File Rewriting Configuration Guide

Published August 2020

Document Version 1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

File Rewriting Configuration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

File Rewriting

File Rewriting Overview

A file resource profile controls access to resources on Windows server shares or UNIX servers.

File rewriting is a standard feature on all Connect Secure devices.

When creating a file resource profile, you must use the following formats when defining a resource policy's primary resource as well as its autopolicy resources.

Windows resources:

\\server[\share[\path]]

UNIX resources:

server[/path]

Within these formats, the three components are:

- **Server** (required) - Possible values:
  - **Hostname** - You may use the system variable <username> when defining the hostname.
  - **IP address** - The IP address needs to be in the format: a.b.c.d

  The leading two back slashes are required for Windows, non-Nfs resources.
- **Share** (required, Windows only) - The system variable <username> is allowed. Note that when the system tries to connect to a Windows file share, it connects to ports 445 and 139.
- **Path** (optional) - Special characters allowed include:

*	Matches any character. Note that you cannot use the * wildcard character when defining a resource profile's primary resource (that is, the Server/share field for Windows resources or the Server field for UNIX resources).
%	Matches any character except slash (/)
?	Matches exactly one character

Valid Windows resources include:

\\pulsesecure.net\dana

\\10.11.0.10\share\web

\\10.11.254.227\public\test.doc

Valid UNIX resources include:

\\pulsesecure.net\dana

10.11.0.10/share/web

10.11.254.227/public/test.doc

Creating a File Rewriting Resource Profile

To create a file rewriting resource profile:

1. In the admin console, choose **Users > Resource Profiles > Files**.
2. Click **New Profile**.
3. From the **Type** list, select **Windows or Unix**.
4. Enter a unique name and optionally a description for the resource profile. (This name becomes the default bookmark's name.)
5. Enter the resource to which you want to control access. Note that the format of the resource varies depending on which type of resource profile you are creating:
   - **Windows** - Enter the server name or IP address, share name, and optionally the path that you want to control access to in the Server/share field. When entering the resource, use the format: \\server[\share[\path]].
   - **Unix** - Enter the server name or IP address and optionally the path that you want to control access to in the Server field. When entering the resource, use the format: server[/path]
6. In the **Autopolicy: Windows File Access Control** section or the **Autopolicy: UNIX Access Control** section, create a policy that allows or denies users access to the resource specified the previous step. At minimum, you need to click **Add** in order to use the access control policy that is automatically created for you. This policy allows access to the specified directory and all of its sub-directories.
7. (Optional) Click **Show ALL autopolicy** types to create additional autopolicies that fine-tune access to the resource. Then, create the autopolicies.
8. Click **Save** and **Continue**.
9. In the **Roles** tab, select the roles to which the resource profile applies and click **Add**.

   The selected roles inherit the autopolicies and bookmarks created by the resource profile. If it is not already enabled, the system automatically enables the **Files, Windows** option or the **Files**, **UNIX/NFS** option in the **Users > User Roles > Select Role > General > Overview** page of the admin console for all of the roles you select.
10. Click **Save Changes.**
11. (Optional) In the **Bookmarks** tab, modify the default bookmark and/or create new ones. (By default, the system creates a bookmark to the resource defined in the Windows or UNIX field and displays it to all users assigned to the role specified in the **Roles** tab.)

Creating a File Access Control Autopolicy

File access control policies specify resources on your file servers that users may access. When defining a file resource profile, you must create a corresponding access control autopolicy that enables access to the profile's primary resource. The system simplifies the process for you by automatically creating an autopolicy that allows access to the directory specified in the Server/share field (Windows) or the Server field (UNIX) and all of its sub-directories. To enable this autopolicy, you simply need to select it and click Add.

If necessary, you may choose to modify this default autopolicy or create supplementary file access control autopolicies that allow or deny access to additional resources.

To create a new file access control autopolicy:

1. Create a file resource profile.
2. If it is not already enabled, select the **Autopolicy: Windows File Access Control** check box or the **Autopolicy: Unix Access Control** check box.
3. In the **Resource** field, specify the resource to which this policy applies using the format: \\server[\share[\path]] for Windows resources and \\server[\path] for UNIX resources.
4. From the **Action** list, select one of the following options:
   - **Allow** - Select this option to enable access to the specified resource.
   - **Read-only** - Select this option to allow users to view but not edit the specified resource.
   - **Deny** - Select this option to block access to the specified resource.
5. Click **Add**.
6. Click **Save Changes**.

Creating a File Compression Autopolicy

Compression autopolicies specify which types of file data to compress when you enable GZIP compression through the **Maintenance > System > Options** page of the admin console.

To create a file compression autopolicy:

1. Create a file resource profile.
2. Click **Show ALL autopolicy** types.
3. Select the **Autopolicy: Windows File Compression** check box or the **Autopolicy: Unix File Compression** check box.
4. In the **Resource** field, specify the resource to which this policy applies using the format: \\server[\share[\path]] for Windows resources and \\server[\path] for UNIX resources.
5. In the **Action** field, select one of the following options:
   - **Compress** - Select this option to compress data from the specified resource.
   - **Do not compress** - Select this option to disable compression for the specified resource.
6. Click **Add**.

Creating a Single Sign-On Autopolicy (Windows Only)

Single sign-on (SSO) autopolicies configure the system to automatically submit credentials to a Windows share or directory so that the user does not have to reenter his credentials.

To create a Windows SSO autopolicy:

1. Create a Windows file resource profile.
2. Click **Show ALL autopolicy** types.
3. Select the **Autopolicy: Windows Server Single Sign-On** check box.
4. In the **Resource** field, specify the resource to which this policy applies using the format: *\\server[\share[\path]]*.
5. Select one of the following options:

- **Use predefined credentials** - Select this option if you want to specify credentials to pass to the Windows share or directory. Then:
  - In the **Username** field, enter variable (such as <username> or a static username (such as administrator) to submit to the Windows share or directory. When entering a variable, you may also include a domain. For example, yourcompany.net\<username>.
  - Enter a variable (such as <password> in the **Variable Password** field or enter a static password in the **Variable** field. Note that the system masks the password you enter here with asterisks.

    When entering static credentials, note that the file browsing server maintains the connections open to a server share, however, so connecting to a different folder on the same share using a different account may not work reliably.

    If the specified credentials fail, the system may submit alternative credentials.
  - **Disable SSO** - Select this option if you do not want the system to automatically submit credentials to the specified Windows share or directory.

6. Click **Save Changes.**

Configuring File Resource Profile Bookmarks

When you create a file resource profile, the system automatically creates a bookmark that links to the primary resource that you specified in the resource profile. The system enables you to modify this bookmark as well as create additional bookmarks within the same domain.

When configuring bookmarks, note that:

- You can only assign bookmarks to roles that you have already associated with the resource profile-not all of the roles defined in the system. To change the list of roles associated with the resource profile, use settings in its Roles tab.
- Bookmarks simply control which links to display to users-not which resources the users can access. For instance, if you enable access to a Windows directory but do not create a bookmark to that directory, users can access the directory through Windows Explorer.

- You cannot create bookmarks that link to additional servers defined through file access control autopolicies.
- If you use a bookmark to reference a file shortcut, note that the system only displays bookmarks with shortcuts to files or folders on a network share such as \\server5\share\users\jdoe\file.txt. However, the system does not display bookmarks with shortcuts to local directories such as C:\users\jdoe\file.txt.

To configure file resource profile bookmarks:

1. If you want to create a resource profile bookmark through the standard resource profiles page:
   a. Navigate to the **Users > Resource Profiles > Files > Resource Profile Name > Bookmarks** page in the admin console.
   b. Click the appropriate link in the **Bookmark** column if you want to modify an existing bookmark. Or, click **New Bookmark** to create an additional bookmark.

Alternatively, if you want to create a resource profile bookmark through the user roles page:

   a. Navigate to the **Users > User Roles > Role Name > Files > Windows Bookmarks|Unix Bookmarks** page in the admin console.
   b. Click **New Bookmark.**

2. From the **Type** list, choose **File Resource Profile**. This option appears only if you have already created a file resource profile.
3. Select an existing resource profile.
4. Click **OK**. If you have not already associated the selected role with the resource profile, the system automatically makes the association for you. The system also enables any access control policies for the role that are required by the resource profile.
5. If this role is not already associated with the selected resource profile, the system displays an informational message. If you see this message, click **Save Changes** to add this role to the resource profile's list of roles and to update the profile's autopolicies as required. Then, repeat the previous steps to create the bookmark.

Note: When you create a resource profile bookmark through the user roles page (instead of the standard resource profiles page), the system only associates the generated bookmark with the selected role. The system does not assign the bookmark to all of the roles associated with the selected resource profile.

6. Optionally change the name and description of the bookmark. (By default, the system populates names the bookmark using the resource profile name.)
7. In the **File Browsing Path** field, add a suffix to the resource if you want to create links to sub-directories of the resource defined in the primary resource profile.

   Make sure to enter a unique server and path in this field. If you create two bookmarks that contain the same concatenated server and path string, the system deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.

8. In the Appearance section, choose one of the following options:
   - **Appear as bookmark on homepage and in file browsing** - Select this option if you want the bookmark to appear both on a user's welcome page and when browsing network files.

- **Appear in file browsing only** - Select this option if you want the bookmark to appear only when users are browsing network files.

9. If you are configuring the bookmark through the resource profile pages, under Roles, specify the roles to which you want to display the bookmark:
   - **ALL selected roles** - Select this option to display the bookmark to all of the roles associated with the resource profile.
   - **Subset of selected roles** - Select this option to display the bookmark to a subset of the roles associated with the resource profile. Then select roles from the **ALL Selected Roles** list and click **Add** to move them to the **Subset of selected roles** list.
10. Click **Save Changes**.

Windows File Bookmarks

Creating Windows File Bookmarks

You can use two different methods to create Windows file bookmarks:

- **Create bookmarks through existing resource profiles** (recommended) - When you select this method, the system automatically populates the bookmark with key parameters (such as the primary server and share) using settings from the resource profile. Additionally, while you are creating the associated resource profile, the system guides you through the process of creating any required policies to enable access to the bookmark.
- **Create standard bookmarks** - When you select this option, you must manually enter all bookmark parameters during configuration. Additionally, you must enable access to the file browsing at the role level and create resource policies that enable access to the servers defined in the bookmark.

  You can create Windows bookmarks that appear on the welcome page for users mapped to this role. You can insert the user's username in the URL path to provide quick access to the user's network directories.

  When users are browsing files on a DFS server, the DFS server uses the site configuration data stored in Active Directory to return DFS referrals to the system in the right order. Referrals to closer servers are put higher in the list than referrals to servers that are farther away. Clients try referrals in the order in which they are received. If a request comes from a client which resides in a subnet which is not in this list, the server will not know where the client is coming from and will return the list of referrals to the customer in an arbitrary order. This could potentially cause the DFS requests from the system (acting as the client in this case) to access a server much farther away. In turn, this could cause serious delays, especially if the system attempts to access a server which is unreachable from the subnet which the system resides in. If the system is installed on a subnet which is not in the DFS server's list, the DFS administrator may use the "Active Directory Sites and Services" tool on the domain controller to add the system's subnet to the appropriate site.

Creating Advanced Bookmarks to Windows Resources

Information in this topic is provided for backwards compatibility. We recommend that you configure access to Windows shares and directories through resource profiles instead, since they provide a simpler, more unified configuration method.

To create a bookmark to a Windows resource:

1. In the admin console, choose **Users > User Roles > Role Name > Files > Windows Bookmarks.**
2. Click **New Bookmark** and then browse to or enter the server and share name. Specify a path to further restrict access. If you want to insert the user's username, enter <username> at the appropriate place in the path. For information about additional system variables and attributes that you can include in the bookmark. If you specify a name and description for the bookmark, this information displays on the home page instead of the server/share.

   You may not bookmark a Windows server. You must specify both the server and share name.

   Make sure to enter a unique server and path in this field. If you create two bookmarks that contain the same concatenated server and path string, the system deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.
3. For Appearance, choose either:
   - **Appear as bookmark on homepage and in file browsing** - if you want the bookmark to appear both on a user's welcome page and when browsing network files.
   - **Appear in file browsing** - only if you want the bookmark to appear only when browsing network files.
4. For Access, click **Enable auto-allow access** to this bookmark if you want the system to automatically create a corresponding Windows Access resource policy. Note that this functionality applies only to role bookmarks and not bookmarks created by users. Next, select:
   - **Read** - write access to enable users to save files on the server. Note that users cannot upload files greater than 500 MB to the server.
   - **Include sub-folders** - to enable users to view files in directories below the specified bookmark path.

Note: You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

5. Click **Save Changes** or **Save + New** to add another.

Creating Windows Bookmarks that Map to LDAP Servers

To create a bookmark that automatically maps to a user's LDAP home directory:

1. Create an **LDAP server** instance.
2. Add the **LDAP attribute homeDirectory** to the **Server Catalog.**
3. Configure a **realm** and bind **LDAP** as the authentication server.
4. Configure role-mapping rules, as needed.
5. Create a **Windows bookmark**. During configuration, specify <u***serAttr.homeDirectory***> in the bookmark.
6. Click **Save Changes**.

Defining General Windows File Browsing Options

To specify general Windows file browsing options:

1. In the admin console, choose **Users > User Roles > Role Name > Files > Options**.
2. Under **Windows Network Files,** specify which options to enable for users:
   - **User can browse network file shares** - If enabled, users can view and create bookmarks to resources on available Windows file shares.
   - **User can add bookmarks** - If enabled, users can view and create bookmarks to resources on available Windows file shares.
3. Click **Save Changes**.

Writing a File Resource Policy

When you enable the File access feature for a role, you need to create resource policies that specify which Windows and UNIX/NFS resources a user may access, as well as the encoding to use when communicating with Windows and NFS file shares. When a user makes a file request, the system evaluates the resource policies corresponding to the request, such as Windows access resource policies for a request to fetch an MS Word document (.doc file). After matching a user's request to a resource listed in a relevant policy, the system performs the action specified for the resource.

You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

When writing a File resource policy, you need to supply key information:

- **Resources** - A resource policy must specify one or more resources to which the policy applies. When writing a File policy, you need to specify File servers or specific shares.
- **Roles** - A resource policy must specify the roles to which it applies. When a user makes a request, the system determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions** - Each type of resource policy performs a certain action, which is either to allow or deny a resource or to perform or not perform some function, such as allow a user to write to a directory. You can also write detailed rules that apply more conditions to a user request.

The system engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

Windows File Resources Canonical Format

Information in this section is provided for backwards compatibility. We recommend that you configure access to Windows file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

When writing a resource policy for a Windows file resource, you need to understand the following canonical format.

\\server[\share[\path]]

The three components are:

- **Server** (required) - Possible values:
  - **Hostname** - The system variable <username> may be used.
  - **IP address** - The IP address needs to be in the format: a.b.c.d
- **Share** (optional) - If the share is missing, then star (*) is assumed, meaning ALL paths match. The system variable <username> is allowed.
- **Path** (optional) - Special characters allowed include:

*	Matches any character
%	Matches any character except slash (/)
?	Matches exactly one character

If the path is missing, then slash (/) is assumed, meaning only top-level folders are matched. For example:

\\%.danastreet.net\share\<username>*

\\pulsesecure.net\dana*

\\10.11.0.10\share\web*

\\10.11.254.227\public\%.doc

Writing a Windows Access Resource Policy

Information in this topic is provided for backwards compatibility. We recommend that you configure access to Windows file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To write a Windows access resource policy:

1. In the admin console, choose **Users > Resource Policies > Files > Access > Windows.**
2. On the Windows File Access Policies page, click **New Policy**.
3. Enter a name to label this policy (required) and a description of the policy. (optional)
4. In the Resources section, specify the resources to which this policy applies.
5. In the Roles section, specify:
   - **Policy applies to ALL roles**-To apply this policy to all users.
   - **Policy applies to SELECTED roles**-To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
   - **Policy applies to all roles OTHER THAN those selected below-**To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:
   - **Allow access** - To grant access to the resources specified in the Resources list. Check Read-only to prevent users from saving files on the server.

- **Deny access** -To deny access to the resources specified in the Resources list.
- **Use Detailed Rules** - To specify one or more detailed rules for this policy.

7. Click **Save Changes**.
8. On the Windows File Access Policies page, order the policies according to how you want to evaluate them. Keep in mind that once the system matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

   If you want to write a File resource policy that enables you to specify credentials to submit to a file server when a user request matches a resource in the Resource list, you can use the following procedure to do so. You can also configure the system to prompt users for credentials.

Writing a Windows SSO Resource Policy

Information in this topic is provided for backwards compatibility. We recommend that you configure access to Windows file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To write a Windows credentials resource policy:

1. In the admin console, choose **Users > Resource Policies > Files > SSO > Windows**.
2. On the **Windows Credentials Policies** page, click **New Policy.**
3. Enter a name to label this policy (required) and a description of the policy. (optional)
4. In the Resources section, specify the resources to which this policy applies.
5. In the Roles section, specify:
   - **Policy applies to ALL roles** - To apply this policy to all users.
   - **Policy applies to SELECTED roles** - To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
   - **Policy applies to all roles OTHER THAN those selected below** - To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify the action to take when a resource requires credentials:

- **Use System Credentials** - If the system has stored credentials for the specified user and resource in its cache, it submits the stored credentials. If the stored credentials fail or if no stored credentials exist for that user, the system prompts for new credentials and stores the new credentials.
- **Use Specific Credentials** - tYou specify static credentials that the system submits to resources. The file browsing server maintains the connections open to a server\share so connecting to a different folder on the same share using a different account may not work reliably. If the specified credentials fail, the system may submit alternative credentials. Note that the system masks the password you enter here with asterisks.

- **Prompt for user credentials** - The system intermediates the share challenge by presenting an authentication challenge the first time a user attempts to access the share. The user enters the credentials and the credentials are stored in the system. If the credentials later fail, the system again prompts the user for their credentials.
- **Use Detailed Rules** - To specify one or more detailed rules for this policy.

7. Click **Save Changes.**
8. On the Windows File Access Policies page, order the policies according to how you want to evaluate them. Keep in mind that once the system matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Writing a Windows Compression Resource Policy

Information in this section is provided for backwards compatibility. We recommend that you configure compression through resource profiles instead, since they provide a simpler, more unified configuration method.

Compression policies specify which types of file data to compress when you enable GZIP compression through the Maintenance > System > Options page of the admin console.

The system comes pre-equipped with two file compression policies (*:*/*) which compress all applicable file data. You may enable these policies through the Resource Policies > Files > Compression pages of the admin console.

To write a Windows file compression resource policy:

1. In the admin console, choose **Resource Policies > Files > Compression**.
2. Select the **Windows** tab.
3. Click **New Policy**.
4. Enter a name to label this policy (required) and a description of the policy. (optional)
5. In the Resources section, specify the resources to which this policy applies.
6. In the Roles section, specify:

- **Policy applies to ALL roles** - To apply this policy to all users.
  - **Policy applies to SELECTED roles** - To apply this policy only to users who are mapped to roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.
- **Policy applies to all roles OTHER THAN those selected below** - To apply this policy to all users except for those who map to the roles in the **Selected roles** list. Make sure to add roles to this list from the **Available roles** list.

7. In the Action section, specify:
   - **Compress** - Compress the supported content types from the specified resource.
   - **Do not compress** - Do not compress the supported content types from the specified resource.
   - **Use Detailed Rules** - Select this option to specify one or more detailed rules for this policy.

8. Click **Save Changes**.

Defining General File Writing Options

You can specify File resource options that apply to your File resource policies. When you enable a File resource policy option, the system compiles a list of hostnames specified in the Resources field of each File resource policy. The system then applies the enabled options to this comprehensive list of hostnames.

To specify resource options for Windows file servers:

1. In the admin console, choose **Users > Resource Policies > Files > Options**.
2. Select:
   - **IP based matching for Hostname based policy resources** - The system looks up the IP address corresponding to each hostname specified in a File resource policy. When a user tries to access a server by specifying an IP address rather than the hostname, the system compares the IP to its cached list of IP addresses to determine if a hostname matches an IP. If there is a match, then the system accepts the match as a policy match and applies the action specified for the resource policy.

   This option does not apply to hostnames that include wildcards and parameters.
   - **Case sensitive matching for the Path component in File resources** - Require users to enter a case-sensitive path component.
   - **Encoding** - Select the encoding to use when communicating with Windows and NFS file shares.
   - **Use NTLM v1, NTLM v1 will be used for all NTLM negotiations** - Select this option to use only NTLM V1 for file share authentication.
   - **Use NTLM v2, NTLM v2 will be used for all NTLM negotiations** - Select this option to use only NTLM V2 for file share authentication.
   - **Number of NTLM authentication protocol variant attempts** - Controls the number of login attempts while doing SSO, Select "Low" if you are seeing account lockout issues.
3. Click **Save Changes**.

Unix File Bookmarks

Creating UNIX File Bookmarks

You can use two different methods to create UNIX file bookmarks:

- Create bookmarks through existing resource profiles (recommended)-When you select this method, the system automatically populates the bookmark with key parameters (such as the server) using settings from the resource profile. Additionally, while you are creating the associated resource profile, the system guides you through the process of creating any required policies to enable access to the bookmark.
- Create standard bookmarks-When you select this option, you must manually enter all bookmark parameters during configuration. Additionally, you must enable access to the file browsing at the role level and create resource policies that enable access to the servers defined in the bookmark.

You can create UNIX bookmarks that appear on the welcome page for users mapped to this role. You can insert the user's username in the URL path to provide quick access to the user's network directories.

Creating Advanced Bookmarks to UNIX Resources

Information in this topic is provided for backwards compatibility. We recommend that you configure access to UNIX servers through resource profiles instead, since they provide a simpler, more unified configuration method.

You can create UNIX/NFS bookmarks that appear on the home page. You can insert the user's username in the URL path to provide quick access to the user's network directories.

To create a bookmark to a UNIX/NFS resource:

1. In the admin console, choose **Users > User Roles > Role Name > Files > UNIX Bookmarks**.
2. Click **New Bookmark** and then enter the server hostname or IP address and the path to the share. If you want to insert the user's username, enter <username> at the appropriate place in the path. If you specify a name and description for the bookmark, this information displays on the home page instead of the server/path.

   Make sure to enter a unique server and path in this field. If you create two bookmarks that contain the same concatenated server and path string, the system deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.
3. For Appearance, choose either:
   - **Appear as bookmark on homepage and in file browsing** - if you want the bookmark to appear both on a user's welcome page and when browsing network files.
   - **Appear in file browsing only** if you want the bookmark to appear only when browsing network files.
4. For Access, click **Enable auto-allow access to this bookmark** if you want to automatically create a corresponding UNIX/NFS resource policy. Note that this functionality applies only to role bookmarks and not bookmarks created by users. Next, select:
   - **Read-write access** - to enable users to save files on the server. Note that users cannot upload files greater than 500 MB to the server.
   - **Include sub-folders** - to enable users to view files in directories below the specified bookmark path.

   Note: You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.
5. Click **Save Changes** or **Save + New** to add another.

Defining General UNIX File Browsing Options

For NFS file browsing to work properly, you must configure a NIS server on the system before enabling NFS file browsing.

To specify general file browsing options:

1. In the admin console, choose **Users > User Roles > Role Name > Files > Options**.
2. Under UNIX Network Files, specify which options to enable for users:
   - **User can browse network file shares** - If enabled, users can view and create bookmarks to resources on available UNIX file shares.
   - **User can add bookmarks** - If enabled, users can view and create bookmarks to resources on available UNIX file shares.
   - **Allow automount shares** - If enabled, users access to automount shares specified on a NIS server.
3. Click **Save Changes.**

Defining UNIX/NFS File Resource Policies

When you enable the File access feature for a role, you need to create resource policies that specify which Windows and UNIX/NFS resources a user may access, as well as the encoding to use when communicating with Windows and NFS file shares. When a user makes a file request, the system evaluates the resource policies corresponding to the request, such as Windows access resource policies for a request to fetch an MS Word document (.doc file). After matching a user's request to a resource listed in a relevant policy, the system performs the action specified for the resource.

You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

When writing a File resource policy, you need to supply key information:

- **Resources** - A resource policy must specify one or more resources to which the policy applies. When writing a File policy, you need to specify File servers or specific shares.
- **Roles** - A resource policy must specify the roles to which it applies. When a user makes a request, the system determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions** - Each type of resource policy performs a certain action, which is either to allow or deny a resource or to perform or not perform some function, such as allow a user to write to a directory. You can also write detailed rules that apply more conditions to a user request.

The engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

Canonical Format: UNIX/NFS File Resources

When writing a resource policy for a UNIX/NFS file resource, you need to understand the following canonical format.

server[/path]

The two components are:

- **Server** (required) - Possible values:
  - **Hostname** - The system variable <username> may be used.
  - **IP address** - The IP address needs to be in the format: a.b.c.d

- **Path** (optional) - Special characters allowed include:

*	Matches any character
%	Matches any character except back slash (\)
?	Matches exactly one character

If the path is missing, then back slash (\) is assumed, meaning only top-level folders are matched. For example:

%.danastreet.net/share/users/<username>

.\\pulsesecure.net\dana/

10.11.0.10/web/*

10.11.254.227/public/%.txt

Writing UNIX/NFS Resource Policies

Information in this section is provided for backwards compatibility. We recommend that you configure access to UNIX file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To write a UNIX/NFS resource policy:

1. In the admin console, choose **Users > Resource Policies > Files > Access > Unix/NFS**.
2. On the UNIX/NFS File Access Policies page, click **New Policy.**
3. Enter a name to label this policy (required) and a description of the policy. (optional)
4. In the Resources section, specify the resources to which this policy applies.
5. In the Roles section, specify:
   - **Policy applies to ALL roles** - To apply this policy to all users.
   - **Policy applies to SELECTED roles** - To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
   - **Policy applies to all roles OTHER THAN those selected below** - To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:
   - **Allow access** - To grant access to the resources specified in the Resources list. Check Read-only to prevent users from saving files on the server.
   - **Deny access** - To deny access to the resources specified in the Resources list.
   - **Use Detailed Rules** - To specify one or more detailed rules for this policy.
7. Click **Save Changes**.

8. On the UNIX/NFS File Access Policies page, order the policies according to how you want to evaluate them. Keep in mind that once the system matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Writing a UNIX/NFS Compression Resource Policy

Information in this section is provided for backwards compatibility. We recommend that you configure access to UNIX file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

Compression policies specify which types of file data to compress when you enable GZIP compression through the Maintenance > System > Options page of the admin console.

The system comes pre-equipped with two file compression policies (*:*/*) which compress all applicable file data. You may enable these policies through the Resource Policies > Files > Compression pages of the admin console.

To write a UNIX/NFS file compression resource policy:

1. In the admin console, choose **Resource Policies > Files > Compression.**
2. Select the **Unix/NFS** tab.
3. Click **New Policy.**
4. Enter a name to label this policy (required) and a description of the policy. (optional)
5. In the Resources section, specify the resources to which this policy applies.
6. In the Roles section, specify:
   - **Allow access** - To grant access to the resources specified in the Resources list. Check Read-only to prevent users from saving files on the server.
   - **Deny access** - To deny access to the resources specified in the Resources list.
   - **Use Detailed Rules** - To specify one or more detailed rules for this policy.
7. In the Action section, specify:
   - **Compress** - Compress the supported content types from the specified resource.
   - **Do not compress** - Do not compress the supported content types from the specified resource.
   - **Use Detailed Rules** - Select this option to specify one or more detailed rules for this policy.
8. Click **Save Changes**.

Defining General UNIX/NFS File Writing Options

You can specify File resource options that apply to your File resource policies. When you enable a File resource policy option, the system comp78iles a list of hostnames specified in the Resources field of each File resource policy. The system then applies the enabled options to this comprehensive list of hostnames.

To specify options for UNIX/NFS resources:

1. In the admin console, choose **Users > Resource Policies > Files > Options.**
2. Select:

   - **IP based matching for Hostname based policy resources** - The system looks up the IP address corresponding to each hostname specified in a File resource policy. When a user tries to access a server by specifying an IP address rather than the hostname, the system compares the IP to its cached list of IP addresses to determine if a hostname matches an IP. If there is a match, then the system accepts the match as a policy match and applies the action specified for the resource policy.

   Note: Note This option does not apply to hostnames that include wildcards and parameters.

   - **Case sensitive matching for the Path component in File resources** - Select this option to require users to enter a case-sensitive URL to an NFS resource. Use this option when passing username or password data in a URL.

   Note: This option does not apply to Windows servers.

   - **Encoding** - Select the encoding to use for communicating with the Windows and NFS file shares.
   - **NTLM Version** - Select whether to fall back to NTLM version 1 or version 2 authentication if Kerberos authentication of administrator credentials fails.
   - **Number of NTLM authentication protocol** - Select High to allow a large number of authentication attempt to be made to the backend server. This applies only to NTLM, not basic authentication. If your server locks users out for too many failed attempts, select Low.

   Note: Many servers do not support the different NTLM protocol variant attempts when you select High. If you find that authentication is failing even though the username and password are correct, set this option to Low.

3. Click **Save Changes**.