computer is indicated by a large red dot next to the **Name** column. Check the **Status** column for an indicator of the issue causing the unhealthy status.



Table 2. Descriptions of the columns on the Managed Computer tab

Column	Description
Name	The name of the computer being managed, which is the computer that the agent is scanning and reporting data to the Access Explorer database.
Domain	The name of the domain in which the managed computer resides.
Management Methods	The type of management used on the managed computer, either Locally Managed or Remotely Managed. <ul style="list-style-type: none">• Locally Managed indicates the managed computer and the agent computer are the same.• Remotely managed indicates the managed computer and agent computer are different.
Agent Computer	The name of the server on which the Access Explorer agent is installed.
Status	The status of the agent. The status updates automatically, but you also can click Refresh to update the Status column. If the status is OK, the agent is running successfully.


Table 2. Descriptions of the columns on the Managed Computer tab

Column	Description
Data State	The status of the data obtained by the agent. The status updates automatically, but you also can click Refresh to update the Data State column. If the data state displays data available, the last scan performed was successful and data is in the Access Explorer database.
Keyword	An optional word that you can add to the Managed Computer properties to help you filter the list. For more information, see Modifying managed computer properties .

To sort a column

- Click  to sort in descending alphabetical order (Z to A).
- Click  to sort in ascending alphabetical order (A to Z).


To filter a column

- Click  in a column heading to display a list of every entry in that column and select a value on which to filter.
 - (Blanks) displays rows with a blank entry in that column.
 - (Non-blanks) displays rows with an entry.
 - (Custom) opens a Custom AutoFilter where you can create a custom filter.

- OR -

If an empty row is displayed under the column headers, enter text in each column of this row to perform an exact-match search to narrow the results.

To clear a filter

- With a filter selected for a particular column, click  in that column heading and choose **(All)**.

Modifying managed computer properties

The properties that you can change depend on the type of installation you selected for the Access Explorer agent.

- For a locally managed computer, you can add a keyword and modify the scope of the scan.
- For a remotely managed computer, you can add a keyword, modify the scope of the scan, change the service account, and change the scanning schedule.

Topics:

- [Adding a keyword](#)
- [Changing the scan schedule](#)
- [Modifying the scope of a scan](#)

Adding a keyword

You can assign a keyword to a managed computer to help you sort and filter the list of managed computers.

To add a keyword to a managed computer

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.

- 3 Open the **Manage Computers** tab.
- 4 Select a managed computer and click **Edit**.
- OR -
Right-click a managed computer and select **Edit**.
- 5 On the **Details** page, type a keyword to identify the managed computer.
- 6 Click **OK**.

The keyword displays in the **Keyword** column. You can sort and filter the Keyword column to help you quickly find a managed computer.

Changing the scan schedule

You can change only the schedule of a remotely managed computer.

To change the scan schedule of a remotely managed computer

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Manage Computers** tab.
- 4 Select a remotely managed computer and click **Edit**.
- OR -
Right-click a remotely managed computer and select **Edit**.
- 5 Open the **Agent** page and change the schedule.
- 6 Click **OK**.

Modifying the scope of a scan

On a locally managed computer, the Access Explorer agent always scans all folders.

During setup of a remotely managed computer, you set the scope for the Access Explorer agent, but you can modify it at any time.

To modify the scope of the Access Explorer agent scan for a remotely managed computer

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Manage Computers** tab.
- 4 Select a remotely managed computer and click **Edit**.
- OR -
Right-click a remotely managed computer and select **Edit**.
- 5 Open the **Scopes** page.
- 6 Select the folders or shares to scan.
- 7 Click **OK**.

Managing Access Explorer agents

The Access Explorer agent scans selected folders, files, and shares on managed computers.

Topics:

- [Viewing agent details](#)
- [Changing the service account](#)
- [Adding an agent to a locally-managed computer](#)
- [Adding an agent to a remotely-managed computer](#)
- [Removing a managed computer](#)
- [Restarting an agent](#)
- [Understanding the status of your agent](#)

Viewing agent details

The Details page of the managed computer properties lists information about the agent that might be helpful in troubleshooting. You can see the date and time of the last scan performed, the port used by the agent service, and the version of the agent service.

To view agent details

- 1 Select **Tools | Access Explorer Configuration**.
- 1 Click **Configure Access Explorer**.
- 1 Open the **Manage Computers** tab.
- 1 Select a managed computer and click **Edit**.
- OR -
Right-click a managed computer and select **Edit**.
- 2 Open the **Details** page, if necessary.

Changing the service account

You can change the service account only on a remotely managed computer. If you need to change the service account on a locally managed computer, you must remove the installed agent first and then reinstall the agent with a new service account.

To change the service account on a remotely managed computer

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Manage Computers** tab.
- 4 Select a remotely managed computer and click **Edit**.
- OR -
Right-click a remotely managed computer and select **Edit**.
- 5 Open the **Agent** page, and select a Service Account.
If the service account you want is not listed, you need to add it. See [Adding service accounts](#).
- 6 Click **OK**.
The agent automatically updates. You also can click **Refresh** to update the **Status** column.

Adding an agent to a locally-managed computer

When setting up locally managed computers, you can choose to install the Access Explorer agent automatically. If you choose to install the agent manually, the locally managed computer is added to the list but the Access Explorer agent is not installed. The status of the computer remains at **Waiting for agent first connection** until the agent is installed.

To install the agent manually on a locally managed computer

- Run the agent installer located in the Security Explorer installation folder (Program Files\Quest\Security Explorer\Access Explorer\Agent Management\Agent).

Adding an agent to a remotely-managed computer

You can have multiple computers running the Access Explorer agent to scan a managed computer.

To add an agent to a remotely managed computer

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a remotely managed computer and click **Add Agent**.
- OR -
Right-click a remotely managed computer and select **Add Agent**.
- 3 On the **Scopes** page, select which folders or shares you want the agent to scan.
Folders, files, or shares assigned to other agents are unavailable for selection. If you need to reassign which folders or shares to scan, see [Modifying the scope of a scan](#).
- 4 Click **Next**.
- 5 On the **Agent** page, assign an Agent Computer and Service Account.
- 6 Set the schedule.
- 7 Click **Finish**.

Removing a managed computer

Removing the Access Explorer agent does not affect the contents of the Access Explorer database. Once the agent is removed, no new data is entered into the database, but the existing data remains.

To remove a managed computer

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Manage Computers** tab.
If a managed computer has multiple agents, the managed computer will be listed once for each agent.
- 4 To remove only one agent, select that agent and click **Remove**.
- OR -
If the entire managed computer needs to be removed, select all of its rows and click **Remove**.
- 5 Click **Yes**.
- 6 Click **OK**.

The **Status** column reflects the **Deconfiguration** and **Uninstall** of the Access Explorer agent. The status updates automatically, but you also can click **Refresh** to update the **Status** column. See [Agent status descriptions](#).

Restarting an agent

Restarting the agent causes a full rescan of the selected managed computer. A full scan occurs with a restart if you have enabled this option on the **Agent** page in the Properties of the managed computer. See [Changing the scan schedule](#).

i | **NOTE:** To determine whether data in the client is the most current from the agent, ensure that the data state of the managed computer being examined is marked as **Data Available**.

To restart an agent

- 1 Select **Tools | Access Explorer Configuration**.
- 2 Click **Configure Access Explorer**.
- 3 Open the **Manage Computers** tab.
- 4 Select the managed computer and click **Restart**.
- 5 Click **Yes**.
- 6 Click **OK**.

A red dot appears next to the managed computer and the status becomes **Agent unregistered** while the agent is restarted. The status updates automatically, but you also can click **Refresh** to update the status. When the restart is complete, the status is **OK**.

Understanding the status of your agent

When an agent is installed and scanning data, the **Status** column indicates **OK** and the **Data State** column indicates **Data Available**. If there is anything wrong with the agent, the state of the agent becomes unhealthy and the Status column displays text that may help with your troubleshooting.

Agent status descriptions

The following table details the possible entries in the **Status** field:

Table 3. Agent status descriptions in Access Explorer

Agent status	Description
Agent Unregistered	Agent has unregistered.
Configuration Failed	An error has occurred while creating the agent on the agent host computer.
Configuration in Progress	Agent is being configured.
Deconfiguration Failed	An error occurred while removing the agent from the agent host computer.
Deconfiguration in Progress	The agent is being removed.
Deleting	The agent is being deleted.
Deleting and Uninstalling	The agent software is being uninstalled.
Expired Lease	The agent has failed to renew its lease, which is often an indication of an error on the agent computer. Ensure that the agent is capable of communicating with the server.
Incompatible Agent Version	An unsupported agent version has attempted to register with the server.
Install Failed	An error occurred while installing the agent.
Install in Progress	The agent installation is in progress.
OK	The agent is in a good state and not experiencing any problems.
Registration Failed	An error occurred while the agent was attempting to register with the server.
Resolved	The agent computer has been resolved. This is a temporary state.

Table 3. Agent status descriptions in Access Explorer

Agent status	Description
Uninstall in Progress	The agent is being uninstalled.
Uninstalled	The uninstall has finished. This is a temporary state.
Unresolvable	The agent computer has not yet been resolved.
Upgrading Agents	The agents for this host are being upgraded to a newer software version.
Waiting for Agent First Connection	The management server is waiting for the agent to register with the server for the first time.

Data state descriptions

The following table details the possible entries in the **Data State** column:

Viewing Access Explorer objects

Table 4. Data state descriptions in Access Explorer

Data state	Description
A scanner error has occurred	A scanner error has occurred with one or more of the agent scanners for this managed computer.
Data Available	Agents deployed to this managed computer have completed their initial scans and returned their data.
Performing an initial scan	Agents deployed to this managed computer report that the scanners have begun their initial scans.
Waiting for scanner status	Agents have been deployed for this managed computer but they have not yet reported their scanner status to the server.
Waiting for scanners to start	Agents for this managed computer have reported back to the server but not all of the scanners have started up.

Access Explorer objects are visible in the All Management Targets and NTFS modules only. In the Navigation pane, expand or select an Access Explorer server to view the objects.

Topics:

- [Viewing groups and users](#)
- [Viewing computers](#)
- [Viewing resource groups](#)
- [Viewing permissions](#)

Viewing groups and users

In the Navigation pane, expand a management server to view a list of accounts that have permissions on the managed Access Explorer server, or click an object to display the list in the Objects pane.

If a group or user is not listed, the account has no permissions on the Access Explorer server. You can add a group or user from Security Explorer. See [Creating a new group](#) and [Creating a new user](#).

Viewing computers

To browse for permissions, expand a node in the Navigation pane to display the computers where Access Explorer has found permissions for the specified account. Expanding a computer displays a list of Resource Groups, which are Access Explorer results (folders and files) grouped by permission type (explicit or group membership).

Viewing resource groups

Resource groups provide a way of managing folders and files. Selecting a resource group in the Navigation pane displays a list of folders and files in the Objects pane.

Grouping folders and files into resource groups is optional and can be turned off on the **Access Explorer** tab of the **Options** dialog box. See [Setting options for Access Explorer](#). If you clear the **Display folder and file resource groups** check box, the full list of folders and files is displayed as soon as a computer is expanded.

Security Explorer displays results in pages to manage large volumes of results. Use the arrow keys to move through the pages of results.

Displaying results in pages is optional and can be turned off on the **Access Explorer** tab of the **Options** dialog box. See [Setting options for Access Explorer](#). If you clear the **Use Paging** when displaying results check box, all the folders and files are displayed as soon as a computer is expanded.

Viewing permissions

In the Objects pane, select a result to display its permissions in the Permissions pane. Permissions are grouped into two tabs.

- The **Access Explorer Permissions** tab displays the permissions for the selected account as they exist in the Access Explorer database.
- Open the **Live Permissions** tab to view the current live permissions.

Select a permission to perform typical NTFS Security module functions, such as Grant, Revoke, or Clone. See [Managing permissions](#) for more information about NTFS Security module functionality.

If you want to extend the NTFS functionality to Access Explorer objects, select the **Allow operations to be performed directly on Enterprise Objects** check box on the Access Explorer tab in the Options dialog box. See [Setting options for Access Explorer](#).

Searching Access Explorer servers

You can add only Access Explorer servers to an NTFS module search scope. All standard NTFS module search options are available and the search process is the same as any other search in the NTFS Security module. See [Using the Browse tab to search](#).

Using the Access Explorer permission wizard

The Access Explorer Permission Wizard helps you manipulate explicit permissions and/or group memberships for Access Explorer accounts, computers, and/or resource groups.

The Access Explorer Permission Wizard is available only when an Access Explorer account, computer, and/or resource group is selected. The Permission Wizard supports multiple-selection. The Permission Wizard is not

available if you select an Access Explorer result, such as a folder or file. In these cases, use the standard NTFS module functions, such as Grant, Modify, or Delete.

You can use the functions available in the NTFS Security module to make changes to permissions on a folder or file. If you want to make changes to an Access Explorer object, such as deleting all permissions on an account on a specific computer, it is recommended that you use the Permissions Wizard.

If you want to extend the NTFS functionality to Access Explorer objects, select the **Allow operations to be performed directly on Enterprise Objects** check box on the **Access Explorer** tab in the **Options** dialog box. See [Setting options for Access Explorer](#).

i | IMPORTANT: Changes made using the Access Explorer Permission Wizard can potentially affect many folders or files. Apply these type of changes with extreme caution.

To run the Access Explorer Permission wizard

- 1 Select Access Explorer accounts, computers, or resource groups.
- 2 Select **Tools | Access Explorer Permission Wizard**.
–OR–
Press **F10**; or right-click a selection, and choose **Permission Wizard**.
- 3 Click **Next**.
- 4 Select an option.

Table 5. Access Explorer Permission Wizard options

Option	Description
Change all permissions	Select to change all the permissions for the selected Access Explorer object. See Changing all permissions .
Clone all permissions	Select to clone all the permissions for the selected Access Explorer object from the selected source to a new selected target (or targets). See Cloning all permissions .
Delete all permissions	Select to delete all permissions for the selected Access Explorer object. See Deleting all permissions .
Export all permissions	Select to export all permissions for the selected Access Explorer object. See Exporting all permissions .
Backup all permissions	Select to back up all permissions for the selected Access Explorer object. See Backing up permissions .

Changing all permissions

To change all permissions

- 1 Select Access Explorer accounts, computers, or resource groups.
- 2 Select **Tools | Access Explorer Permission Wizard**.
–OR–
Press **F10**; or right-click a selection, and choose **Permission Wizard**.
- 3 Click **Next**.
- 4 Select **Change all permissions**, and click **Next**.
- 5 Choose to change all explicit permissions and/or remove all permissions applicable through group membership. To preview the types of changes, click **Preview**.

i | TIP: If you preview changing all explicit permissions, you also can export the list.

- 6 Click **Next**.
- 7 Choose the new permission, and click **Next**.
- 8 Select options.

Table 6. Change permission options

Option	Description
Perform full permission backup before making changes	Select to back up permissions before changes are made. Type a path or browse to locate a path. NOTE: Performing a backup may significantly slow down processing, especially if there is a large number of Access Explorer results.
Create report (will list changed items)	Select to create a report that lists all the changed items. Type a path or browse to locate a path.
Produce report only (i.e. no changes will be made)	Select to create the report only. No changes to the permissions are made.

- 9 Click **Finish**.

Cloning all permissions

Choose this option to clone all the permissions for the selected Access Explorer object from the selected source to a new selected target (or targets).

To clone all permissions

- 1 Select Access Explorer accounts, computers, or resource groups.
- 2 Select **Tools | Access Explorer Permission Wizard**.
–OR–
Press **F10**, or right-click a selection, and choose **Permission Wizard**.
- 3 Click **Next**.
- 4 Select **Clone all permissions**, and click **Next**.
By default, all explicit permissions for the selected account(s) are cloned and group memberships are ignored.
- 5 Choose to clone all explicit permissions, and/or clone all permissions applicable through group membership. You also can choose to replace the source permissions with the destination permissions and clone ownership. To preview the types of changes, click **Preview**.
- 6 Click **Next**.
- 7 Type a destination account, or click **Find** to locate an account.
- 8 Click **Add**. The account is added to the Destination Accounts list.
 - To remove selected accounts from the list, click **Remove**.
 - To remove all accounts from the list, click **Clear**.
- 9 Click **Next**.
- 10 Select options.

Table 7. Clone options

Option	Description
Perform full permission backup before making changes	Select to back up permissions before changes are made. Type a path or browse to locate a path. NOTE: Performing a backup may significantly slow down processing, especially if there is a large number of Access Explorer results.
Create report (will list changed items)	Select to create a report that lists all the changed items. Type a path or browse to locate a path.
Produce report only (i.e. no changes will be made)	Select to create the report only. No changes to the permissions are made.

- 11 Click **Finish**.

Deleting all permissions

Choose this option to delete all the permissions for the selected Access Explorer object.

To delete all permissions

- 1 Select Access Explorer accounts, computers, or resource groups.
- 2 Select **Tools | Access Explorer Permission Wizard**.
–OR–
Press **F10**; or right-click a selection, and choose **Permission Wizard**.
- 3 Click **Next**.
- 4 Select **Delete all permissions**, and click **Next**.
By default, all explicit permissions for the selected account(s) are deleted and group memberships are ignored.
- 5 Choose to delete all explicit permissions and/or remove all permissions applicable through group membership. To preview the types of changes, click **Preview**.
- 6 Click **Next**.
- 7 Select options.

Table 8. Delete options

Option	Description
Perform full permission backup before making changes	Select to back up permissions before changes are made. Type a path or browse to locate a path. NOTE: Performing a backup may significantly slow down processing, especially if there is a large number of Access Explorer results.
Create report (will list changed items)	Select to create a report that lists all the changed items. Type a path or browse to locate a path.
Produce report only (i.e. no changes will be made)	Select to create the report only. No changes to the permissions are made.

- 8 Click **Finish**.

Exporting all permissions

Choose this option to export all permissions for the selected Access Explorer object.

To export all permissions

- 1 Select Access Explorer accounts, computers, or resource groups.
- 2 Select **Tools | Access Explorer Permission Wizard**.
–OR–
Press **F10**; or right-click a selection, and choose **Permission Wizard**.
- 3 Click **Next**.
- 4 Select **Export all permissions**, and click **Next**.
- 5 By default all permissions for the selected accounts are exported. If you want to include permissions applicable to the selected account through group membership, select the check box.
- 6 Click **Finish**. See [Exporting security](#).

Backing up permissions

Choose this option to back up all permissions for the selected Access Explorer object.

To back up permissions

- 1 Select Access Explorer accounts, computers, or resource groups.
- 2 Select **Tools | Access Explorer Permission Wizard**.
–OR–
Press **F10**; or right-click a selection, and choose **Permission Wizard**.
- 3 Click **Next**.
- 4 Select **Backup all permissions**, and click **Next**.
- 5 Click **Finish**. See [Backing up security](#).

Setting options for Access Explorer

To set options for Access Explorer

- 1 Choose **Tools | Options**, and open the **Access Explorer** tab.
- 2 Set view options.

Table 9. View options

Option	Description
Display folder and file resource groups	By default, folders and files are grouped into resource groups. You have to select a resource group to display the folders and files in that group. To display all the files and folders when you select an account or computer, clear the check box. It is recommended that you keep this option selected as the list of folders and files could be very large.
Use "Paging" when displaying results	By default, when you select a resource group, the folders and files are grouped in pages with a maximum of 2500 results per page. You can change the number of results per page by typing a new value in the Page Size box. To display all the folders and files at once, clear the check box. It is recommended that you keep this option selected as the list of folders and files could be very large.

3 Set options for Grant, Revoke, and Clone operations.

Table 10. Grant, Revoke, and Clone options

Option	Description
Always reload results when performing management operations	By default, management operations, such as Grant, Revoke, or Clone, and changes applied through the Permission Wizard are performed on cached Access Explorer results. A warning message displays and gives you the opportunity to force an update and reload the results before the operation is performed. If you want to bypass this warning message and always reload the results, select this check box.
Allow operations to be performed directly on Enterprise objects	By default, management operations, such as Grant, Revoke, or Clone, are performed on Access Explorer results (folders and files) only. If you want to perform these operations on Access Explorer objects (accounts, computers, and resource groups), select this check box. NOTE: It is strongly recommended that you use the Permissions Wizard to perform these operations on Access Explorer objects (accounts, computers, and resource groups).
Show warning dialogs for grant, revoke, and clone operations	By default, a warning message displays if a Grant, Revoke, Clone, or Set Owner operation is selected for an Access Explorer account, computer, or resource group. If you want to suppress the display of this warning message, clear the check box. <i>Available only if Allow operations to be performed directly on Enterprise objects is selected.</i>
Include group memberships	By default, only explicit permissions for the parent account are included in any Security Explorer management operation. If you want to also include group membership results, select this check box.
Do not perform operations on the 'Domain User' group	By default, operations are not performed on the Domain User group.

Working with Microsoft Active Directory

In the Active Directory Security module, you can easily manage permissions on objects in Active Directory® to secure and protect your data.

Topics:

- [Viewing Active Directory permissions](#)
- [Granting Active Directory permissions](#)
- [Revoking Active Directory permissions](#)
- [Cloning Active Directory permissions](#)
- [Searching for Active Directory objects](#)
- [Modifying Active Directory permissions](#)
- [Modifying group memberships](#)
- [Modifying Active Directory properties](#)
- [Deleting Active Directory permissions](#)
- [Backing up and restoring Active Directory security](#)
- [Exporting Active Directory permissions](#)
- [Setting options for Active Directory Security](#)

Viewing Active Directory permissions

i | NOTE: The **View Permissions** task opens the **Browse** tab.

To view Active Directory permissions

- 1 Open the **Active Directory Security** module.
- 2 In the Navigation pane, expand the Active Directory® node to browse all Active Directory objects in the default naming contexts of the specified domains. See [Using the Navigation pane](#).
 - If loading is taking too long, you can click **Stop** in the loading progress bar. To reload the current node, click **Reload** or press **F5**. See [Using the loading progress bar](#).
- 3 In the Navigation pane, select an object.
The Objects pane displays the LDAP path, the children of the selected object, the object name, and owner. See [Using the Objects pane](#).
- 4 In the Objects pane, select a child object. The Permissions pane displays permissions for the selected object. The **Owner** box displays the user or group that owns the selected object.
- 5 Set options for the displayed permissions. See [Using the Permissions pane](#).

i **TIP:** The contents of the columns may be too long to view on the page. You can size the columns or select the permissions, use Ctrl+C to copy the selection to the clipboard, and paste into a text file. You also can select the object and export a permissions report. See [Exporting Active Directory permissions](#).

Granting Active Directory permissions

You can grant permissions to domain users and groups without affecting the permissions of any other user. First, choose the permissions to grant, and select a domain user or group. You can grant different permissions for several domain users and groups with one operation.

i **TIP:** The Grant task provides a quick way to grant permissions. See [Using the Grant task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**.

NOTE: You can grant permissions on only domain groups and users.

To grant permissions

- 1 Open the **Active Directory Security** module.
- 2 Locate the object with the permission to grant. See [Viewing Active Directory permissions](#).
- 3 Right-click selected permission(s), and choose **Grant Permissions**.

The **Grant Active Directory Permissions** dialog box displays the path, and the associated groups and users for the current object. The navigation tree is hidden by default. To view the navigation tree, click **►**.

- 4 Select the domain groups and users to apply the permission. There are a few methods for selecting groups and users.
 - Choose from the list of domain groups and users in the navigation tree.
 - To filter the list in the left pane, type a server name or base path in the box, and click **Set**.
 - To return the full list to view, click **Reset**. The list returns to full view the next time you open Grant Permissions.
 - Select from the list of domain groups and users associated with the current object.
 - To change to another domain, select the domain from the **List Names From** list.
 - To display users in the list, click **Show Users**. To return the list to show only groups, click **Refresh**.
 - To select a group/user not displayed, type a name or click **Advanced User Selection**.
 - Browse for a domain group or user.
- 5 From the **Permission** list, select the permissions to grant, and whether or not to Allow or Deny. If the choice is not available in the list, click **Advanced Permission Selection** to create a custom choice.
- 6 From the **Applies To** list, select how to apply the permissions.
- 7 To propagate the client permission to the subtree, select the check box.
- 8 To add the domain group/user to the **List of users and groups to grant** list, click **Add**.

i **TIP:** To add additional domain groups or users to the **List of users and groups to grant** list with the selected permission settings, you can hold down CTRL or SHIFT, and click a domain group or user from the list, or double-click a group or user in the navigation tree.
- 9 Click **OK**. The **Granting Permissions** box displays the progress. See [Completing a process](#).

Revoking Active Directory permissions

You can revoke access for domain users and groups.

i | **TIP:** The Revoke basic task provides a quick way to revoke permissions. See [Using the Revoke tasks](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**.

To revoke permissions

- 1 Open the **Active Directory Security** module.
- 2 Locate the object with the permission to revoke. See [Viewing Active Directory permissions](#).
- 3 Right-click selected permission(s), and choose **Revoke Permissions**.
The **Revoke Permissions** dialog box displays the path, and the associated groups and users for the current object. The navigation tree is hidden by default. To view the navigation tree, click ►.
- 4 Select the domain groups and users to revoke the permission. There are a few methods for selecting groups and users.
 - Choose from the list of domain groups and users in the navigation tree.
 - To filter the list in the left pane, type a server name or base path in the box, and click **Set**.
 - To return the full list to view, click **Reset**. The list returns to full view the next time you open Revoke Permissions.
 - Select from the list of domain groups and users associated with the current object.
 - To change to another domain, select the domain from the **List Names From** list.
 - To display domain users in the list, click **Show Users**. To return the list to show only groups, click **Refresh**.
 - Browse for a domain group or user or click **Advanced User Selection**.
- 5 From the **Permission** list, select the permissions to revoke, and whether or not to Allow or Deny. If the choice is not available in the list, click **Advanced Permission Selection** to create a custom choice.
- 6 Choose options.

Table 1. Revoke options

Option	Description
Revoke all permissions (Allow and Deny) for the selected user	Select to revoke all permissions (Allow and Deny) for the selected user.
Propagate client permissions down to subtree	Select to revoke the specified permissions from the child objects of the client.

- 7 To add the domain group/user to the **List of users and groups to revoke** list, click **Add**.
i | **TIP:** To add additional domain groups or users to the **List of users and groups to revoke** list with the selected permission settings, you can hold down CTRL or SHIFT, and click a domain group or user from the list or double-click a group or user in the navigation tree.
- 8 Click **OK**. The **Revoking Permissions** box displays the progress. See [Completing a process](#).

Cloning Active Directory permissions

Use the Clone feature to copy the permissions of one user/group to another user/group..

i | **TIP:** The Clone task provides a quick way to clone permissions. See [Using the Clone task](#). For more options, add a path, and click **Switch to Security Explorer Classic (Advanced)**.

To clone permissions

- 1 Open the **Active Directory Security** module.
- 2 Locate the object with the permission to clone. See [Viewing Active Directory permissions](#).
- 3 Select **Security | Clone Group or User**.

-OR-

Right-click the objects, and choose **Clone Group or User**.

i | **NOTE:** If the selected object has subnodes, you can select multiple objects in the Objects pane to clone.

The **Clone Active Directory Permissions** box opens to the **Manual User/Group Selection** tab and displays the path to the selected object and the associated groups and users.

- 4 Select the groups or users to clone. See [Selecting users and groups manually](#).
- 5 Select options.

Table 2. Clone options

Option	Description
Clone permissions	By default, permissions are cloned.
Clone group memberships	Select to add the destination account to the groups of which the source user is a member. If you choose this check box, a warning message displays. The destination is cloned into the same parent groups as the source. The contents of the groups selected as the source are not cloned.
Propagate permissions down to subtree	Write over the permissions of the child objects.

- 6 Click **OK**. See [Completing a process](#).

Searching for Active Directory objects

i | **TIP:** The Search basic task provides a quick way to search for permissions. See [Using the Search tasks](#).

To search for Active Directory® objects

- 1 Open the **Active Directory Security** module.
- 2 Locate the object to search. See [Viewing Active Directory permissions](#).

i | **NOTE:** If you open the **Search** tab in the Navigation pane without selecting an object, you need to add a Search Scope before you set criteria. See [Adding a search scope](#).

- 3 Select **Search | Search in a New Window (Empty)**.

-OR-

Click  on the Tool Bar; or right-click an object, and choose **Search in a New Window**.

- 4 The object you select is added as a Search Scope so you can just set the criteria for the search.

i | **NOTE:** All selected scopes must be from the same forest.

Table 3. Permission search criteria

Option	Description
Name	Enter or browse for the name of the principal that you want to find. Use * to match any number of characters. Use ? to match any single character. The comparison is not case sensitive.
Include all group memberships	Select to include all group memberships. The groups to which the account belongs appear in the drop-down list.
Permission	You can search for a name or a permission type. If you want to search for permissions, type the permissions in the box separated by commas. Alternatively, browse to select permissions from a list.
Allow Permissions	By default, allow permissions are included in the search results. To exclude allow permissions, clear the check box.
Inherited Permissions	By default, inherited permissions are included in the search results. Inherited permissions are indicated by (I) in the Type column. To exclude inherited permissions, clear the check box.
Deny Permissions	By default, deny permissions are included in the search results. To exclude deny permissions, clear the check box.
Explicit Permissions	By default, explicit permissions are included in the search results. To exclude explicit permissions, clear the check box.
Search for unknown accounts	Select to search for accounts deleted from Active Directory.
Search for disabled accounts	Select to search for disabled accounts.
Search for inheritance-disabled objects	Select to search for inheritance-disabled objects.

- 5 Click **Start Search**.
- 6 Use the buttons to manage the results. You can save the search, save the search results, or generate a report.

Table 4. Search tab buttons

Button	Description
Start Search	Start the search based on the current Search Scope and selected criteria.
Stop Search	Stop the search process.
Clear Results	Clear the results area.
Defaults	Return to the default selections on all search criteria tabs.
Save Results	Save the results as a .txt file.
Report	Display the results in a report format that you can save, print, or export.
Schedule	Schedule a search.

Modifying Active Directory permissions

Modify the permissions of groups or users on the selected Active Directory® object. Use this feature for quick changes to accounts displayed in the permissions list. Use the Grant feature to give permissions to accounts that are not displayed in the permissions list. See [Granting Active Directory permissions](#).

i | IMPORTANT: You cannot modify inherited permissions directly. Inherited permissions are indicated by **Allow (I) in the Type** column. To modify these permissions, you must modify the parent object.

To modify permissions

- 1 Open the **Active Directory Security** module.

- 2 Locate the object with the permissions to modify. See [Viewing Active Directory permissions](#).
- 3 Select the object in the Objects pane or the permissions in the Permissions pane.

i | NOTE: If you choose multiple permissions, the selected permissions must be under the same path or object. If the paths are not the same, you receive a warning message.
- 4 Select **Security | Modify Permission**.

-OR-

Right-click the permissions, and choose **Modify Permission**.
- 5 Select the principal name, if necessary.
- 6 Select the permission role, if necessary.
- 7 Select how to apply the permission, if necessary.
- 8 Modify the current permissions.
- 9 Select whether to modify permissions on child objects.

Table 5. Modify options

Option	Description
Propagate modifications down to subtree	<p>The selected modifications are propagated to child objects.</p> <ul style="list-style-type: none"> • If the child object does not have the selected modified permission, it is granted to the child object. • If the child object has the selected modified permission and the modification is less than the parent object, the permission is revoked. • If the child object has the selected modified permission and the permission is greater than the parent object, the permission is not changed.

- 10 Click **OK**.

You are asked to verify that the selected permissions will be revoked and the new permissions you selected will be granted.
- 11 Click **Yes**.

Modifying group memberships

To modify group memberships

- 1 Open the **Active Directory Security** module.
- 2 Display the permissions for a selected object. See [Viewing Active Directory permissions](#).
- 3 In the Permissions pane, select a group or user. You can view the members of a group or view the groups of which the user is a member.

- To view the members of a selected group, select **Tools | Display Group Contents**.

-OR-

Click **Contents** in the Control Button Bar; or right-click a group, and choose **Display Group Contents**
 - To view the groups of which a selected user is a member, select **Tools | Display Memberships**.

-OR-

Right-click a user and choose **Display Memberships**.

- 4 Use the buttons to modify the group memberships.

Table 6. Modify group membership options

Button	Description
Add	Add members to the selected group.
Remove	Remove selected members from the selected group.
Refresh	Refresh the list after adding or removing a member.
Print	Print the list.
Save	Save the list as a .txt file.
Show Group Contents	View the members of a selected group.
Show Memberships	Show the groups of which the selected group or user is a member.
Close	Close the Group contents box.

Modifying Active Directory properties

i | **NOTE:** To display Active Directory properties, Administration Tools Pack (adminpak) must be installed on the client computer.

To modify Active Directory properties

- 1 Open the **Active Directory Security** module.
- 2 Display the objects. See [Viewing Active Directory permissions](#).
- 3 Select an object in the Navigation or Objects pane, and select **Tools | Active Directory Properties**.

–OR–

Right-click an object in the Objects pane, and choose **Active Directory Properties**.

Deleting Active Directory permissions

To delete permissions

- 1 Open the **Active Directory Security** module.
- 2 Locate the type of permission to delete. See [Viewing Active Directory permissions](#).
- 3 Right-click selected permission(s), and choose **Delete Permission**.

The permissions will be deleted from the object, and also from sub-objects that inherited those permissions. If you also want to delete the same independent permissions from the sub-objects, select the **Propagate client permissions down to subtree** check box.

- 4 To delete the permission(s), click **Yes**. See [Completing a process](#).

Backing up and restoring Active Directory security

Table 7. Backup and restore Active Directory® security

Task	Description
Backup	See Backing up security .
Restore	See Restoring security .
Scheduled Backups	See Scheduling a backup .

Exporting Active Directory permissions

By default, permissions are exported to a report, which you can save, print, or export. You can generate a report or export permissions to a delimited file for use with Microsoft® Excel®. This report is useful when you are asked to see which users have access to a specific Active Directory path.

TIP: The Export task provides a quick way to export permissions to a report that you can save, print, or export. See [Using the Active Directory Export task](#). For more options, click **Switch to Security Explorer Classic (Advanced)**.

To export Active Directory permissions


- 1 Open the **Active Directory Security** module.
 - 2 Locate the object to export. See [Viewing Active Directory permissions](#).
 - 3 Select **Security | Export**.
- OR–
- Click  on the Tool Bar; or right-click an object, and choose **Export**.
- 4 Select to include group members in the export. You can include nested groups and members of the Domain Users group.
 - 5 Select the output option.

Table 8. Output options

Option	Description
Generate Report	By default, permissions are exported to a report, which you can save, print, or export.
Save to Microsoft Excel(R) Spreadsheet	Permissions can be saved only to a delimited file for use with Microsoft Excel. Select either Comma-delimited file (.CSV) or Tab-delimited file (.TXT) . Browse to locate a destination for the file.

- 6 Click **OK**.

Using the Active Directory Export task

The Export task provides a quick way to export permissions to a report that you can save, print, or export. For more options, click **Switch to Security Explorer Classic (Advanced)**. See [Exporting Active Directory permissions](#).

i | **NOTE:** The **Tasks** tab is hidden by default. To display the **Tasks** tab, select **View | Tasks tab**.

To export permissions using the Export task

- 1 Open the **Active Directory Security** module.
- 2 Open the **Tasks** tab.
- 3 Click **Export**.
- 4 Click **Add** to add paths.
- 5 Click **OK**.

Setting options for Active Directory Security

By default, the Active Directory Security module attempts to connect to the default naming context of the current domain on which the user is logged on. You can add more connections to reach the default naming context of other domains with specified credentials. If you add a connection for the current domain, Security Explorer will use the new connection setting instead of the default connection.

i | **NOTE:** Security Explorer only supports domains that have a trusted relationship with the current domain on which the user is logged on.

To add more connections

- 1 Select **Tools | Options**.
- 2 Open the **Active Directory** tab.
- 3 Click **Add**.
- 4 Type the target domain DNS name or domain controller server name with or without the port number.

i | **NOTE:** If no port number is specified, Security Explorer uses the default port number 389.

- 5 Set optional credentials.

i | **NOTE:** If you do not specify alternate credentials, the credentials of the currently logged on user are used.

- 6 Click **OK**.

You can add more connections; or edit or delete selected connections. To remove all connections from the list, click **Clear**.

- 7 Click **OK**.

Customizing Security Explorer

The Security Explorer® Options provide flexibility to the appearance and functionality of Security Explorer.

i | **NOTE:** The tabs available with **Tools | Options** that are not described in this chapter are covered in other chapters. See [Setting SharePoint options](#), [Setting options for SQL Server](#), [Setting options for Exchange security](#), [Setting options for Access Explorer](#), and [Setting options for Active Directory Security](#).

Topics:

- [Setting general options](#)
- [Setting view options](#)
- [Setting alternate credentials for workgroups](#)
- [Setting alternate credentials for services and tasks](#)
- [Setting alternate credentials NAS devices](#)
- [Setting advanced options](#)
- [Controlling access to Security Explorer](#)

Setting general options

To set general options

- 1 Choose **Tools | Options**.
- 2 Set the startup option.

Table 1. Startup option

Option	Description
Reload window state (size and view menu entries)	By default, the size of the Security Explorer window and choices on the View menu are saved upon exiting the application. Clear to use the standard size and center the Security Explorer window on your display.

- 3 Set options to occur when modifying permissions.

Table 2. Modify options

Option	Description
Always display progress dialog	Select an option to manage the display of the progress dialog when you modify permissions. Choosing to display the progress dialog for long operations only (default) or to never display the progress dialog may help with memory management.
Display progress dialog for long operations only	
Never display progress dialog	

Table 2. Modify options

Option	Description
Auto-close progress dialog on completion	Select to always close the progress dialog upon completion of a process, such as granting or cloning.
Perform an inheritance check after creating new folders	Select to always perform an inheritance check and repair after creating new folders.

- 4 Set the option for Windows® Explorer.

Table 3. Windows Explorer option

Option	Description
Include Security Explorer context menu	Select to display the Security Explorer context menu in Windows Explorer. You can access the context menu from the Start menu, the Windows Explorer File menu or a shortcut menu. NOTE: If the current user is not a member of local Administrator group, the Include Security Explorer context menu check box is disabled.

- 5 Set options for scheduled backups.

Table 4. Scheduled backups option

Option	Description
Prefix backup name with date and time	By default, backup file names begin with the date and time. To remove the date and timestamp prefix from backup file names, clear the check box.
Purge NTFS Backup Files	Click to purge backup files. See Purging backup files and Scheduling a backup purge .

- 6 Set options for email notification.

Table 5. Email notification options

Option	Description
Send email notification upon completion of a scheduled task	Select to send an email notification when a scheduled task completes.
SMTP Settings	Click to configure SMTP settings for the email notification.

- 7 Set options for logging.

Table 6. Logging options

Option	Description
Log all security changes	Select to log all permission changes to the selected root path displayed in the box. Browse to locate the root folder. Only information about the selected root path is logged; no information about changes to sub-items is logged. To prefix each security change entry, type a string in the Change management prefix box. If the Change Management prefix is set to 0 (zero), no prefix is used.
Show detailed error messages	Select to show detail for error messages in the log file.

- 8 Click **OK**.

Setting view options

To set view options

- 1 Choose **Tools | Options**, and open the **View** tab.
- 2 Set permissions options.

Table 7. Permission options

Option	Description
Use advanced style for users and groups	Select to include a UPN, if available, following the name in the Name column. For example: Joseph Smith (J.Smith@123.com). If the UPN is unavailable, the basic style is used. The advanced style may slow the display of permissions.
Use basic style for users and groups (ie name only)	By default, only the domain name\user name displays in the Name column. For example: ACME\JSmith.
Include SID on permission change/search dialogs	Select to show the SID column in dialog boxes. By default, the SID column is hidden.

- 3 Set options for objects, such as groups, users, or shares.

Table 8. Objects options

Option	Description
Show Workgroup collection (Groups/Users module only)	<i>Group and User Management module only.</i> Select to display workgroup computers of local groups and local users in the navigation pane. Also adds the Workgroup tab to Security Explorer options. See Setting alternate credentials for workgroups .
Show domain controllers when selecting groups and users	Select to enable domain controller selection when browsing groups and users on the Grant, Revoke, and Clone dialog boxes. In addition, a Domain Controllers node displays under each domain parent node in the Navigation pane.
Show description column for permissions (not SharePoint, Exchange)	Select to display a Description column in the Permissions pane. <i>Not available in the Exchange Security and SharePoint Security modules.</i>
Highlight disabled users (may slow browsing performance)	Select to display an icon next to disabled users in the Permissions pane and Owner box.
Highlight shared folders (may slow performance)	Select to display icons next to shared folders in the Navigation pane and in the Objects pane.
Show Printer Shares	Select to display printer shares in the Objects pane. By default, printer shares do not display.
Do not show disabled users (Groups/Users module only)	<i>Group and User Management module only.</i> Select to hide disabled users from the display.

- 4 Set options for warnings.

Table 9. Warnings options

Option	Description
Display warning message before loading large NTFS folders, registry keys and Exchange mailboxes	By default, a warning message displays if the number of NTFS subfolders and files, registry keys, or Exchange mailboxes exceeds the value specified in the Trigger box.
Display warning if inheritance fault detected (NTFS only)	Select to display a warning if incorrectly inherited permissions are found.

- 5 Click **OK**.

Setting alternate credentials for workgroups

Group and User Management module only. Use alternate credentials to specify additional accounts that have administrative privileges to various computers on your network. Each account in the list is tried in the order listed until an account is found with sufficient privileges. If no account is found with administrative privileges, Access Denied is displayed.

By default, Security Explorer uses the credentials of the logged-in user. Alternate credentials are used only for command processing, such as management operations, and not for search operations, which are executed under the logged-in user's account.

- NOTE:** To use alternate credentials for workgroups, you need to select the **Show Workgroup collection** check box on the **View** tab in Security Explorer Options. See [Setting view options](#).
- NOTE:** For many operations, such as adding a new user/group, you must use the local Administrator account.

To set alternate credentials for workgroups

- 1 Choose **Tools | Options**, and open the **Workgroup** tab.
- 2 To add alternate credentials:
 - a Click **Add**.
 - b Type an account name, or browse to select an account.
 - c Type the password.
 - d Type a computer name (optional).
 - e Click **OK**.
- 3 Use the buttons to manage alternate credentials.
 - To modify the selected alternative credential, click **Edit**.
 - To delete the selected alternative credentials, click **Del**.
 - To clear the list of alternative credentials, click **Clear**.
- 4 Click **OK**.

Setting alternate credentials for services and tasks

Use alternate credentials to specify additional accounts that have administrative privileges to various computers on your network. Each account in the list is tried in the order listed until an account is found with sufficient privileges. If no account is found with administrative privileges, Access Denied is displayed.

By default, Security Explorer uses the credentials of the logged-in user. Alternate credentials are used only for command processing, such as management operations, and not for search operations, which are executed under the logged-in user's account.

- NOTE:** To use alternate credentials for Services/Tasks, you need to run Security Explorer under a local administrator account.

To set alternate credentials for services and tasks

- 1 Choose **Tools | Options**, and open the **Services/Tasks** tab.
- 2 To add alternate credentials:
 - a Click **Add**.
 - b Type an account name, or browse to select an account.
 - c Type the password.
 - d Type a computer name (optional).
 - e Click **OK**.
- 3 Use the buttons to manage alternate credentials.
 - To modify the selected alternative credential, click **Edit**.
 - To delete the selected alternative credentials, click **Del**.
 - To clear the list of alternative credentials, click **Clear**.
- 4 Click **OK**.

Setting alternate credentials NAS devices

Use alternate credentials to specify additional accounts that have administrative privileges to various NAS devices on your network. Each account in the list is tried in the order listed until an account is found with sufficient privileges. If no account is found with administrative privileges, Access Denied is displayed.

i | **NOTE:** For some NAS devices, Security Explorer may require that you explicitly provide credentials, because Security Explorer uses Secure Shell (SSH) connections for certain actions.

To set alternate credentials for NAS devices

- 1 Choose **Tools | Options**, and open the **NAS Devices** tab.
- 2 To add alternate credentials:
 - a Click **Add**.
 - b Type an account name, or browse to select an account.
 - c Type the password.
 - d Type a computer name (optional).

i | **NOTE:** Security Explorer recognizes NAS devices by computer name, so it is beneficial to identify the device by entering a computer name.
 - e Click **OK**.
- 3 Use the buttons to manage alternate credentials.
 - To modify the selected alternative credential, click **Edit**.
 - To delete the selected alternative credentials, click **Del**.
 - To clear the list of alternative credentials, click **Clear**.
- 4 Click **OK**.

Setting advanced options

To set advanced options

- 1 Select **Tools | Options**, and open the **Advanced** tab.
- 2 Set options for domains and computers.

Table 10. Domain and computer options

Option	Description
Load domains using Active Directory	Select to load domains when you select items in the Navigation pane.
Load computers using Active Directory	By default, computers, groups, and users are loaded when you select items in the Navigation pane.
Include unknown computers when browsing/searching domains	To activate this check box, clear the Load computers, groups and users using Active Directory check box. Select to include unknown computers in the Navigation pane.
Highlight domain controllers when browsing domains	By default, an icon displays next to domain controllers.
Highlight workstations and servers when browsing domains	By default, servers and workstations are identified by different icons. If you clear this check box, both servers and workstations are identified by the same icon.
Auto-detect computers which are members of a cluster	Select to automatically select the Show Cluster File Shares check box when browsing computers that are members of a cluster. If selected, a warning message displays when you click OK . Click Yes to verify the selection. See Viewing permissions .
Check connection before loading (Ping)	Select to ping computers before loading. If a computer is unavailable, a warning message appears. The default time-out is set to 1,500 ms. By default, Security Explorer does not check the connection, which could cause a response delay if that computer is unavailable.

- 3 Set options for modifying permissions (NTFS).

Table 11. Modifying Permissions (NTFS) options

Option	Description
Do not set 'Archive' attribute when setting security	By default, the Archive attribute is set to Archive when a change is made to a permission. Select to leave the Archive attribute set to Normal if a change is made.
Skip reparse points when processing permission changes	By default, reparse points are skipped when processing permission changes.
Skip subfolders and files when processing This Folder Only permissions (Grant/Delete only)	By default, child items under the parent folder are processed when granting or deleting the This Folder Only permission. Select to skip processing child items when granting or deleting the This Folder Only permission, which may speed up the process. NOTE: If you choose to skip subfolder processing, any existing inheritance issues are not corrected automatically as part of the processing.

- 4 Set the thread count.

By default, up to 10 searches and some process operations can run concurrently. To change the number, type a value in the Thread Count box.

- 5 Set the options for the browsing cache.

Table 12. Saved Information and Browsing Cache options

Option	Description
Use cache when browsing	By default, if the user browses to a path, such as c:\windows, the contents of c:\windows is stored in either a display (stored in memory) or a persistent (stored in an SQLite database) cache and can be reloaded immediately. Clear the check box to disable the caches and always reload information from the original target.
Use persistent cache	By default, a persistent SQLite database cache is used to store and quickly display lists, even if the console has been restarted since the cache contents were loaded originally.
View indicator when items loaded from cache	By default, a C displays next to items loaded from the cache and CACHE displays in the status bar. The default size of the display cache is 25 entries. Clear the check box to remove the indicator from display.
Do not use cached entries older than	By default, the age of the cache entry is examined prior to loading a path. By default, entries older than 3 hours are reloaded from the disk. You can set the value in the Display cache box up to 24 hours and in the Persistent cache box up to 999 hours. If the user revisits a path, the age of the cached entry is inspected to determine if the path is loaded from the cache or disk. <ul style="list-style-type: none"> • If the age of the cache entry is less (younger) than the values set in the Display cache and Persistent cache boxes, the entry is reloaded from the cache. • If the age of the cache entry is greater (older) than the values set in the Display cache and Persistent cache boxes, then the cache entry is removed and the entry is reloaded from disk.
Cache Reset All	Click to clear the database caches for all modules. Active only if the Use cache when browsing or Use persistent cache check boxes are selected.

- 6 Set the options for sharing saved information and changing the configuration settings load path.

You can choose to copy configuration information from the All Users account to your user account or copy your configuration information to the All Users account.

i NOTE: The Cache folder and the PersistantData.xml file are not shared in this process.

IMPORTANT: Folders and files are overwritten in this process. You may want to make copies of your original files before starting this process.

By default, the configuration folders and files of a user are saved to **C:\Users\<Current User>\AppData\Local\Quest\Security Explorer\9**. You can choose to change the location where your configuration folders and files are stored.

i NOTE: The mapping between each user and their specified config load path is saved to the UserConfigSettings.xml file located at **C:\ProgramData\Quest\Security Explorer\9**. When a user starts Security Explorer, this file is checked for a user-specific setting. If a specified config load path mapping is found, Security Explorer loads the configuration settings from the path specified in the UserConfigSettings.xml file. If a mapping is not found, Security Explorer uses the settings from the default path: **C:\Users\<Current User>\AppData\Local\Quest\Security Explorer\9**.

Table 13. Configuration information

Folders and files saved	Description
PersistentData.xml	User settings
BackupSavedTasks.xml	List of scheduled backups
ExportSavedTasks.xml	List of scheduled exports
SavedAccessManagerServers.xml	List of Access Explorer servers (<i>NTFS Security module only</i>)
SavedPermissionTemplates.xml	Saved Permission Templates (<i>NTFS Security module only</i>)
SavedSharePointSites.xml	Saved SharePoint farms and sites (<i>SharePoint Security module only</i>)
SavedLocations.xml	Favorites and Enterprise Scopes
Saved Searches folder	Saved searches for all modules

To share configuration information and change the configuration load path

- a Click **Advanced**.
- b Select how to share configuration information.
 - To copy configuration information from the All Users account to your account, leave the **Share information with all users** check box blank, and click **Copy Shared Data**.
 - To copy your configuration information to the All Users account, select the **Share information with all users** check box, and click **Copy User Specific Data**.
- c By default, the configuration information of a user is saved to **C:\Users\<Current User>\AppData\Local\Quest\Security Explorer\lv9**. To change the location, select the **Change config load path** check box, browse to select the new location, and click **OK**.
- d Click **OK**.
- e If you selected to change the config path, you are asked to confirm your selection. Click **Yes** to confirm.

7 Click **OK**.

Controlling access to Security Explorer

Use Security Explorer Role Based Management (SXPRoleBasedManagement.exe) to disable specific users from accessing a specific module. The module is hidden from the user.

i | **NOTE:** You must be a Domain Administrator or have the necessary permissions to manage domain groups to apply the changes.

Usage

SXPRoleBasedManagement

Select a module, and click **Add** to add users to the list. Once you click **Close**, those users are prevented from accessing the selected module the next time they start Security Explorer.

i | **NOTE:** The first time you use this command, a message box displays. Security Explorer must create a global domain group for each module, such as SXP_NTFS_Disabled. Once the groups are created, you can add users manually to these groups to prevent module access. See [Modifying group memberships](#).

Using the command line

Security Explorer® includes support for command line usage through separate programs that were copied to your install directory during the installation process. In addition, Security Explorer supports cmdlets for use with Windows PowerShell®.

i | **IMPORTANT:** All command utilities should be run while logged on as an Administrator. The Security Explorer cmdlets must be run as an administrator with elevated privileges (if UAC is enabled).

Topics:

- [Opening a command prompt window](#)
- [SxpBackup.exe](#)
- [SxpClone.exe](#)
- [SxpExport.exe](#)
- [SxpGrant.exe](#)
- [SxpHomeDir.exe](#)
- [SxpInheritance.exe](#)
- [SxpOwner.exe](#)
- [SxpRestore.exe](#)
- [SxpRevoke.exe](#)
- [SXPActiveDirectoryBackup](#)
- [SxpSearch.exe](#)

Opening a command prompt window


You can open a Command Prompt window directly from a selected folder.

i | **NOTE:** The Command Prompt function is available only in the NTFS Security module.

To open a command prompt window

- 1 Open the **NTFS Security** module.
- 2 In the Navigation or Objects pane, select a folder, and select **Tools | Command Prompt Here**.

-OR-

Click  on the Tool Bar; or right-click the folder, and select **Command Prompt Here**.

SxpBackup.exe

Back up permissions from the command line. See [Backing up security](#). You may wish to schedule regular backups through the schedule service or any other scheduling software. See [Scheduling a backup](#).

Usage

```
SXPBackup -backup -recurse -reparse -repair [wild card] [source path] [backup file]
```

<code>[-backup]</code>	Backup flag (compulsory argument)
<code>[-recurse]</code>	Recurse [recursion depth]
<code>[-reparse]</code>	Do *NOT* skip reparse points, not recommended (optional argument)
<code>[repair]</code>	Repair inheritance before backup flag (optional argument)
<code>[wild card]</code>	Wild card (eg *.*) (compulsory argument)
<code>[source path]</code>	Folder base path for backup (compulsory argument)
<code>[backup file]</code>	Path to the backup file (*.sec) (compulsory argument)

Note: Arguments must be supplied in the order specified above.

Examples

Back up \\Accounting\c\$ to c:\123.sec

```
SXPBackup.exe -backup *.* \\Accounting\c$ c:\123.sec
```

Back up \\Accounting\c\$ to c:\123.sec, recurse to depth 3, do not skip reparse points, and repair inheritance

```
SXPBackup.exe -backup -recurse 3 -reparse -repair *.* \\Accounting\c$ c:\123.sec
```

SxpClone.exe

Use to clone group or user permissions on a set of files and folders on the network. See [Cloning permissions](#).

Usage

```
SXPClone <options> <source user name> <destination user name> <source path>
```

<code>/?</code>	This help message
<code>/progress</code>	Show progress
<code>/replace</code>	Add/Replace flag (Replace=true, Add=false)
<code>/file</code>	Source path represents a file (default: folder)
<code>/force</code>	Clone protected objects
<code>/ownership</code>	Clone ownership of objects owned by source account

Return Codes

Success	= 0
Invalid arguments	= 1
Could not find account	= 2
Exception encountered	= 3 (*)
Errors detected	= 4 (during processing **)
Source path not found	= 5

(* The system error code will be returned when possible)

(** Error details will be displayed during processing if the correct argument is set)

Example

Clones the permissions for ACME\JSmith onto ACME\BJones on c:\Accounting

```
SXPClone.exe /progress ACME\JSmith ACME\BJones c:\Accounting
```

SxpExport.exe

You can export permissions on a folder to a Microsoft® Access® 2000 database (.mdb file) or to a delimited file for use with Microsoft® Excel®. Used in conjunction with any scheduling utility, you can export permissions to a database off hours automatically. See [Exporting security](#).

Usage

```
SXPExport <options> <source path> <destination file name>
/?                This help message
/s               Export to spreadsheet
/d               Export to database
/r               Generate report
/summary         Summary mode
/folders         Process folders
/files           Process files
/recurse         Recurse [recursion depth]
/all             Recurse all
/wildcard        Wildcard [wildcard characters]
/columns         Specify columns
/exclusion        Exclusion paths
/showprogress    Show detailed progress
/showgroupmembers Show group members [group members option]
/sqlite          Export to SQLite database
```

GROUP MEMBERS OPTIONS

- 1 Exclude nested groups and include 'Domain Users' group members
- 2 Exclude both nested groups and 'Domain Users' group members
- 3 Include both nested groups and 'Domain Users' group members
- 4 Include nested groups and exclude 'Domain Users' group members

Note: If using showgroupmembers then next argument must be group member option.

Note: /s /d or /r must be supplied

Note: If using /recurse then next argument must be recursion depth

Note: If using /wildcard then next argument must be wildcard characters

Note: If using /wildcard then wildcard should not include '*' (examples '.lic' and '.jpg')

Note: Summary mode will export folders and files only where their permissions differ from the parent.

Note: Command line progress updates are always displayed whenever a folder or file permission is written to the exported destination file. If the '/showprogress' argument is supplied then progress updates will also be displayed when a folder or file is processed. This is useful if you are exporting a large number of folders and files with summary mode enabled.

Note: Columns is only available when exporting to a spreadsheet or generating a report.

Note: If using columns then next argument must include column names separated by commas: /columns "Path,Is Container,Is Protected,Owner Domain,Owner Name,Allow

Deny,Inherited,Account Domain,Account Name,Permissions Text,Applies To,SID,Permissions Raw, Group Members, Conditional Expression"

Note: If using /exclusion, then next argument must include exclusion paths separated by commas. Enclose each path with double quotation marks. Do not end path with a backslash. (example "C:\Folder 1","C:\export-1.pdf")

Note: Use /sqlite with /d to export to a SQLite database. Use /d only to export to a Microsoft Access database.

Return Codes

Success = 0
Invalid arguments = 1
Could not find account = 2
Exception encountered = 3 (*)
Errors detected = 4 (during processing **)
Source path not found = 5
(* The system error code will be returned when possible)
(** Error details will be displayed during processing if the correct argument is set)

Examples

Exports all permissions on c:\Accounting

```
SXPExport.exe /s /folders /files /all c:\Accounting c:\Acct.csv
```

Exports the named columns to the test.csv spreadsheet

```
SXPExport.exe /s /columns "Path,Owner Domain,Owner Name,Allow Deny,Is  
Inherited,Account Domain,Account Name,Permissions Text,Applies To" c:\nn  
c:\Test\test.csv
```

Exports a report of all permissions excluding a specified folder and a file.

```
SXPExport.exe /r /folders /files /recurse /all /exclusion "C:\Accounting\personal",  
"C:\export-1.pdf"
```

Exports a report of permissions on the specified folder, excluding nested groups and including the group members of Domain Users

```
SXPExport.exe /r /folders /showgroupmembers 1 c:\nn c:\a.pdf
```

SxpGrant.exe

Grant group and user file permissions without affecting other user and group permissions while recursing across subfolders. See [Granting permissions](#).

Usage

SXPGrant <options> <user name> <source path>

/?	This help message
/progress	Show progress
/force	Force down tree
/overwrite	Overwrite permissions
/replace	Replace flag (default is add)
/deny	Deny flag (default is allow)
/noprop	No propagate
/noarch	Do not set archive attribute
/file	Source path represents a file (default: folder)
/perm	Permission [permission type] (default: full control)
/scope	Scope [scope type] (default: this folder, subfolders and files)

Permission Types

full	Full control
modify	Modify
readexecute	Read and execute
list	List folder contents
read	Read
write	Write

Scope Types

1	This folder only
2	This folder subfolders and files
3	This folder and subfolders
4	This folder and files
5	Subfolders and files only
6	Subfolders only
7	Files only

Note: If using /perm then next argument must be permission type

Note: If using /scope then next argument must be scope type

Return Codes

Success	= 0
Invalid arguments	= 1
Could not find account	= 2
Exception encountered	= 3 (*)
Errors detected	= 4 (during processing **)
Source path not found	= 5 (sxpgrant.exe only)

(* The system error code is returned when possible)

(** Error details display during processing if the correct argument is set)

Example

Grants a new full control permission to ACME\JSmith on c:\Accounting.

```
SXPGrant.exe /progress /perm full /scope 1 ACME\JSmith c:\Accounting
```

SxpHomeDir.exe

i | **TIP:** NTFS Security module only. You also can use the Home Directory advanced task to change permissions on a specified folder in a specified domain.

Usage

```
SXPHomeDir <options> /mode <mode> /domain <domain name> /path <path> /user  
<additional user - optional>
```

Mode

- A Removes all existing permissions, removes inheritance, grants full control for user (plus optional additional user)
- B Grants full control for user (plus optional additional user)

/?	This help message
/progress	Show progress
/recurse	Recurse all subfolders

Return Codes

```
Success = 0
Invalid arguments = 1
Could not find account = 2
Exception encountered = 3 (*)
Errors detected = 4 (during processing **)
Source path not found = 5 (sxpgrant.exe only)

(* The system error code will be returned when possible)
(** Error details will be displayed during processing if the correct argument is set)
```

Example

```
SXPHomeDir /progress /recurse /mode A /domain "DOMAIN" /path "\\SERVER\C$"
```

SxpInheritance.exe

Repairs the inheritance on the specified source path. See [Repairing inheritance](#).

i | NOTE: The process of repairing inheritance changes the permissions on the selected folder, subfolder, and file. Review the selected folder to verify that important permissions are not removed during the process.

Usage

```
SXPInheritance <options> <source path>

/?          This help message
/progress   Show progress
/file       Source path represents a file (default: folder)
/add        Add inheritance to specified path
/copy       Remove inheritance from specified path (and make
            inherited permissions explicit)
/remove     Remove inheritance from specified path
```

Return Codes

```
Success = 0
Invalid arguments = 1
Could not find account = 2
Exception encountered = 3 (*)
Errors detected = 4 (during processing **)

(* The system error code will be returned when possible)
(** Error details will be displayed during processing if the correct argument is set)
```

SxpOwner.exe

Set the owner an object. See [Setting ownership](#).

Usage

```
SXPOwner <options> <user name> <source path>

/?          This help message
```

```
/progress Show progress
/files      Process files
/folders    Process Folders
/recurse     Recurse subfolders and files
/wildcard Wildcard [wildcard characters]
```

Note: If using /wildcard then next argument must be wildcard characters

Note: If using /wildcard then wildcard should not include '*' (examples '.lic' and '.jpg')

Return Codes

```
Success                = 0
Invalid arguments      = 1
Could not find account = 2
Exception encountered  = 3 (*)
Errors detected        = 4 (during processing **)
(* The system error code will be returned when possible)
(** Error details will be displayed during processing if the correct argument
is set)
```

SxpRestore.exe

Restore a backup file. See [Restoring security](#).

Usage

SXPRestore <options> <source backup file>

```
/?          This help message
/progress   Show progress
/owner      Restore owner
/perm       Restore permissions
/missing    Restore missing folders
/alt        Restore to alternate location
```

Note: If using /alt then next argument must be alternate path

Return Codes

```
Success                = 0
Invalid arguments      = 1
Could not find account = 2
Exception encountered  = 3 (*)
Errors detected        = 4 (during processing **)

(* The system error code will be returned when possible)
(** Error details will be displayed during processing if the correct argument is
set)
```

SxpRevoke.exe

Revokes unknown or deleted accounts. See [Revoking permissions](#).

Usage

SXPRevoke <options> <source path>

```
/?           This help message
/progress    Show progress
/force       Force down tree
```

Return Codes

```
Success                = 0
Invalid arguments      = 1
Could not find account = 2
Exception encountered  = 3 (*)
Errors detected        = 4 (during processing **)
```

(* The system error code will be returned when possible)

(** Error details will be displayed during processing if the correct argument is set)

SXPActiveDirectoryBackup

Back up Active Directory permissions from the command line. See [Backing up security](#).

i | **NOTE:** Security Explorer does not support restoring Active Directory permissions from the command line. See [Restoring security](#).

Usage

SXPActiveDirectoryBackup <options> <source LDAP path> <target file name>

```
/progress          Show the progress of the backup
-nodatetimestamp   Do not add the date time as the prefix of the backup file
source LDAP path    LDAP path for backup (compulsory argument)
target file name    Path to the backup file (*.adb) (compulsory argument)
```

Example

```
SXPActiveDirectoryBackup.exe /progress -nodatetimestamp
"LDAP://erse.wm.zhu.cn.qsft/ OU=Zhuhai,DC=qasp,DC=wm,DC=zhu,DC=cn,DC=qsft"
c:\123.adb
```

Example

The command line can also support the file mode.

```
SXPActiveDirectoryBackup.exe /file c:\123.ini
```

SxpSearch.exe

Search for permissions from the command line. See [Searching](#). You may wish to schedule regular searches through the schedule service or any other scheduling software. See [Scheduling a search](#).

Usage

SXPSearch <options> <module name> <search definition file path> <report file name>

module name	NTFS, Shares, Registry, Printers, GroupsAndUsers, Exchange, SQL, SharePoint, or ActiveDirectory
search definition file path	An XML file that defines search scope and criteria. Export a saved search in GUI to create the XML file
report file name	Path to the report file (in PDF format) and a status file (<report file name>_status.txt)
/?	This help message
/progress	Show progress

Return Codes

Success	= 0
Invalid arguments	= 1
Could not find account	= 2
Exception encountered	= 3 (*)
Errors detected	= 4 (during processing **)
Source path not found	= 5
Search canceled	= 6

(* The system error code will be returned when possible)

(** Error details will be displayed during processing if the correct argument is set)

Example

Searches with the definition file JacksPermissionOfFolderA.xml, and saves result to c:\jacksFolderA.pdf along with a status file c:\jacksFolderA_status.txt.

```
SXPSearch.exe /showprogress NTFS c:\JacksPermissionOfFolderA.xml c:\jacksFolderA.pdf
```

Using PowerShell cmdlets

Microsoft® Windows PowerShell® is a Windows® command-line shell and scripting language designed specifically for system administrators and built on top of the Microsoft .NET Framework. Security Explorer supports the use of PowerShell cmdlets.

Topics:

- [What are cmdlets?](#)
- [Using Security Explorer cmdlets](#)
- [Using cmdlets to set up Access Explorer](#)
- [Using cmdlets to get information about Access Explorer objects](#)
- [Using cmdlets to manage Access Explorer agents](#)
- [Using cmdlets to remove Access Explorer objects](#)

What are cmdlets?

Windows PowerShell® has the concept of cmdlets. A cmdlet is a simple, single-function command that manipulates objects and is designed to be used in combination with other cmdlets.

If you already had Windows PowerShell installed on your computer before you installed Security Explorer, the Security Explorer cmdlets were automatically installed and registered with Windows PowerShell.

The examples in this section show you leverage the cmdlets available in Security Explorer. These cmdlets allow you to perform many of the functions of Security Explorer in an automation environment. The cmdlets also can be of great use in any environment where a repetitive process involving Security Explorer is needed.

This table lists the Access Explorer cmdlets included with Security Explorer.

Table 1. Access Explorer cmdlets for use with Windows PowerShell®

Cmdlet	Module	Reference
Add-AEManagedComputer	AccessExplorer	Adding managed computers
Add-AEManagedDomain	AccessExplorer	Adding a domain to manage
Add-AEServiceAccount	AccessExplorer	Adding a service account
Connect-AEService	AccessExplorer	Getting service account information
Export-AEResourceAccessAsCSV	AccessExplorer	Getting resource access information
Get-AEAccessibleComputersForAccount	AccessExplorer	
Get-AEAccountsForComputer	AccessExplorer	
Get-AEAgentInstances	AccessExplorer	Identifying agents on a managed computer
Get-AEDatabases	AccessExplorer	
Get-AEIndexedAccounts	AccessExplorer	
Get-AEIndexedComputers	AccessExplorer	

Table 1. Access Explorer cmdlets for use with Windows PowerShell®

Cmdlet	Module	Reference
Get-AEManagedComputers	AccessExplorer	Getting managed computer information
Get-AEManagedDomains	AccessExplorer	Getting managed domain information
Get-AEResourceAccess	AccessExplorer	Getting resource access information
Get-AEResourceSecurity	AccessExplorer	Getting security information for a resource
Get-AEServiceAccounts	AccessExplorer	Getting service account information
Get-AEServiceConnectionPoints	AccessExplorer	
Remove-AEManagedComputer	AccessExplorer	Removing a managed computer
Remove-AEManagedDomain	AccessExplorer	Removing a managed domain
Remove-AEServiceAccount	AccessExplorer	Removing a service account
Restart-AEAgent	AccessExplorer	Restarting the agent
Restart-AEAgentForComputer	AccessExplorer	Restarting a single agent
Set-AEAccountPassword	AccessExplorer	Changing the service account password
Set-AEAgentConfiguration	AccessExplorer	Changing the agent configuration on a managed computer
Set-AEDatabase	AccessExplorer	Creating the Access Explorer database
Set-AEDBAccessAccount	AccessExplorer	Changing the SQL account password
Update-AEAgent	Access Explorer	Updating an agent

Using Security Explorer cmdlets

i | IMPORTANT: All command utilities should be run while logged on as an Administrator. The Security Explorer® cmdlets must be run as an administrator with elevated privileges (if UAC is enabled). The Security Explorer cmdlets should be used only by those familiar with Windows PowerShell®.

The Security Explorer cmdlets function very similarly to the included command utilities. You can view help by typing the cmdlet name with no arguments or by typing `get-help set-sxpbackup`.

To use the Security Explorer cmdlets, you must create or edit the PowerShell.exe.config file, and install the cmdlets.

Topics:

- [Creating or editing the PowerShell.exe.config file](#)
- [Installing Security Explorer cmdlets](#)
- [Installing Security Explorer cmdlets manually](#)
- [Removing Security Explorer cmdlets](#)

Creating or editing the PowerShell.exe.config file

PowerShell.exe.config is found at:

- Windows® 64 bit: %SystemRoot%\SysWOW64\WindowsPowerShell\v1.0

- Windows 32 bit: %SystemRoot%\system32\WindowsPowerShell\v1.0

Create or edit the file as follows:

```
<?xml version="1.0"?>
<configuration>
  <startup
    useLegacyV2RuntimeActivationPolicy="true">
      <supportedRuntime version="v4.0.30319"/>
      <supportedRuntime version="v2.0.50727"/>
    </startup>
  </configuration>
```

Installing Security Explorer cmdlets

If the script execution policy on your system prevents the execution of SXPPowerShellControl.exe, which is used to install Security Explorer cmdlets, you need to install the DLLs manually. See [Installing Security Explorer cmdlets manually](#).

NOTE: Before using the Security Explorer cmdlets, you must start Security Explorer at least once to implement and check licensing.

To install Security Explorer cmdlets

- Click **Start**, point to **Programs | Quest | Security Explorer | PowerShell | Run PowerShell**. A message appears explaining that if the attempt to add the cmdlets fails, you need to add them manually.

Installing Security Explorer cmdlets manually

The install command line will vary according to whether you are working with Windows PowerShell® 1 or Windows PowerShell® 2. The following instructions are for working with Windows PowerShell 1. If you are working with Windows PowerShell 2, adjust the command text accordingly.

To install Security Explorer cmdlets manually

- 1 Open Windows PowerShell.
- 2 Change the directory to where Security Explorer is installed, which is normally:

```
cd C:\Program Files\Quest\Security Explorer
```

- 3 Install the cmdlets.

If you are running the **32-bit version of Windows PowerShell**, type:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe
SXPEExchangePowerShell9.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe
SXPNtfsPowerShell9.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe
SXPSharePointPowerShell9.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe
SXPSharesPowerShell9.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe
SXPSqlPowerShell9.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe '.\Access
Explorer\Quest.AccessExplorer.Powershell.dll'
```

If you are running the **64-bit version of Windows PowerShell**, type:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\installutil.exe
SXPEExchangePowerShell9.dll
```

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\installutil.exe
SXPNTfsPowerShell9.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\installutil.exe
SXPSharePointPowerShell9.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\installutil.exe
SXPSharesPowerShell9.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\installutil.exe
SXPSqlPowerShell9.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\installutil.exe '.\Access
Explorer\Quest.AccessExplorer.Powershell.dll'
```

4 To register the snap-ins, type:

```
add-pssnapin SXPEExchangePowerShell9
add-pssnapin SXPNTfsPowerShell9
add-pssnapin SXPSharePointPowerShell9
add-pssnapin SXPSharesPowerShell9
add-pssnapin SXPSqlPowerShell9
add-pssnapin Quest.AccessExplorer.Powershell
```

Removing Security Explorer cmdlets

To remove Security Explorer cmdlets

- Click **Start**, point to **Programs | Quest | Security Explorer | PowerShell | Uninstall Security Explorer PowerShell Plugins**.

Using cmdlets to set up Access Explorer

Before Access Explorer can be used to manage computers or servers, you must at least create a service account, create a database, and add a domain.

This section contains the following topics:

- [Creating the Access Explorer database](#)
- [Adding a service account](#)
- [Adding a domain to manage](#)
- [Adding managed computers](#)

Creating the Access Explorer database

The Access Explorer database stores all the data that Access Explorer needs to manage computers and servers.

Syntax

```
Set-AEDatabase [-DatabaseServer] <String> [-DatabaseName] <String> [-
DatabaseAccount] <String> [-DatabaseAccountPassword] <SecureString> [[-
ConnectToExistingDatabase] [<SwitchParameter>]]
```

Example

In this example, the first step encrypts the password used by the service account before sending it across the network. Next, the database used by Access Explorer is created on the SQL Server identified in the DatabaseServer parameter and given the name dbReporter_AccessExplorer, which is the default name provided when creating a database in Access Explorer. The service account used to create the database needs to have permission to create and access the database. If the cmdlet creates the database successfully, Operation Complete is returned.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force  
Set-AEDatabase -DatabaseServer AMERGEN01 -DatabaseName dbReporter_AccessExplorer -  
DatabaseAccount AMER\Administrator -DatabaseAccountPassword $secpasswd
```

Adding a service account

A service account is used to access the database, install agents, and access domains. The service account needs the necessary credentials to create the SQL Server database.

Syntax

```
Add-AEServiceAccount [-AccountDomain] <String> [-AccountName] <String> [-Password]  
<SecureString> [[-IsDefaultObjectResolution] [<Boolean>]]
```

Example

This example involves a two-step process. The first step encrypts the password used by the service account before sending it across the network. The second step supplies the password, along with the domain and the account for that domain.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force  
Add-AEServiceAccount -AccountDomain AMER1 -AccountName Administrator -Password  
$secpasswd
```

Adding a domain to manage

The next main step to setting up Access Explorer is to add a managed domain. You can manage any domain that your service account can access, including a remote domain. A trust needs to be established between domains and it is useful to have a service account in the trusted domain that you add to Access Explorer.

You need the ID of the service account to add a managed domain. For more information, see [Adding a domain to manage](#).

Syntax

```
Add-AEManagedDomain [-DomainName] <String> [-ServiceAccountId]
```

Example 1

In this example, a managed domain is added to Access Explorer. Use the Get-AEServiceAccounts cmdlet to obtain the value for the ServiceAccountId parameter. Make sure the service account belongs to the domain specified by the DomainName parameter.

```
Add-AEManagedDomain -DomainName AMER -ServiceAccountId ca94cd34-7c83-46ed-8f7d-  
34af19b98a1e
```

Example 2

In this example, a new trusted domain is added to Access Explorer. First, a password is created and stored in the \$secpasswd variable. Next, a service account with the password stored in the \$secpasswd variable is added for

the AMER1 domain. Next, the Get-AEServiceAccounts cmdlet is used to return the ID for the service account. Finally, the AMER1 domain is added.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force

Add-AEServiceAccount -AccountDomain AMER1 -AccountName Administrator -Password
$secpasswd

Get-AEServiceAccounts
ServiceAccountId      : 0602bedd-b081-45e2-92cf-44ed8cb3b374
AccountSid            : S-1-5-21-102124880-1633684138-1207526451-500
UserDomainName        : AMER1
UserName              : Administrator

Add-AEManagedDomain -DomainName AMER1 -ServiceAccountId 0602bedd-b081-45e2-92cf-
44ed8cb3b374
```

Adding managed computers

Once the service accounts, domain, and database are created, you can add managed computers so data can be retrieved. The data can be seen in the Report Manager on the Explorer tab, or you can use a cmdlet to retrieve data for a specific share, folder, or file.

The cmdlet for adding a managed computer has several parameters, but we will show the minimum you need to accomplish the task.

Syntax

```
Add-AEManagedComputer [-ComputerAccountName] <String> [[-Keyword] <String>] [[-
DeploymentType] <DeploymentMethodType>] [[-ResourceActivityEnabled]
[<SwitchParameter>]] [[-Granularity] <Int32>] [[-ExcludedTrusteesImportFile]
<String>] [[-ExcludedFileTypesImportFile] <String>] [[-ExcludedFoldersImportFile]
<String>] [[-AgentHostName] <String>] [[-SelectedDataRoots] <List`1[String]>] [[-
ScheduleType] <AgentInfo+DataRootScanSchedule+ScanScheduleType>] [[-ScheduledDays]
<List`1[String]>] [[-ScheduledTime] <String>] [[-ScanInterval] <Int32>] [[-
ServiceAccountId] <String>] [[-EnableRemoteFileSystemChangeWatching]
[<SwitchParameter>]] [[-PerformImmediateScanOnWatchError] [<SwitchParameter>]] [[-
OverrideScanScheduleOnStartup] [<SwitchParameter>]] [[-AccountNameSpecifiedIsSID]
[<SwitchParameter>]] [[-AgentHostNameSpecifiedIsSID] [<SwitchParameter>]]
```

Example

This example deploys an agent to the AMERGENDC server with a deployment type of ManagementServerInstall, which automatically deploys an agent. The other deployment type, External, marks the managed computer as requiring an external agent installation. In most cases you will want to deploy as ManagementServerInstall.

All of the other parameters are not necessary and the default setting for those options (parameters) are correct for a normal install of the agent on the managed computer. In this case with a local install, all of the files (data roots) on the managed computer will be scanned for file access permission, which is the normal setting if done using **Configuration Manager | Access Explorer | Manage Computers**.

```
Add-AEManagedComputer -ComputerAccountName AMERGENDC -DeploymentType
ManagementServerInstall
```

Using cmdlets to get information about Access Explorer objects

Most of the parameters used by Access Explorer cmdlets are identifications or IDs. To aid you in getting these IDs, there are of Get cmdlets that return the ID in a GUID format that you use in other cmdlets.

Topics:

- [Getting service account information](#)
- [Getting managed domain information](#)
- [Getting managed computer information](#)
- [Getting security information for a resource](#)
- [Getting resource access information](#)

Getting service account information

You need the service account ID to add a managed domain. The `Get-AEServiceAccount` cmdlet returns the information for all of the service accounts that are available.

Syntax

```
Get-AEServiceAccounts
```

Example

```
Get-AEServiceAccounts
```

Output

```
ServiceAccountId      : 9787f160-56e1-4095-88c2-51ae62a60f78
AccountSid            : S-1-5-21-3504372180-144029308-885861804-500
UserDomainName        : AMER
UserName              : Administrator
UserPrincipalName      : Administrator@AMER.amer.sitraka.com
Description            :
IsDefaultObjectResolution : True
StatusDetailMessage    :
Status                : OK
CanManageDomains       : True
ServiceAccountName     : AMER\Administrator
```

Getting managed domain information

The `Get-AEManagedDomains` cmdlet returns information for all managed domains, along with the name of the service account used to access the domain.

Syntax

```
Get-AEManagedDomains
```

Example

In this example, information for all managed domains is returned. In addition to the managed domain ID, you also get the ID for the service account, which is used as input for other cmdlets.

```
Get-AEManagedDomains
```

Output

```
ManagedDomainId      : 9d95d834-0b13-4ada-b42d-981261a96560
DomainDnsName         : AMER.amer.sitraka.com
ForestDnsName         : AMER.amer.sitraka.com
Status                : OK
NetbiosName           : AMER
DomainSid              : S-1-5-21-3504372180-144029308-885861804
ServiceAccountId      : ca94cd34-7c83-46ed-8f7d-34af19b98a1e
AccessGroupSid        : S-1-5-21-3504372180-144029308-885861804-1
ServiceAccountInfo    : AMER\Administrator
DomainControllerName  :
ExtendedRightsCreated : False
ServiceConnectionPointsCreated : True
```

Getting managed computer information

Now that there is a managed computer you will want to know the status of the agent and the identification for the managed computer.

An important field to note in the output is the Status field as it provides information as to the status of the agent. For example, if you see the Status is still reporting DeployingAgent 15 minutes after you deployed the agent, then something is wrong as deployment should only take a few minutes.

Syntax

```
Get-AEManagedComputers [-ManagedComputerName <String>] [-ManagedComputerId <String>]
```

Examples

In this example, because a managed computer is not specified, the cmdlet returns information on all managed computers.

```
Get-AEManagedComputers
```

Output

```
Agents                : {AMER\AMERGENDC S-1-5-21-3504372180-144029308-885861804-1001}
ManagedHostId        : f13a510b-dc5d-43f6-815b-0020f3da275d
ManagedHostSid       : S-1-5-21-3504372180-144029308-885861804-1001
ComputerSamSid        :
ManagedDomainId      : da4e1710-f80b-4fc5-84fb-2582f9519995
HostName              : AMERGENDC
SamAccountName        : AMERGENDC
HostDnsName           : AMERGENDC.AMER.amer.sitraka.com
HostDomainName        : amer.amer.sitraka.com
SiteName              :
HostType              : 1
Management            : Local
Features              : 0
Status                : DeployingAgent
InternalStatus        : Ok
ResourceNodeId        : 3
Keywords              :
ResourceActivityTrackingSupported : True
```

Example 2

In this example, a managed computer is specified, so the cmdlet returns information on only the AMERGENDC managed computer.

```
Get-AEManagedComputers -ManagedComputerName AMERGENDC
```

Output

```
Agents                : {AMER\AMERGENDC S-1-5-21-3504372180-144029308-885861804-1001}
```

```

ManagedHostId          : f13a510b-dc5d-43f6-815b-0020f3da275d
ManagedHostSid         : S-1-5-21-3504372180-144029308-885861804-1001
ComputerSamSid          : S-1-5-21-2573059503-884258253-2950429726
ManagedDomainId       : da4e1710-f80b-4fc5-84fb-2582f9519995
HostName                : AMERGENDC
SamAccountName          : AMERGENDC
HostDnsName             : AMERGENDC.AMER.amer.sitraka.com
HostDomainName          : amer.amer.sitraka.com
SiteName                :
HostType                : 1
Management              : Local
Features                : 0
Status                  : Ok
InternalStatus          : Ok
ResourceNodeId          : 3
Keywords                :
ResourceActivityTrackingSupported : True

```

Example 3

In this example, information about the managed computer specified by the ManagedComputerId (also known as the ManagedHostId) is returned.

```
Get-AEManagedComputers -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Output

```

Agents                  : {AMER\AMERGENDC S-1-5-21-3504372180-144029308-885861804-1001}
ManagedHostId          : f13a510b-dc5d-43f6-815b-0020f3da275d
ManagedHostSid         : S-1-5-21-3504372180-144029308-885861804-1001
ComputerSamSid          : S-1-5-21-2573059503-884258253-2950429726
ManagedDomainId       : da4e1710-f80b-4fc5-84fb-2582f9519995
HostName                : AMERGENDC
SamAccountName          : AMERGENDC
HostDnsName             : AMERGENDC.AMER.amer.sitraka.com
HostDomainName          : amer.amer.sitraka.com
SiteName                :
HostType                : 1
Management              : Local
Features                : 0
Status                  : Ok
InternalStatus          : Ok
ResourceNodeId          : 3
Keywords                :
ResourceActivityTrackingSupported : True

```

Getting security information for a resource

All of the components needed for Access Explorer are now in place so now you can start to retrieve security information in the form of the ACL (access control list) about specific resources (shares, folders, and files) on your managed computers. The resource in question is to be in the format `\\computer\share\folder\file.ext` and wild characters are not permitted. Note that the cmdlet requires not only the computer name, but also the domain in which the computer resides, because the service account for the domain is needed to access the resource.

Syntax

```
Get-AEResourceSecurity [-ResourceUri] <String> [-ResType] <String> [-DomainDNSName] <String>
```

Example

In this example, the cmdlet returns the ACL for the file specified in the ResourceUri parameter.

```
Get-AEResourceSecurity -ResourceUri \\AMERGENDC\files\SmallClassDataset\test4.txt -
ResType Files -DomainDNSName AMER.amer.sitraka.com
```

Output

```

O:BAG:DUD:AI (A;ID;FA;;;S-1-5-21-3504372180-144029308-885861804-1106)
(A;ID;FA;;;SY) (A;ID;FA;;;BA) (A;ID;0x1200a9;;;BU)

```

Example 2

In this example, the cmdlet returns the ACL for the folder specified in the ResourceUri parameter.

```
Get-AEResourceSecurity -ResourceUri \\AMERGENDC\files\SmallClassDataset -ResType Folders -DomainDNSName AMER.amer.sitraka.com
```

Output

```
O:BAG:DUD:AI (A;OICI;FA;;;S-1-5-21-3504372180-144029308-885861804-1106) (A;OICIID;FA;;;SY) (A;OICIID;FA;;;BA) (A;OICIID;0x1200a9;;;BU) (A;CIID;LC;;;BU) (A;CIID;DC;;;BU) (A;OICIIOID;GA;;;CO)
```

Example 3

In this example, the cmdlet returns the ACL for the share specified in the ResourceUri parameter.

```
Get-AEResourceSecurity -ResourceUri \\AMERGENDC\Files -ResType Shares -DomainDNSName AMER.amer.sitraka.com
```

Output

```
D: (A;;;FA;;;WD)
```

Getting resource access information

In addition to the security information ACL for a resource, you also can get information on who currently has access to the resource. Since the information obtained by the Get-AEResourceAccess cmdlet cannot be read from the command line, you must use the Export-AEResourceAccessAsCSV cmdlet to export the information to a CSV file.

Exporting access information to a CSV file

Syntax

```
Export-AEResourceAccessAsCSV [-ResourceAccessResults] <ResourceAccessQueryResults> [-OutputPath] <String> [[-DisplayInheritedSecurity] [<SwitchParameter>]] [[-OptimizeForExcel] [<SwitchParameter>]]
```

Example

In this example as this cmdlet works in conjunction with the cmdlet used to get access information the first thing and not shown here, is to get some information on a resource stored into a variable, \$resourceAccess. The variable is then piped into the Export-AEResourceAccessAsCSV, which outputs the CSV file. In this case the variable is used as an input parameter for the cmdlet and CSV file is optimized for Excel.

```
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath "C:\ResourceAccessInfo.csv"
Export-AEResourceAccessAsCSV -ResourceAccessResults $resourceAccess -OutputPath "C:\ResourceAccessInfo.csv" -OptimizeForExcel
```

Syntax

Now that you have seen how to get the information out to a file in any location you wish, let's look at how to get the access information for a resource. With the cmdlet used to get the access information you can retrieve file, folder, share, and service identity rights.

```
Get-AEResourceAccess [-ManagedComputerId] <String> [-ResourceType] <ResourceAccessQueryResourceType> [[-Resources] <String[]>] [-ExcludeSubObjectDeviations [<SwitchParameter>]]
```


Example 3

In this example, the `Get-AEResourceAccess` cmdlet gets resource access (folder security) for the folder `SmallClassDataset` that resides on a locally managed computer with the id `f13a510b-dc5d-43f6-815b-0020f3da275d`. The results are saved to the `$resourceAccess` variable, which is then exported to a file using the `Export-AEResourceAccessAsCSV` cmdlet.

```
$resourceAccess = Get-AEResourceAccess -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d -ResourceType Folder -Resources \\AMERGENDC\Files\SmallClassDataset -ExcludeSubObjectDeviations
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath "C:\ResourceAccessInfo.csv"
```

Example

In this example, resource access (folder security) is obtained for two folders, `\\AMERGENDC\C$\Test1` and `\\AMERGENDC\C$\Test2`, that are located on a remotely managed computer with the ID `973c7042-c413-45fb-9f52-057c64d4f800`. The results are placed in the `$resourceAccess` variable and exported to a CSV file using the `Export-AEResourceAccess` cmdlet.

```
$resourceAccess = Get-AEResourceAccess 973c7042-c413-45fb-9f52-057c64d4f800 Folder "\\AMERGENDC\C$\Test1", "\\AMERGENDC\C$\Test2"
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath "C:\ResourceAccessInfo.csv"
```

Example

In this example, resource access (share security) is obtained for the share, `Files`, that is located on a managed computer with the ID `f13a510b-dc5d-43f6-815b-0020f3da275d`. The results are placed in the `$resourceAccess` variable and exported to a CSV file using the `Export-AEResourceAccessAsCSV` cmdlet.

```
$resourceAccess = Get-AEResourceAccess -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d -ResourceType Share -Resources "Files"
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath "C:\ResourceAccessInfo.csv"
```

Example

In this example, resource access (security identities) is obtained for the services, `TermService` (Remote Desktop Services) and `SessionEnv` (Remote Desktop Configuration), that are located on a managed computer with the ID `f13a510b-dc5d-43f6-815b-0020f3da275d`. The results are placed in the `$resourceAccess` variable and exported to a CSV file using the `Export-AEResourceAccessAsCSV` cmdlet.

```
$resourceAccess = Get-AEResourceAccess -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d -ResourceType ServiceIdentity -Resources TermService, SessionEnv
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath "C:\ResourceAccessInfo.csv"
```

Output of the `Export-AEResourceAccessAsCSV` cmdlet

The following is an example of the information in an output CSV file from the `Export-AEResourceAccessAsCSV` cmdlet.

```
*****
Resource Access Report (CSV Format)
*****

"C:\Files - dummy files for scanning\SmallClassDataset"
"Uri","C:\Files - dummy files for scanning\SmallClassDataset",
"DisplayName","",
"ResourceType","NTFS\Folder",
DataRoot,"True"
ParentUri,""

TrusteeName,TrusteeSid,TrusteeType,"Rights","RightType","Inheritance","AppliesTo","Explicit",
"CREATOR OWNER","S-1-3-0","WellKnownGroup","Full Control","Allow Access","Inherited","Subfolders and Files Only","False",
"NT AUTHORITY\SYSTEM","S-1-5-18","WellKnownGroup","Full Control","Allow Access","Inherited","This Folder, Subfolders, and Files","False",
```

```
"RPTCH\ABARCAK", "S-1-5-21-3504372180-144029308-885861804-1106", "User", "Full Control", "Allow
Access", "Explicit", "This Folder, Subfolders, and Files", "True",
"BUILTIN\Administrators", "S-1-5-32-544", "Alias", "Full Control", "Allow Access", "Inherited", "This Folder,
Subfolders, and Files", "False",
"BUILTIN\Users", "S-1-5-32-545", "Alias", "Create Files / Write Data", "Allow Access", "Inherited", "This Folder
and Subfolders", "False",
"BUILTIN\Users", "S-1-5-32-545", "Alias", "Create Folders / Append Data", "Allow Access", "Inherited", "This
Folder and Subfolders", "False",
"BUILTIN\Users", "S-1-5-32-545", "Alias", "Read And Execute", "Allow Access", "Inherited", "This Folder,
Subfolders, and Files", "False",
*****End*****
```

Using cmdlets to manage Access Explorer agents

You use Security Explorer to install the Access Explorer agents, but you can manage the installed agents using the Access Explorer cmdlets.

Topics:

- [Identifying agents on a managed computer](#)
- [Changing the agent configuration on a managed computer](#)
- [Restarting the agent](#)
- [Updating an agent](#)
- [Changing the service account password](#)
- [Changing the SQL account password](#)

Identifying agents on a managed computer

A managed computer may have more than one agent installed on it. Not only could there be a local agent, there could be an agent for a remote computer, or an agent for a Net-App server or a cluster. The Get-AEAgentInstances cmdlet finds all agent instances registered with Security Explorer Access Explorer. A filter can be specified to retrieve agent instance information for only a single hosting system. Only managed computers with at least one agent instance (either local or remote) are returned. Note that the computers returned by this cmdlet are not the same as managed hosts; they are the computers that physically host the agent service.

Syntax

```
Get-AEAgentInstances [[-HostingSystem] <String>]
```

Example 1

In this example, the cmdlet returns the agents installed on the managed computer identified in the HostingSystem parameter.

```
Get-AEAgentInstances -HostingSystem AMERGENDC.AMER.amer.sitraka.com
```

Output

AgentComputer	AgentComputerDnsName	RecommendedAgentInstanceCap	Agents
AMER\AMERGENDC	AMERGENDC.AMER.amer.sitraka.com	20	{AMER\AMERGENDC S-1-5-21-35...

Example 2

In this example, the cmdlet returns all managed computers with their installed agents.

```
Get-AEAgentInstances
```

Output

AgentComputer	AgentComputerDnsName	RecommendedAgentInstanceCap	Agents
AMER\AMERGENDC	AMERGENDC.AMER.amer.sitraka.com		20 {AMER\AMERGENDC S-1-5-21-35...
AMER\AMERGEN02	AMERGEN02.AMER.amer.sitraka.com		20 {AMER\AMERGEN02 S-1-5-21-3...

Example 3

In this example, we look at how to expand the information returned by the `Get-AEAgentInstances` cmdlet as it is used in other cmdlets, such as the `Restart-AEAgent` cmdlet. To use the `Restart-AEAgent` cmdlet to restart an agent on a computer, you need to specify the Agent ID.

The first line stores information on the agent in the `$a` variable. The second line displays the information stored in the `$a.agents` property, which is where you find the agent Id, `BW_aaabd11494ed4f19921a91b92ee0979d`, that you need for the `Restart-AEAgent` cmdlet.

The `$a | Get-Member` (in the example output) displays the member types available for the data returned by `Get-AEAgentInstances` cmdlet.

```
$a = Get-AEAgentInstances -HostingSystem AMERGENDC.AMER.amer.sitraka.com
$a.agents
```

Output

```
Id : BW_aaabd11494ed4f19921a91b92ee0979d
ManagedHostId : f13a510b-dc5d-43f6-815b-0020f3da275d
Management : Local
AgentComputer : AMER\AMERGENDC
AgentComputerDnsName : AMERGENDC.AMER.amer.sitraka.com
AgentComputerActiveDirectorySid : S-1-5-21-3504372180-144029308-885861804-1001
AgentComputerManagedDomainId : da4e1710-f80b-4fc5-84fb-2582f9519995
AgentDetails : Quest.Broadway.Common.Interfaces.AgentDetails
UserNotes :
ServiceAccountId : 00000000-0000-0000-0000-000000000000
IsPrimaryAgent : True
ScanSchedule : Quest.Broadway.Common.Interfaces.AgentInfo+DataRootScanSchedule
DataRoots : {Quest.Broadway.Common.Interfaces.AgentInfo+DataRoot}
ConfigurationSettings :
ScannerStates : {NTFS : NamespaceState_DatasetComplete, Service Identities
NamespaceState_DatasetComplete, Windows Computer :
NamespaceState_DatasetComplete}
EnableRemoteFileSystemChangeWatching : False
PerformImmediateScanOnWatchError : True
OverrideScanScheduleOnStartup : False
UsageConfiguration : Quest.Broadway.Common.Interfaces.ResourceUsageConfiguration
QceeServers :
```

```
$a | Get-Member
```

```
TypeName: Quest.Broadway.Common.Interfaces.AgentHostInfo
```

Name	MemberType	Definition
Equals	Method	bool Equals(System.Object obj)
GetHashCode	Method	int GetHashCode()
GetType	Method	type GetType()
ToString	Method	string ToString()
AgentComputer	Property	string AgentComputer {get;set;}
AgentComputerDnsName	Property	string AgentComputerDnsName {get;set;}
Agents	Property	
System.Collections.Generic.List[Quest.Broadway.Common.Interfaces.AgentInfo]		A...
RecommendedAgentInstanceCap	Property	int RecommendedAgentInstanceCap {get;set;}

Changing the agent configuration on a managed computer

At some point you may want to look at specific folders and files on a managed computer. The data roots for the agent can be changed with an `Access Explorer` cmdlet. Note that the cmdlet overwrites the current data roots selection, so if you are already scanning a folder called `Files1`, and you want to include a folder called `Files2`, you cannot just add the new folder with the cmdlet. You need to specify both `Files 1` and `Files 2` in the cmdlet. Also the

ID for the agent is required, which can be found using the Get-AEAgentInstances cmdlet. For more information, see [Identifying agents on a managed computer](#).

Syntax

```
Set-AEAgentConfiguration [-AgentId] <String> [-DataRoots <List`1[String]>] [-ManagedComputerId <String>]
```

Example 1

In this example, the agent with the ID BW_aaabd11494ed4f19921a91b92ee0979d is set to another location for the data roots selection. Any previous setting will be removed as this cmdlet does not add a new data root location, but replaces the current one. Because the managed host ID is provided, the cmdlet does not need to search all of the deployed agent to see if any match the one provided.

```
Set-AEAgentConfiguration -AgentId BW_aaabd11494ed4f19921a91b92ee0979d -DataRoots "\\AMERGENDC\C$\Photos" -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Example 2

In this example, three separate folders on the C:\ Drive are selected for the data roots settings. You can add any number of folders as long as they are separated by a comma. Note that the data root locations are enclosed in quotation marks. The first two data root locations do not need the quotation marks, but the third one does as it contains spaces. It is a good habit to enclose all items like this in quotation marks whether they need them or not.

```
Set-AEAgentConfiguration -AgentId BW_aaabd11494ed4f19921a91b92ee0979d -DataRoots "\\AMERGENDC\C$\Photos", "\\AMERGENDC\C$\BGinfo", "\\AMERGENDC\C$\Documents and Settings" -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Example 3

In this example, the complete C:\ drive is being set as the data root.

```
Set-AEAgentConfiguration -AgentId BW_aaabd11494ed4f19921a91b92ee0979d -DataRoots "\\AMERGENDC\C$" -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Restarting the agent

There are two cmdlets that allow you to restart a single agent or restart all the agents on a managed computer.

Restarting a single agent

The restart operations for the specified agent instances are performed asynchronously by the management server. This cmdlet will not wait for the service restart operations to complete before returning.

Syntax

```
Restart-AEAgent [-AgentId] <AgentId>
```

Example

The agent with the ID BW_aaabd11494ed4f19921a91b92ee0979d is restarted. Use the Get-AEAgentInstances cmdlet to obtain the agent Id for the AgentId parameter. This cmdlet does not return any values.

```
Restart-AEAgent BW_aaabd11494ed4f19921a91b92ee0979d
```

Restarting all agents

Restart operations for the agent instances associated with the specified managed computer are performed asynchronously by the management server. This cmdlet will not wait for the service restart operations to complete before returning.

Syntax

```
Restart-AEAgentForComputer [-ManagedComputerId] <Guid>
```

Example

The agent on the managed computer with the ID 33bf3e5b-5edf-4b28-9eee-7fff84de2bca is restarted. Use the Get-AEManagedComputers cmdlet to obtain the value for the ManagedComputerId parameter. This cmdlet does not return any values.

```
Restart-AEAgentForComputer -ManagedComputerId
```

Updating an agent

There are times when an agent update may be required or may be available. An update can be performed with a cmdlet.

Syntax

```
Update-AEAgent [-AgentId] <AgentId>
```

Example

This example updates the agent specified if there is an agent update available. See the Get-AEAgentInstances cmdlet on how to get the agent Id for the AgentId parameter.

```
Update-AEAgent -AgentId BW_b0c49eb3f8364a37b56be1a92e0deba4
```

Changing the service account password

You may have a requirement to change the password for an account on a regular basis for security purposes. Changing the password for the service account can be done using a cmdlet. In addition you have the option of also re-synchronizing the agents with the new password.

Syntax

```
Set-AEAccountPassword [-AccountName] <String> [-Password] <SecureString> [[-Resynchronize] [<SwitchParameter>]]
```

Example 1

In this example, the first command secures the password to the \$secpasswd variable. The second command applies the new password to the service account.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force
Set-AEAccountPassword -AccountName AMER\Administrator $secpasswd
```

Example 2

In this example, the password is resynchronized on the agents associated with the service account.

```
Set-AEAccountPassword -Resynchronize
```

Changing the SQL account password

As with changing the password for the service account, you can change both the account and password used by the Security Explorer Access Explorer server to communicate with the SQL Server database.

Syntax

```
Set-AEDBAccessAccount [-DomainName] <String> [-AccountName] <String> [-Password]
<SecureString>
```

Example

In this example, a service account is added to the AMER domain with the password stored in the \$secpasswd variable.

```
Set-AEDBAccessAccount -DomainName AMER -AccountName Administrator -Password
$secpasswd
```

Using cmdlets to remove Access Explorer objects

There are a number of cmdlets that allow you to remove objects, such as service account, domains and managed computers, from Access Explorer.

Topics:

- [Removing a managed computer](#)
- [Removing a managed domain](#)
- [Removing a service account](#)

Removing a managed computer

To remove a managed computer that is no longer required, use the Remove-AEManagedComputer cmdlet. First all agents installed on the computer are removed, and then the computer is removed from Access Explorer. When unregistered, any agent instances associated with the managed computer are removed. If the computer does not have any agent instances, the Security Explorer Access Explorer agent software is removed.

Syntax

```
Remove-AEManagedComputer [-ManagedComputerId] <String>
```

Example

In this example, the computer with the Id 6e1f518f-cc9a-4915-86e5-894f47767556 is removed as a managed computer.

```
Remove-AEManagedComputer -ManagedComputerId 6e1f518f-cc9a-4915-86e5-894f47767556
```

Removing a managed domain

Once domains are no longer required in Access Explorer, they can be removed. Only domains which do not contain any registered managed Computers can be removed. Note that the Forest will not be removed with this cmdlet. Remove the Forest using Configuration Manager | Access Explorer | Configuration | Managed Domains.

Syntax

```
Remove-AEManagedDomain [-ManagedDomainId] <String>
```

Example

In this example, the domain with the Id 422dcede-3314-4d6c-9f8d-27abc65ada72 is removed. The forest is not removed

```
Remove-AEManagedDomain -ManagedDomainId 422dcede-3314-4d6c-9f8d-27abc65ada72
```

Removing a service account

The Remove-AEServiceAccount cmdlet removes the specified service account from the list of registered service accounts. To retrieve the ID of the service account, use the Get-AEManagedDomains or Get-AEServiceAccounts cmdlets. Only service accounts that are no longer referenced by managed domains and registered forests can be removed.

Syntax

```
Remove-AEServiceAccount [-ServiceAccountId] <String>
```

Example

In this example, the service account with the Id f0bafac5-46c3-4c52-a28b-6fdf5eb0a3b1 is removed.

```
Remove-AEServiceAccount -ServiceAccountId f0bafac5-46c3-4c52-a28b-6fdf5eb0a3b1
```

Troubleshooting

- [Repairing inheritance](#)
- [Creating test folders and files](#)
- [Using log files](#)
- [SharePoint web service removal fails](#)
- [Uninstalling Security Explorer](#)

Repairing inheritance


You may need to repair the inheritance on folders and files because some or all subfolders and files are not inheriting permissions correctly from their parent. Incorrect inheritance can include missing permissions, such as a subfolder missing an inherited permission from the parent, and unwanted extra permissions, such as a subfolder containing an extra inherited permission that is not present on the parent.

IMPORTANT: Repairing inheritance changes the permissions on the selected folders, subfolders, and files. Review the selected folders to verify that important permissions are not removed during the process.

NOTE: The Repair Inheritance function is available only in the NTFS Security module.

TIP: You also can use the Repair Security advanced task to repair multiple folders.

To repair inheritance

- 1 Open the **NTFS Security** module.
- 2 In the Navigation pane, select a folder, and select **Security | Repair Inheritance**.
-OR-
Click  on the Tool Bar.
- 3 Click **Yes**. See [Completing a process](#).

Creating test folders and files

To help you evaluate or troubleshoot issues, you can create a test folder that contains files and permissions.

To create test folders and files

- 1 Open the **NTFS Security** module.
- 2 Select **Help | Create Test Folders and Files**.
- 3 In the Starting Folder box, type the path to where you want to place the test folder, or browse to designate a location.
- 4 Click **Create Evaluation Folders and Files**. A message box appears asking if you want to apply a standard set of permissions to the folders and files.

- 5 To apply permissions, click **Yes**.

The securityexplorer.try folder appears in the location you designated. If you chose to apply permissions, those display in the Permissions pane.

Using log files

By default, there is one log file written to the Security Explorer installation directory. To get more log information, run Security Explorer.exe with /d key to write two log files to the installation directory.

```
C:\Program Files\Quest\Security Explorer\SecurityExplorer.exe /d
```

For the Exchange Security module, the ExchangeAccess log files contain Exchange module log data.

Because Security Explorer is digitally signed, you may see event log entries when starting Security Explorer if the Update Root Certificates component is turned on and the computer cannot connect to the Windows® Update server on the Internet. The Update Root Certificates component automatically updates trusted root-certificate authorities from the Microsoft Update server at regular intervals.

To resolve this behavior, connect to the Internet, or turn off the Update Root Certificates component.

To turn off the Update Root Certificates component

- 1 In Control Panel, double-click **Add/Remove Programs**.
- 2 Click **Add/Remove Windows Components**.
- 3 Clear the **Update Root Certificates** check box, and continue with the Windows Components Wizard.

SharePoint web service removal fails

If you find that you are unable to remove the SharePoint® Web Service and try the manual process, the manual process may fail because a timer job is still in process.

To delete the timer job and remove the SharePoint web service

- 1 On one of the servers in the SharePoint farm, run the command stsadm.exe -o enumsolutions.

To view the command

- a Open the **SharePoint Security** module.
 - b Select **SharePoint | Manage SharePoint Farms and Sites**.
 - c Click **Manual Web Service Deployment/Removal**.
 - d Click **Manual Web Service Removal**.
 - e Click **Verify Command** to open the SharePoint Web Service Commands page where you can copy and paste the command.
- 2 Examine the output.
 - If the output does not show a solution name **SLWebServices_1.00.0009.wsp** (or similar), then the web service is uninstalled and no further action is required.
 - If the output does show a solution name **SLWebServices_1.00.0009.wsp** (or similar) then the web service is still installed. The Deployed flag will probably display FALSE.
 - 3 Try to remove the solution manually by running two commands in sequence.
 - a Execute the stsadm.exe -o retractsolution -name SLWebServices_1.00.0009.wsp command. You may need to wait a few moments before running the second command to allow the retraction to finish.

- b Execute the `stsadm.exe -o deletesolution -name SLWebServices_1.00.0009.wsp` command.

To view the commands

- a Select **SharePoint | Manage SharePoint Farms and Sites**.
 - b Click **Manual Web Service Deployment/Removal**.
 - c Click **Manual Web Service Removal**.
 - d Click **Removal Commands** to open the SharePoint Web Service Commands page where you can copy and paste the commands.
- 4 Examine the output.
 - If these commands succeed, the web service is uninstalled and no further action is required. You can confirm the uninstall by running the `stsadm.exe -o enumsolutions` command again.
 - If this command does not succeed, the output will mention that a retraction is already in process. This is the timer job that you need to remove.
 - 5 To remove the timer job, browse to the central administration console and delete the timer job (**Central Administration | Operations | Timer Job Definitions**).
 - 6 After the timer job is removed, retry the **retractsolution** and **deletesolution** commands in step 2. This time the commands should succeed.

Uninstalling Security Explorer

Use **Control Panel | Programs and Features** to uninstall Security Explorer 9.

i **NOTE:** Some Security Explorer folders remain after the uninstall process. The folders in the installation directory contain the log files created after the product was installed. These folders may be deleted manually.

The user profile directory contains setting folders with items such as saved search criteria, saved alternate credentials, favorites, and enterprise scopes. During the uninstall process, you are asked if you want to remove these settings folders. If for any reason, Security Explorer is unable to remove the settings folders, you can delete them manually.

- For a single user, the settings folders are located at **C:\Users\<User Name>\AppData\Local\Quest**.
- If the configuration information was shared (see [Setting advanced options](#)) the settings folders are located at **C:\ProgramData\Quest**.

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.