NetWitness® Platform XDR

Version 12.1.0.0

System Security and User Management

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

October, 2022

Contents

Set Up System Security

This guide provides information about setting up system-wide security in NetWitness Platform and controlling user access. The system administrator needs to understand system-wide security settings, user accounts, system roles, permissions, and access to services.

This guide contains the following sections:

Setting Up System Security

Setting up system security involves configuring password complexity and other system-level security settings for users to securely log in to NetWitness and to prevent unauthorized user access.

Set Up System Security Workflow

This figure shows the high-level workflow for setting up the system security.

First, you can configure password complexity by setting up password strength by specifying maximum password length, decimals, special characters, and so on. Next, you should change the default administrator passwords. Then you can configure system-level security by adjusting the security settings such as lockout period, maximum login failures, session timeout, idle period, and case-sensitive usernames. You can also configure optional settings for external authentication, PKI authentication, and a customized login banner.

These are the procedures for setting up system security:

- Configure Password Complexity
- Change the Default Admin Passwords
- Configure System-Level Security Settings
- (Optional) Configure External Authentication
- (Optional) Configure PKI Authentication
- (Optional) Create a Customized Login Banner

Configure Password Complexity

Passwords are an important part of your network security strategy. They provide critical front-line protection for your computer systems and help prevent attacks and unauthorized access to private information.

Password policies, designed to enhance the security of corporate networks, vary depending on the industry, corporate requirements, and regulations. Because of these password policy variations, NetWitness software allows you to configure the password complexity requirements for internal NetWitness users to conform to your corporate password policy guidelines.

Password complexity requirements apply only to internal users and are not enforced for external users. External users rely on their own methods and systems to enforce password complexity.

In addition, you can set a global default user expiration period and determine if and when internal users receive notification that their passwords are about to expire. The password expiration notification consists of a password expiration message when a user logs on to NetWitness.

Password Strength

Strong passwords make it more difficult for attackers to guess user passwords and help prevent unauthorized access to your organization's network. You can define the appropriate level of password strength for your NetWitness users. When you configure the password strength settings, they apply to internal NetWitness users, including the admin user.

You can choose to enforce any combination of the following password strength requirements when a NetWitness user creates or changes their password:

- Minimum password length
- Minimum number of uppercase characters
- Minimum number of lowercase characters
- Minimum number of decimals (0 through 9)
- Minimum number of special characters
- Minimum number of non-Latin alphabetic characters (includes Unicode characters from Asian languages)
- Whether or not the password can contain the username

For example, you can create a strong password requirement that has a minimum of 9 characters, cannot contain the username of the user, and contains a mix of uppercase and lowercase letters, numbers, and special characters.

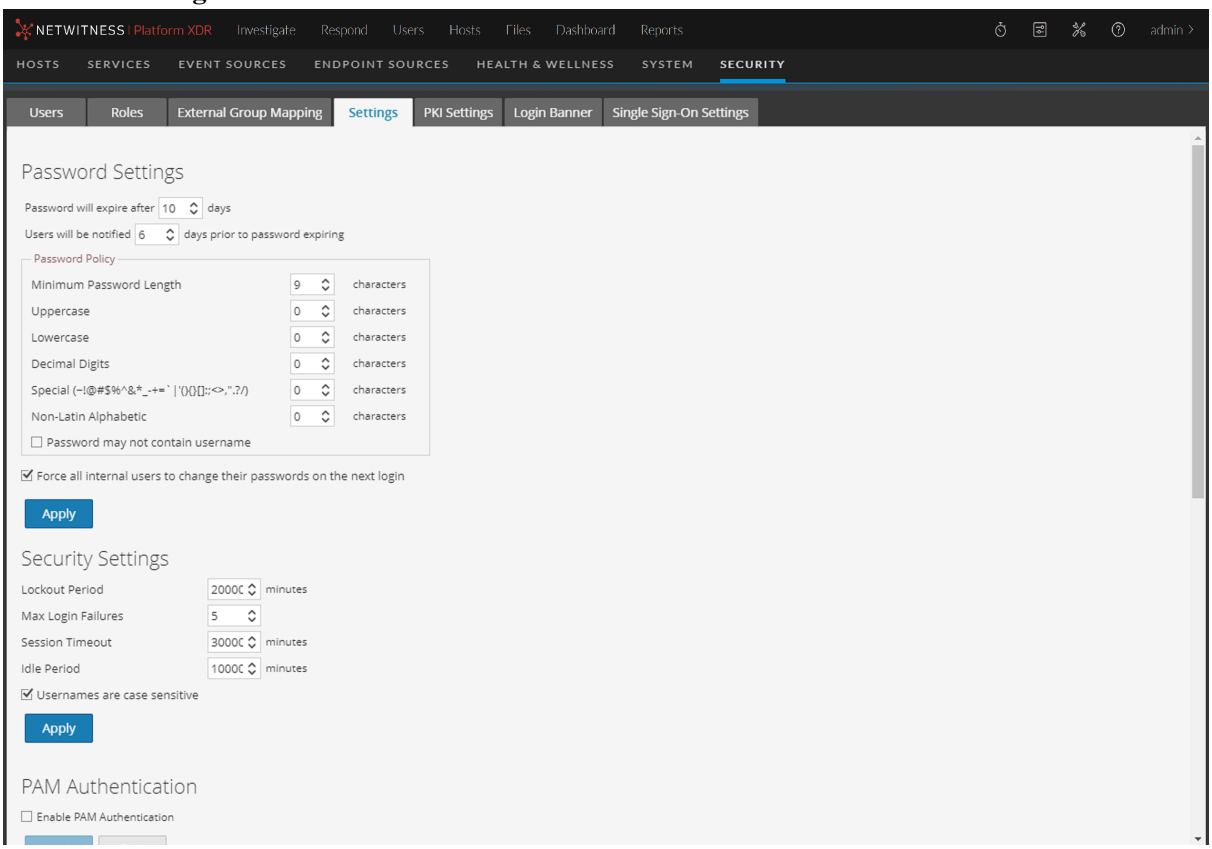
If you choose to enforce a minimum number of non-Latin alphabetic characters, ensure that your users have these characters available to them when setting their passwords.

For an example of a strong password policy, see the "STIG Compliant Passwords" in the *System Maintenance Guide*.

Configure Password Strength

1. In NetWitness, go to  **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.

2. Click the **Settings** tab.



3. In the **Password Settings** section, select the password complexity requirements to enforce when NetWitness users set their passwords and specify the minimum characters required, if applicable. Set the value to 0 for requirements you do not want to enforce, except for Minimum Password Length, which has a minimum value of 9 characters.

Note: In 11.2 and previous versions, the minimum password length is 8. Hence, on upgrade or update from previous versions to 11.3, you must set the minimum password length to 9 characters.

Requirement	Description
Password will expire after <n> days	The default number of days before a password expires for all internal NetWitness users. A value of zero (0) disables password expiration. For new installations, the default value is 30. For upgrades, the previous value will migrate automatically to the upgraded installation.
Users will be notified <n> days prior to password expiring	The number of days before the password expiration date, to notify a user that their password is about to expire. Users see a Password Expiration Message dialog when they log on to NetWitness. The minimum value is 1 day.

Requirement	Description
Minimum Password Length	Specifies a minimum password length. A minimum password length prevents users from using short passwords that are easy to guess. There is a minimum password length of 9 characters required by default. **Note:** In Version 11.2 and earlier versions, the minimum password length is 8. In Version 11.3, the minimum password length changed to 9. On upgrade or update from earlier versions to Version 11.3, users can still create a password with 8 characters until you explicitly set the minimum password length to 9 characters.
Uppercase	Specifies a minimum number of uppercase characters for the password. This includes European language characters A through Z, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic uppercase: Д Ц • Greek uppercase: Π Λ
Lowercase	Specifies a minimum number of lowercase characters for the password. This includes European language characters a through z, sharp-s, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic lowercase: д ц • Greek lowercase: π λ
Decimal Digits	Specifies a minimum number of decimal characters (0 through 9) for the password.
Special (~!@#$%^&*_-+=`|'(){}[];:<>,".?/)	Specifies a minimum number of special characters for the password: `~!@#$%^&*_-+=`|'(){}[];:<>,".?/`
Non-Latin Alphabetic	Specifies a minimum number of Unicode alphabetic characters that are not uppercase or lowercase. This includes Unicode characters from Asian languages. For example: • Kanji (Japanese): 頁 (leaf) 枒 (tree)
Password May Not Contain Username	Specifies that a password cannot contain the case-insensitive username of the user.

4. If you want your password policy changes to take effect at the next login instead of the next password change, select **Force all internal users to change their passwords on the next login**. Note that this setting is selected by default.
5. Click **Apply**.
   The password strength settings take effect when internal users create or change their passwords. If you selected **Force all internal users to change their passwords on the next login**, all internal users must change their password the next time they log on to NetWitness.

Change the Default Admin Passwords

The system administrator's user account is installed with NetWitness. The username is **admin** and the default password is the password that was entered in the Text-based User Interface (TUI) during the NetWitness installation process. The **Administrators** role is assigned to admin. This role has full system privileges to control what a user can do and which services a user can access. The only modification you can make to this account is to change the password. Unlike other NetWitness users, changes to the **admin** user password do not automatically propagate to downstream services. When you configure the password strength settings, they apply to all NetWitness users, including the admin user.

Passwords, an important aspect of computer security, are the front line of protection for your system. The **admin** user is pre-installed in NetWitness and on each Core service. For security, you create the users and roles for your organization in NetWitness, and on each Core service.

Best Practices

NetWitness recommends the following best practices:

- Change the **admin** password of each service from the default.
- Create a different password for the **admin** account on each service.

Change the admin Password for the NetWitness

Change the **admin** password for the NetWitness in the Profile view. See "Change Password" in the *NetWitness Getting Started Guide*. The password of the **admin** user does not propagate to Core services.

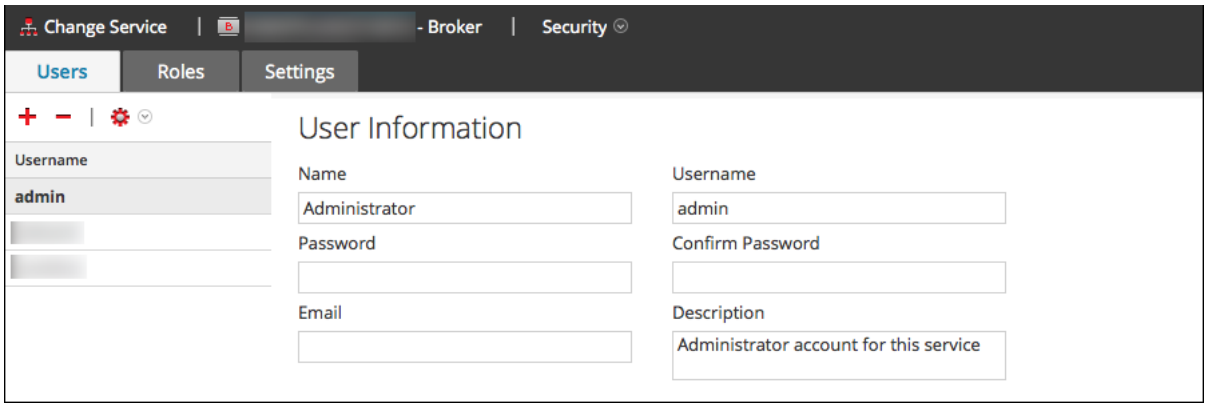
Note: After you change the admin password, you must remove and re-add a data source on the Reporting Engine. For more information, see the **Remove and re-add a Data Source on the Reporting Engine** section below.

Change the admin Password for Core Services

To change the admin password for a Core service:

1. Go to  **(Admin) > Services.**
2. Select a service, and then select  **> View > Security**.

3. On the **Users** tab, select the **admin** user.



4. In the **Password** field, type a new admin password for the selected service.
5. In the **Confirm Password** field, retype the new password.
6. Click **Apply**.

Note: After you change the admin password, you must remove and re-add a data source on the Reporting Engine. For more information, see **Remove and re-add a Data Source on the Reporting Engine** below.

Remove and Re-add a Data Source on the Reporting Engine

Reporting Engine validates a data source using the data source username and password. If you change the username or password of a data source, you must remove and re-add the data source.

To remove and re-add a data source on the Reporting Engine:

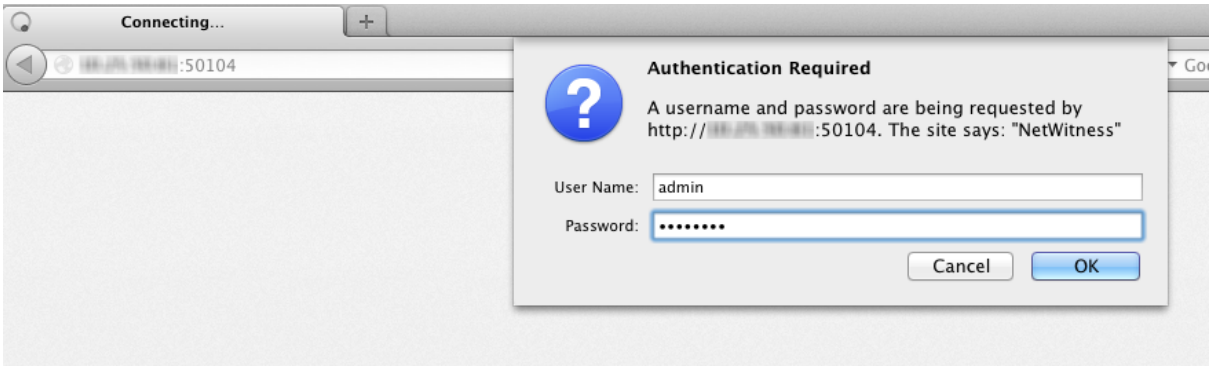
1. Go to **(Admin) > Services**.
2. In the Services view, select Reporting Engine and **View > Config**.
3. Click the **Sources** tab.
4. Select a service to remove and click .
5. Click and select **Available Services.**
6. Select the service you removed in step 4 and click **OK**.
7. When prompted, enter the new username and password for the service.

Change the admin Password for a Service Using the REST API

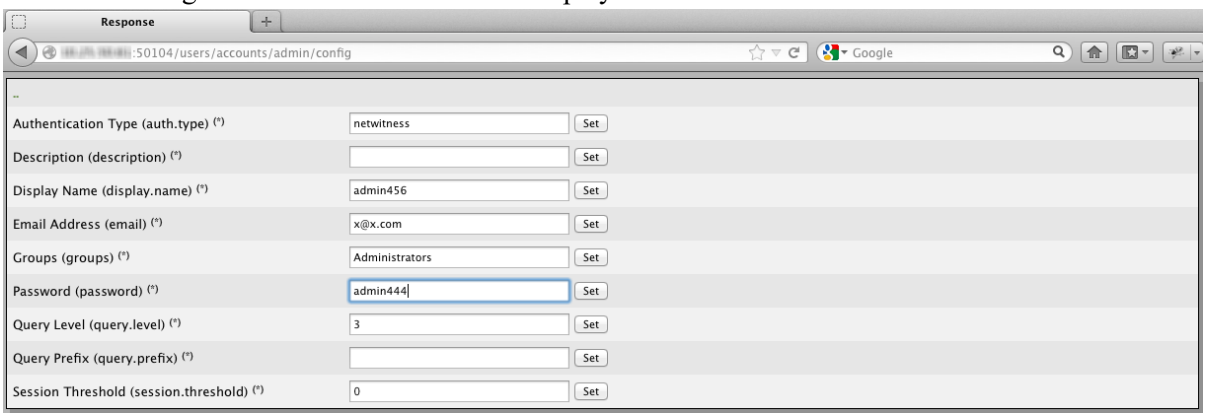
In rare circumstances, you may need to change the admin password for a Core service outside of the NetWitness user interface. This is simply another way to perform the Core service password change, and is not the preferred method.

To change the admin password for the service using the REST User Interface:

1. Open a web browser, and go to the following URL:
   <hostname>:<port>
   where the **hostname** is the name of a NetWitness Core service and **port** is the port used for REST communication. Here is an example for a Decoder: `http://10.20.30.40:50104`
   The authentication dialog is displayed.



2. In the dialog, enter the user name and password used for authentication as admin on the service, and click **OK**. The default user name is **admin** and the default password is **netwitness**.
   The REST window for the service is displayed.
3. Navigate through the node structure to **users/accounts/admin/config**.
   The user configuration fields for admin are displayed in the browser window.



4. In the Password field, type a new admin password and click **Set**.

Configure System-Level Security Settings

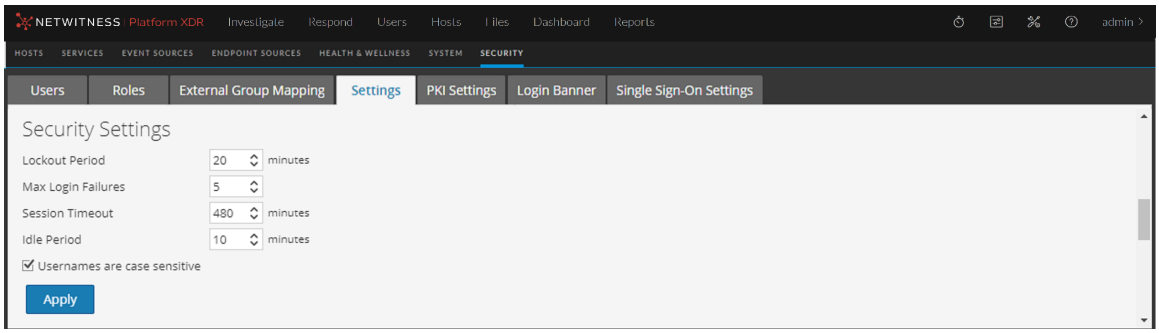
Most global security settings, such as the maximum number of failed login attempts to allow, apply to all NetWitness users and sessions. Settings related to passwords in the Password Strength section, such as password expiration period and the default number of days before user passwords expire, apply to internal NetWitness users, but not external users.

Configure Security Settings

1. Go to  **(Admin) > Security**.

   The Security view is displayed with the **Users** tab open.

2. Click the **Settings** tab.



3. In the **Security Settings** section, specify values for the fields as described in the following table.

Field	Description
Lockout Period	Number of minutes to lock a user out of NetWitness after the configured number of failed logins is exceeded. The default value is 20 minutes.
Max Login Failures	The maximum number of unsuccessful login attempts before a user is locked out. The default value is 5.
Session Timeout	The maximum duration of a user session before timing out in minutes. The default value is 480. The session times out when the configured time has elapsed, after which the user must log in again. The maximum allowed value is 30,000. **Note:** If you migrated to NetWitness 11.x from version 10.6.x and previously used a value of 0 for an unlimited session timeout, the value was reset automatically to 30,000 minutes, as a value of 0 is no longer supported.

Field	Description
Idle Period	Number of minutes of inactivity before a session times out. The default value is 10. The maximum allowed value is 30,000. **Note:** If you migrated to NetWitness 11.x from version 10.6.x and previously used a value of 0 for an unlimited idle period, the value was reset automatically to the default value of 10, as a value of 0 is no longer supported.
Usernames are case sensitive	Select this option if you want the Username field on the NetWitness login to be case sensitive. For example, if usernames are case sensitive, you could use admin to log on to NetWitness, but you could not use Admin.

4. Click **Apply**. The Security Settings take effect immediately. If a password expires, the user receives a prompt to change the password when they log on to NetWitness.

Restrict Access to Incidents

By default, analysts can view all of the incidents, alerts, and tasks in the Respond view. If you have sensitive or restricted information that should not be shared, you can restrict what analysts and other users can see in the Respond view.

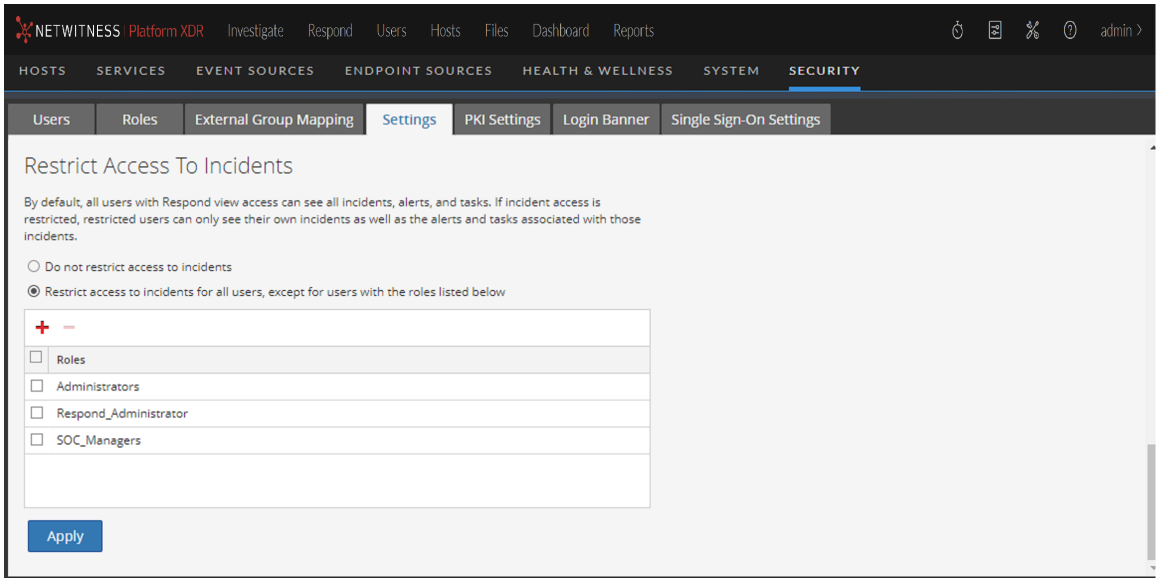
If you restrict access to incidents:

- Analysts can only see incidents assigned to them as well as the alerts and tasks associated with those incidents. Likewise, they can only change the status of and add journal entries (notes) to their own incidents.
- Analysts cannot see the Alerts and Tasks tabs in the Respond view (Respond > Tasks and Respond > Alerts are hidden), so they cannot view all alerts and tasks.
- Analysts cannot see the Assignee button or change the assignee of an incident.
- Analysts cannot see the Related Indicators (alerts) panel (Incident Details view > Find Related tab in the left-side panel).
- When adding events to incidents from the Investigate views, users can only add events to incidents to which they have access. The list of incidents to which users can add events only shows incidents that the user can access.
- When creating incidents from the Investigate views, users must have access to those incidents to view them in the Respond view. For example, when creating incidents from the Investigate view, Analysts must assign the incidents to themselves to view them in the Respond view.

Caution: These restrictions apply to all NetWitness users, except users with the **Administrators**, **Respond_Administrator**, and **SOC_Managers** roles. However, you can adjust the list of user roles whose access to incidents should not be restricted.

To restrict access to incidents:

1. Go to **(Admin) > Security** and click the **Settings** tab.
2. In the **Restrict Access to Incidents** section, select **Restrict access to incidents for all users, except for users with the roles listed below**.



3. In the list, add the user roles whose access to incidents should not be restricted.
4. Click **Apply**.
   Changes take effect on the next log in to NetWitness.

(Optional) Configure External Authentication

When a user logs in, NetWitness first attempts to authenticate locally. If no local user is found, and External Authentication configuration is enabled, an attempt is made to authenticate externally.

External authentication allows users who do not have an internal NetWitness user account to log on to NetWitness and receive role-based permissions.

NetWitness supports two methods of external authentication, Active Directory and Pluggable Authentication Modules (PAM). The below procedures describe how to configure and test each method.

Configure Active Directory

When a user logs in, NetWitness first attempts to authenticate locally. If no local user is found, and Active Directory configuration is enabled, an attempt is made to authenticate with Active Directory Service. You can configure Active Directory settings to enable authentication of external groups in the  (Admin) > Security view > Settings tab.

In an environment with multiple authentication servers, LDAP forwarding allows LDAP referral following for AD group lookups. LDAP forwarding can increase the time required to log on because AD group lookups are extended to connected authentication servers. When your AD instance attempts to contact domain controllers that are blocked by your firewall, users can experience a delay of several minutes in logging on to NetWitness. NetWitness has a configuration option that specifies whether LDAP forwarding occurs; by default, LDAP referrals are disabled. When disabled, your AD instance does not attempt to contact referred domain controllers.

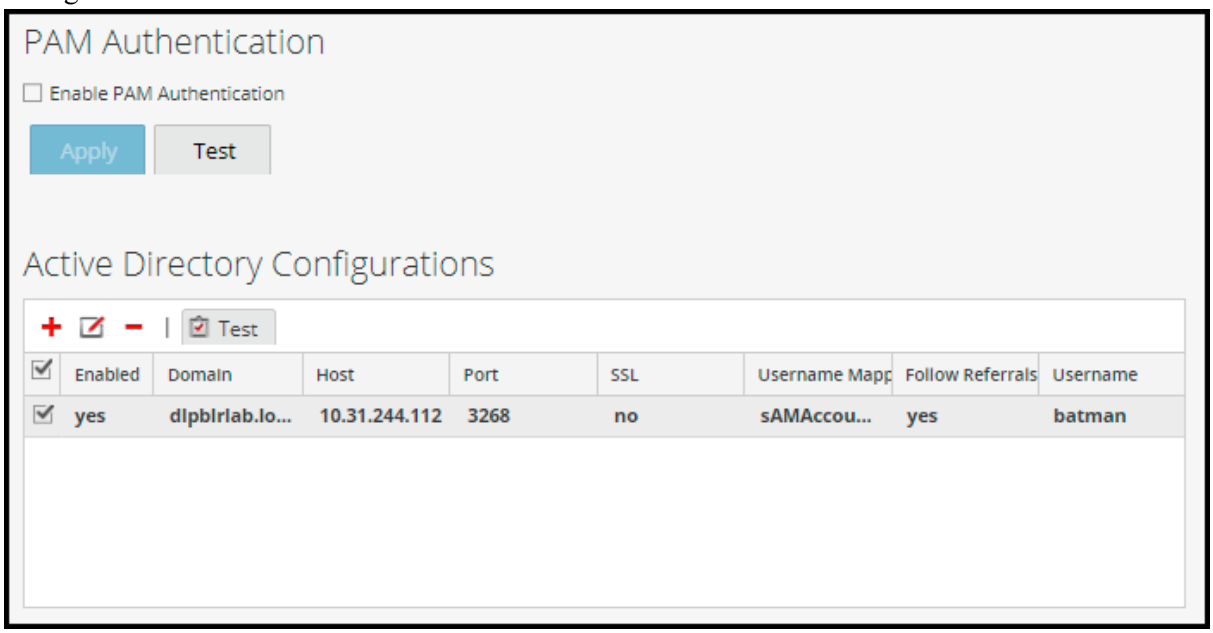
Note: The Settings tab also provides the option to enable PAM configuration, which can be used simultaneously with Active Directory configurations. For information on enabling and configuring PAM authentication, see Configure PAM Login Capability.

Configure Active Directory Authentication

To configure Active Directory authentication:

1. Go to  **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.
   The Active Directory Configurations list is displayed in the panel so that you can add or edit a

configuration.



3. Add, edit, or delete domains as necessary, as described in the following sections.
   The domains added to this list are automatically populated in the External Group Mapping tab so that you can map security roles to each group.

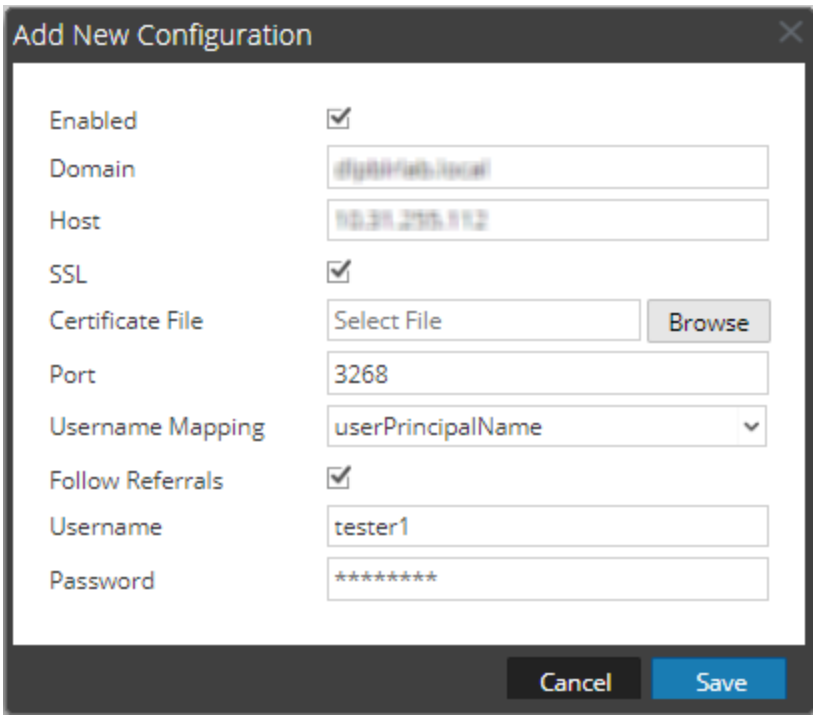
Note: To configure security roles used for Active Directory access, see (Optional) Map User Roles to External Groups.

Note: After configuring an active directory with a domain in **Admin** > **Security** > **Settings**, once you authenticate successfully using the respective active directory credentials, you are tied to that specific active directory and the domain thus configured.

Add a New Active Directory Configuration

To add a new active directory configuration in the Active Directory Configurations list:

1. Under Active Directory Configurations, click +.
   The Add New Configuration dialog is displayed.



2. Select the **Enabled** checkbox.
3. Enter **Domain**, **Host** and **Port** information for the Active Directory Service.
4. (Optional) To select SSL for this configuration, select the **SSL** checkbox. You must then enter the Active Directory server certificate file by clicking **Browse** and selecting the desired file to upload.
5. In the **Username Mapping** field, select the Active Directory search field to use for username mapping. You can select userPrincipalName (UPN) or sAMAccountName.
6. For sites that have multiple authentication servers, click **Follow Referrals** to enable or disable LDAP referral following for AD group lookups.
7. In the **Username** and **Password** fields, enter the username and password for a bind user to access Active Directory. This is usually a service account that has permissions to query the domain and validate user accounts and group membership.

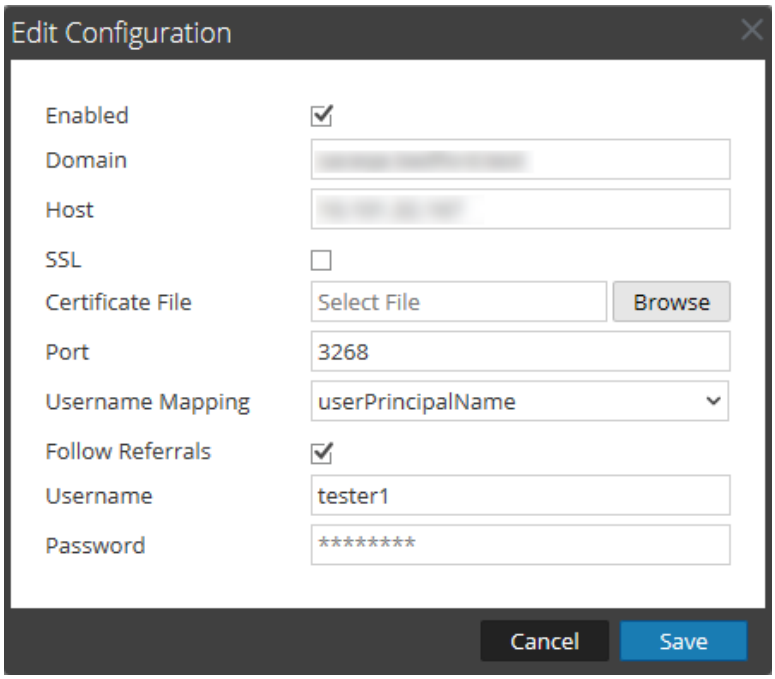
Note: If you selected sAMAccountName in the **Username Mapping** field, you must enter the username in the format "domain\user" to authenticate.

8. Click **Save**.
   The new configuration is listed in the Active Directory Configurations list.

Edit an Active Directory Configuration

To edit an active directory configuration in the Active Directory Configurations list:

1. Under **Active Directory Configurations**, select the configuration you wish to edit and click .
   The Edit Configuration dialog is displayed.



2. (Optional) Enter the **Domain**, **Host** and **Port** information for the Active Directory Service.
3. (Optional) To select SSL for this configuration, select the **SSL** checkbox. You must then enter the Active Directory server certificate file by clicking **Browse** and selecting the desired file to upload.
4. (Optional) In the **Username Mapping** field, select the the Active Directory search field to use for username mapping.
5. To specify the Follow LDAP referrals behavior in environments with multiple authentication servers, select the **Follow Referrals** checkbox.
   a. If you want to disable LDAP forwarding, clear the box.
   b. If you want to enable LDAP forwarding, select the box.
6. In the **Username** and **Password** fields, enter the username and password for a bind user to access Active Directory. This is usually a service account that has permissions to query the domain and validate user accounts and group membership.
7. Click **Save**.
   The configuration is listed in the Active Directory Configurations list.

Test an Active Directory Configuration

To test an Active Directory configuration:

1. Select the configuration to be tested from the Active Directory Configurations list.
2. In the toolbar, click Test.
   A message that the test is successful is displayed.
3. If the test does not succeed, review and edit the configuration.

Delete an Active Directory Configuration

To delete an Active Directory configuration:

1. Under Active Directory Configurations, select the configuration to be deleted from the Active Directory Configurations list.
2. In the toolbar, click −.
   A message is displayed warning you that all users in the selected Active Directory configuration will not be able to log in to NetWitness if it is deleted.
3. Do one of the following:
   a. To confirm the deletion, click **Yes**.
   b. To cancel the deletion, click **No**.

Configure PAM Login Capability

Pluggable Authentication Module (PAM) login capability involves two separate components:

- PAM for user authentication
- NSS for group authorization

Together they provide external users the capability to log on to NetWitness without having an internal NetWitness account, and to receive permissions or roles determined by mapping the external group to a NetWitness security role. Both components are required for a login to succeed.

External authentication is a system-level setting. Before configuring PAM, carefully review all of the information here.

Pluggable Authentication Modules

PAM is a Linux-provided library responsible for authenticating users against authentication providers such as RADIUS, Kerberos, and Agent for SecurID. For implementation, each authentication provider uses its own module, which is in the form of an operating system (OS) package such as pam_krb5. NetWitness uses the OS-provided PAM library, and the module that the PAM library is configured to use, to authenticate users.

Note: PAM provides only the ability to authenticate.

Name Service Switch

NSS is a Linux feature that provides databases that the OS and applications use to discover information like hostnames; user attributes like home directory, primary group, and login shell; and to list users that belong to a given group. Similar to PAM, NSS is configurable and uses modules to interact with different types of providers. NetWitness uses OS-provided NSS capabilities to authorize external PAM users by looking up whether a user is known to NSS and then requesting from NSS the groups of which that user is a member. NetWitness compares the results of the request to the NetWitness External Group Mapping and if a matching group is found, the user is granted access to log on to NetWitness with the level of security defined in the External Group Mapping.

Note: NSS does not provide authentication.

PAM and NSS Combination

Both PAM (authentication) and NSS (authorization) must succeed in order for an external user to be allowed to log on to NetWitness. The procedure for configuring and troubleshooting PAM is different than the procedure for configuring and troubleshooting NSS. The PAM examples in this guide include Kerberos, RADIUS, and SecurID. The NSS example includes UNIX. The PAM and NSS module combination used is determined by site needs.

Process Overview

To configure PAM login capability, follow the instructions in this document to complete each step:

1. Configure and test the PAM module.
2. Configure and test the NSS service.
3. Enable PAM in NetWitness Server.
4. Create group mappings in NetWitness Server.

Before beginning the setup of PAM, review the procedure and gather the external authentication server details depending on the PAM module you want to implement.

Before beginning the setup of NSS, review the procedure, identify the group names that you will use in the External Group mapping, and gather the external authentication server details, depending on the NSS service being used.

Before beginning setup of PAM in NetWitness, identify the group names that you will use in the External Group mapping. When mapping roles, the role in NetWitness must match a group name that exists in the external authentication server.

Configure and Test the PAM Module

Choose one of the following sections to set up and configure the PAM component:

- PAM Kerberos
- PAM RADIUS
- PAM Agent for SecurID

PAM Kerberos

Kerberos Communication Ports – TCP 88

To configure PAM authentication using Kerberos:

1. Execute the following command (but first verify that the `krb5-workstation` package is installed in your environment):
   `yum install krb5-workstation pam_krb5`
2. Edit the following lines in the Kerberos configuration file `/etc/krb5.conf`. Replace variables, which are delimited by <angle brackets>, with your values and omitting the angle brackets. Capitalization is required where shown.

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 dns_lookup_kdc = true
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = <DOMAIN.COM>
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 <DOMAIN.COM> = {
 kdc = <SERVER.DOMAIN.COM>
 admin_server = <SERVER.DOMAIN.COM>
 }

 [domain_realm]
 <domain.com> = <DOMAIN.COM>
 <.domain.com> = <DOMAIN.COM>
```

3. Test the Kerberos configuration with the command:
   `kinit <user>@<DOMAIN.COM>`
   No output after entering the password indicates success.
4. Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:
   `auth sufficient pam_krb5.so no_user_check`

This completes the configuration for PAM Kerberos. Now, go to the next section, Configure and Test the NSS UNIX Service.

PAM RADIUS

Radius Communication Ports - UDP 1812 or UDP 1813

To configure PAM authentication using Radius you must add the NetWitness Server to your Radius Server's Client list and configure a shared secret. Contact the Radius Server Administrator for this procedure.

To configure PAM authentication using RADIUS:

1. Execute the following command (but first verify that the `pam_radius_auth` package is installed in your environment):

   ```
   yum install pam_radius_auth
   ```

2. Edit the RADIUS configuration file, `/etc/raddb/server` as follows:

   ```
   # server[:port] shared_secret  timeout (s)
   server    secret     3
   ```

3. Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:

   ```
   auth sufficient pam_radius_auth.so
   ```

4. Execute the following command to copy the RADIUS library:

   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```

Caution: For PAM RADIUS to work, the `/etc/raddb/server` files must have write permission. The command needed for this is: `chown netwitness:netwitness /etc/raddb/server`.

Caution: You must restart the Jetty server after making the above changes for PAM RADIUS. The command for this is:
`systemctl restart jetty`

The PAM Modules and associated services output information to `/var/log/messages` and `/var/log/secure`. These outputs can be used to assist in troubleshooting configuration problems.

The following procedure is an example of the steps to configure PAM authentication for RADIUS using SecurID:

Note: The examples in these tasks use Authentication Manager as the RADIUS server.

1. Execute the following command (but first verify that the `pam_radius_auth` package is installed in your environment):

   ```
   yum install pam_radius_auth
   ```

2. Edit the RADIUS configuration file, `/etc/raddb/server` and update it with the authentication manager instance hostname, shared secret and timeout value:

   ```
   # server[:port] shared_secret timeout (s)
    111.222.33.44         secret        1
    #other-server        other-secret 3
    192.168.12.200:6369 securid      10
   ```

Note: You must comment out `127.0.0.1` and `other-server` lines and add the IP address of the authentication manager primary instance with RADIUS port number (for example, `192.168.12.200:1812`), RADIUS shared secret, and a timeout value of 10.

3. Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:

   ```
   auth sufficient pam_radius_auth.so
   ```

   Note: You can add `debug` to the end of the above line in the `/etc/pam.d/securityanalytics` file to enables PAM debugging (for example, `auth sufficient pam_radius_auth.so debug`)

4. Run the following command to copy the RADIUS library:

   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```

The PAM Modules and associated services output information to `/var/log/messages` and `/var/log/secure`.These outputs can be used to assist in troubleshooting configuration problems.

Add a RADIUS Client and Associated Agent

Note: The examples in these tasks use Authentication Manager as the RADIUS server.
You must use administrative account credentials to log on Authentication Manager Security Console.

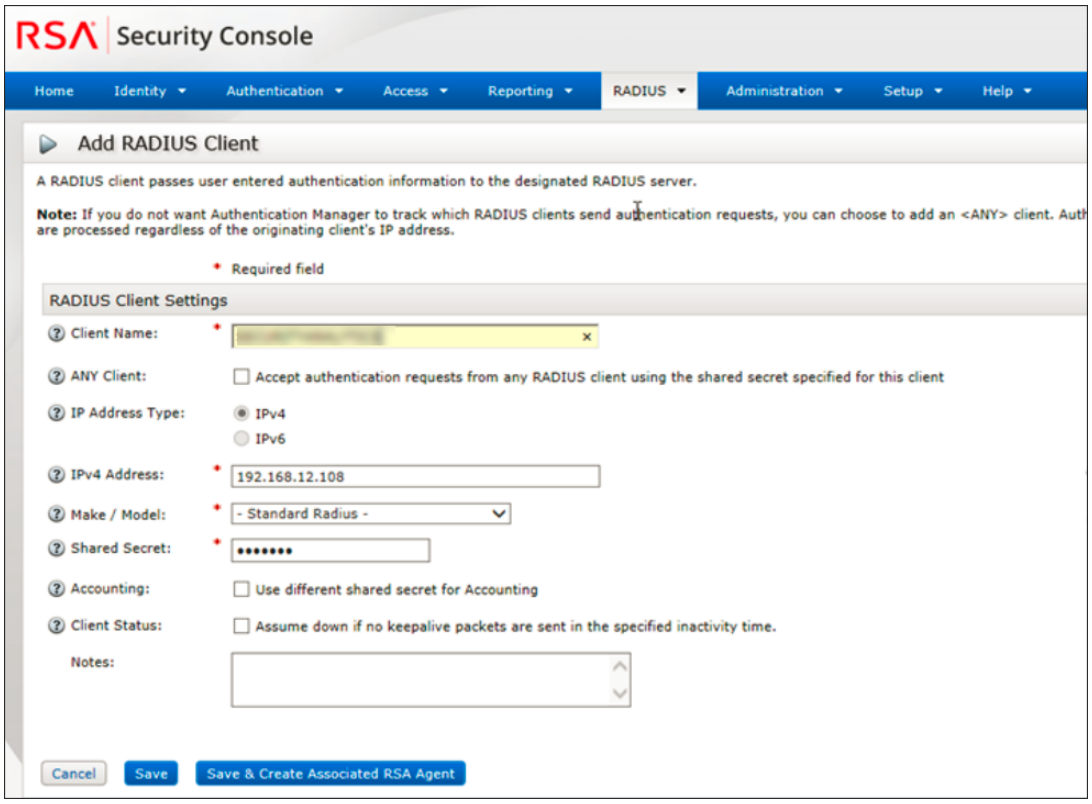
To add a RADIUS Client and Associated Agent:

1. Log on to Authentication Manager.

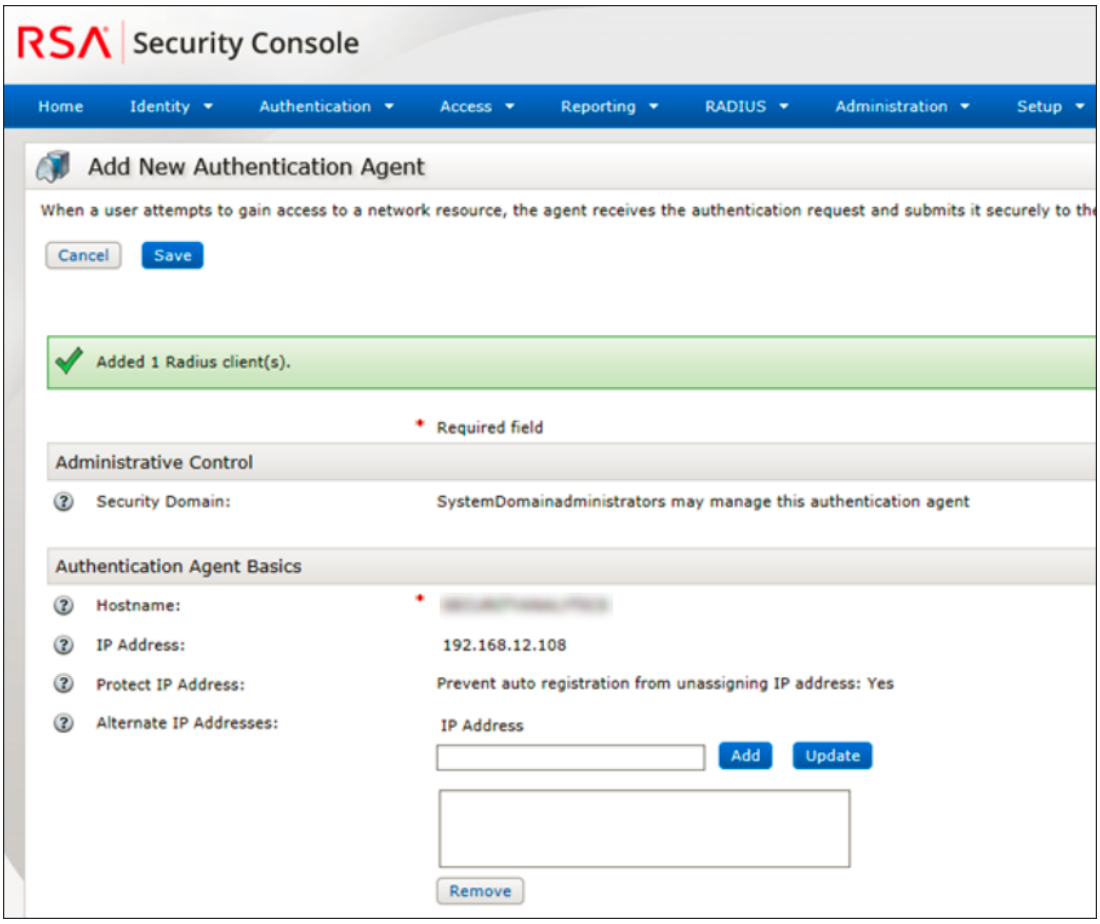
   The Security Console is displayed.

2. In the Security Console, click **RADIUS > RADIUS Client > Add New**.

   The Add RADIUS Client page is displayed.



3. In RADIUS Client Settings, provide the following information:
   a. In the **Client Name** field, enter the name of the client, for example, NetWitness.
   b. In the **IPv4 Address** field, enter the IPv4 address of the RADIUS client, for example, 192.168.12.108.
   c. In the **Make/Model** drop-down list, select the type of RADIUS client, for example, Fortinet.
   d. In the **Shared Secret** field, enter the authentication shared secret.
4. Click **Save & Create Associated Netwitness Agent**.



5. Click **Save**.

If the Authentication Manager instance is unable to find the authentication agent on the network, a warning page is displayed. Click **Yes, Save Agent**.

For more information, see the "Add a RADIUS Client" topic in *Authentication Manager 8.2 Administrator's Guide*.

This completes the configuration for PAM RADIUS. Now, go to the next section, Configure and Test the NSS UNIX Service.

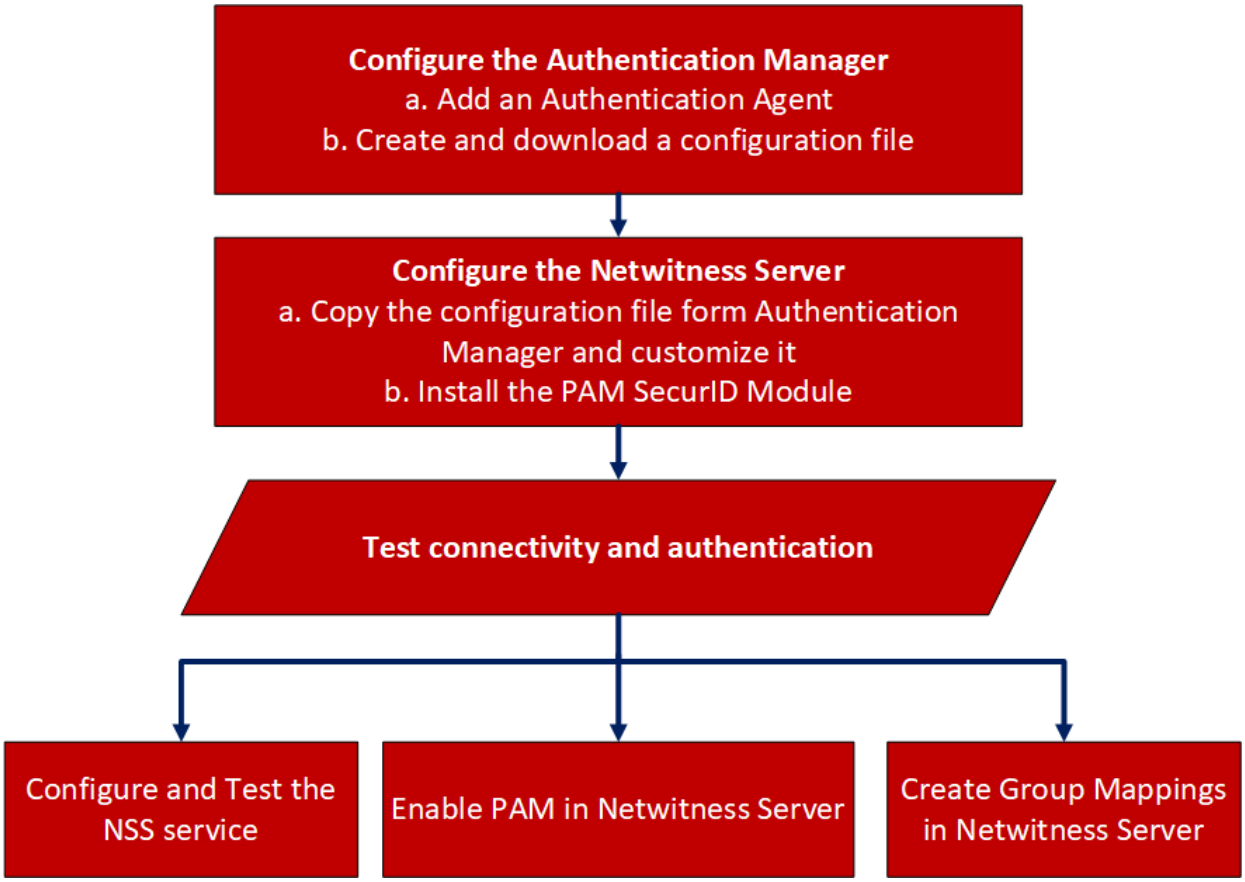
PAM Agent for SecurID

PAM Communication Port - UDP 5500

The SecurID PAM module is supported only under the following condition:

Trusted connections must be enabled and functioning between NetWitness and Core services.

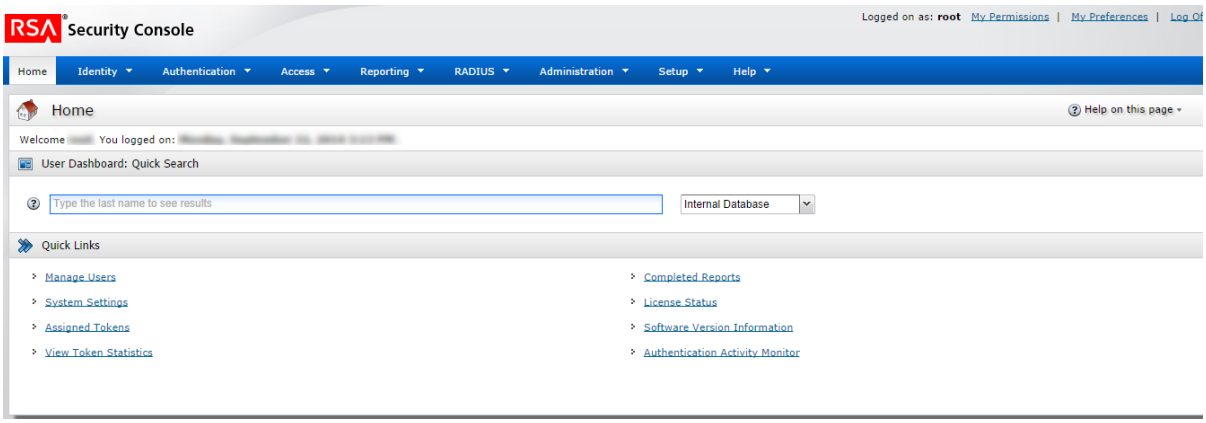
Configure the SecurID PAM Module



To configure Authentication Manager:

1. Log on to Authentication Manager.

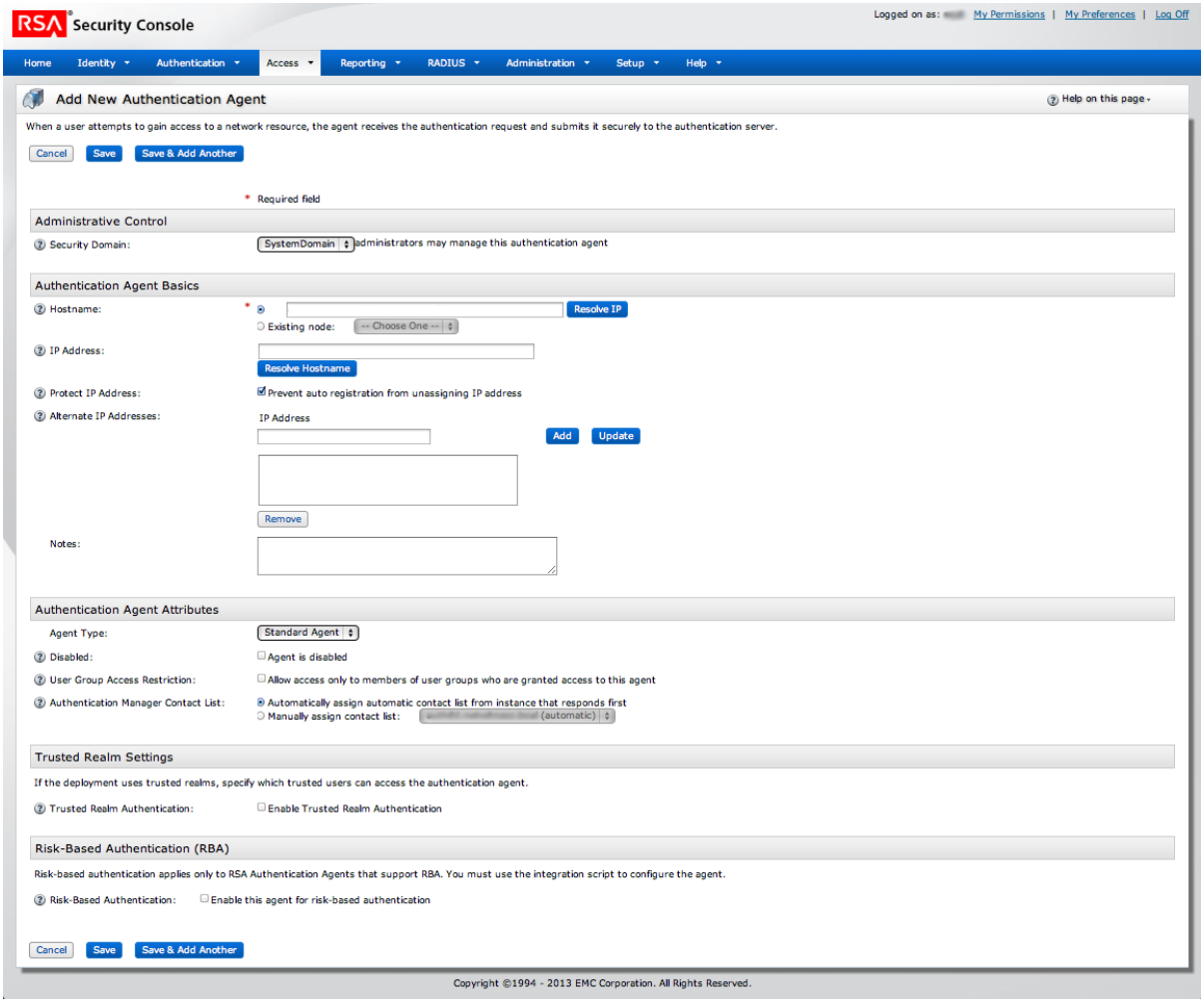
   The Security Console is displayed.



2. In the Security Console, add a new authentication agent.

   Click **Access > Authentication Agents > Add New**.

   The Add New Authentication Agent page is displayed.



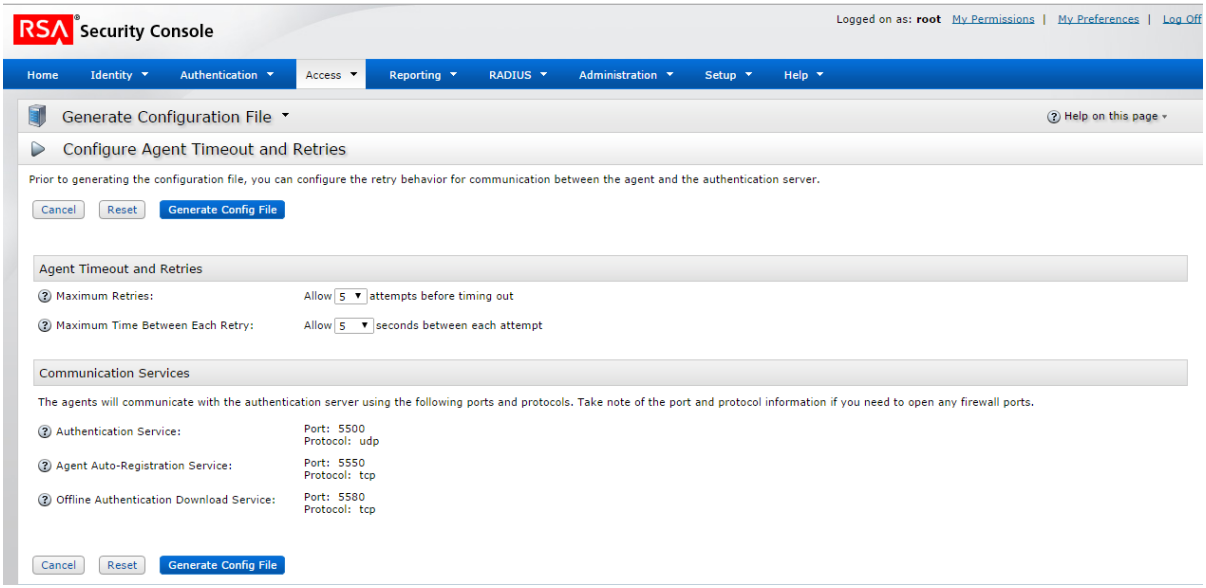
3. In the **Hostname** field, type the hostname of the NetWitness Server.
4. Click **Resolve IP**.

The IP address of the NetWitness Server is automatically displayed in the **IP Address** field.

5. Keep the default settings and click **Save**.
6. Generate a configuration file.

   Go to **Access > Authentication Agents > Generate Configuration File**.

   The Generate Configuration File page is displayed.



7. Keep the defaults and click **Generate Config File**.

   This creates **AM_Config.zip**, which contains two files.

8. Click **Download Now**.

To install and configure the PAM SecurID module:

1. On the NetWitness Server, make the following directory:

   `mkdir /var/ace`

2. On the NetWitness Server, copy `sdconf.rec` from the .zip file to `/var/ace`.
3. Create the text file `sdopts.rec` in the `/var/ace` directory.
4. Insert the following line:

   `CLIENT_IP=<IP address of NetWitness Server>`

5. Install the SecurID Authorization Agent for PAM, which is available in the yum repository:

   `yum install sid-pam-installer`

6. Run the install script:

   `/opt/rsa/pam-agent-installer/install_pam.sh`

7. Follow the prompts to accept or change the defaults.

8. Edit the NetWitness Server PAM configuration file, `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:

   ```
   auth sufficient pam_securid.so
   ```

This completes the installation of the SecurID PAM module. Next, test the connectivity and authentication. Then, follow the procedures in Configure and Test the NSS UNIX Service.

Note: If the PAM SecurID setup is not complete, it may crash the Jetty server and the NetWitness UI will not be displayed. You must wait until the PAM authentication configuration is complete and then restart the Jetty server.

To test connectivity and authentication:

1. Run `/opt/pam/bin/64bit/acetest`, and enter the **username** and **passcode**.
2. (Optional) If acetest fails, turn on debugging:

   ```
   vi/etc/sd_pam.conf
   RSATRACELEVEL=15
   ```

3. Run `/opt/pam/bin/64bit/acestatus`. The output is displayed as shown below.

   ```
   RSA ACE/Server Limits
    ---------------------
    Configuration Version : 15 Client Retries : 5
    Client Timeout : 5 DES Enabled : Yes

   RSA ACE/Static Information
    --------------------------
    Service : securid Protocol : udp Port Number : 5500

   RSA ACE/Dynamic Information
    ---------------------------
    Server Release : 8.1.0.0 Communication : 5

   RSA ACE/Server List
    -------------------
    Server Name :  auth81.netwitness.local
    Server Address :  192.168.100.10
    Server Active Address : 192.168.100.10
    Master : Yes Slave : No Primary : Yes
    Usage : Available for Authentications
   ```

4. (Optional) To troubleshoot the Authentication Manager server, go to **Reporting > Real-time Activity Monitors > Authentication Activity Monitor.** Then click **Start Monitor**.
5. If you changed the setting, reset RSATRACELEVEL to 0:

   ```
   vi/etc/sd_pam.conf
   RSATRACELEVEL=0
   ```

Caution: After installation, verify that VAR_ACE in the `/etc/sd_pam.conf` file points to the correct location of the sdconf.rec file. This is the path to the configuration files. The command needed for this is: `chown -R netwitness:netwitness /var/ace`.

This completes the configuration for PAM Agent for SecurID. Now, go to the next section, Configure and Test the NSS UNIX Service.

Configure and Test the NSS UNIX Service

Configuration

No configuration is necessary to enable the NSS UNIX module; it is enabled in the host operating system by default. To authorize a user for a specific group, simply add that user to the operating system and add them to a group:

1. Create an OS group to use add your external user to with this command:

   ```
   groupadd <groupname>
   ```

2. Add the external user to the OS with this command:

   ```
   adduser -G <groupname> -M -N <externalusername>
   ```

Note: This does NOT permit or allow access to the NetWitness Server console.

This completes the configuration for NSS UNIX. Next, go to Test NSS Functionality.

Test NSS Functionality

To test whether NSS is working with any of the previous NSS services, use the following commands:

```
getent passwd <pamUser>
 getent group <groupOfPamUser>
```

Output should be similar to:

```
[root@~]# getent passwd myuser
 myuser:*:10000:10000::/home/myuser:/bin/sh
[root@~]# getent group mygroup
 mygroup:*:10000:myuser3
```

- If neither command produces output, NSS is not working properly for external authorization. Refer to the troubleshooting guidance for your NSS module provided in this document.
- If `getent` commands succeed and authentication success is confirmed in `/var/log/secure` but NetWitness still fails to allow External users to login:
  - Was the correct group name specified for the NSS group in NW External Group Mapping? See Enable PAM and Create Group Mappings below.
  - It is possible that the NSS configuration has changed and NetWitness has not picked up the change. A reboot of the NetWitness host will cause NetWitness to pick up NSS configuration changes. A restart of the Jetty server is not sufficient.

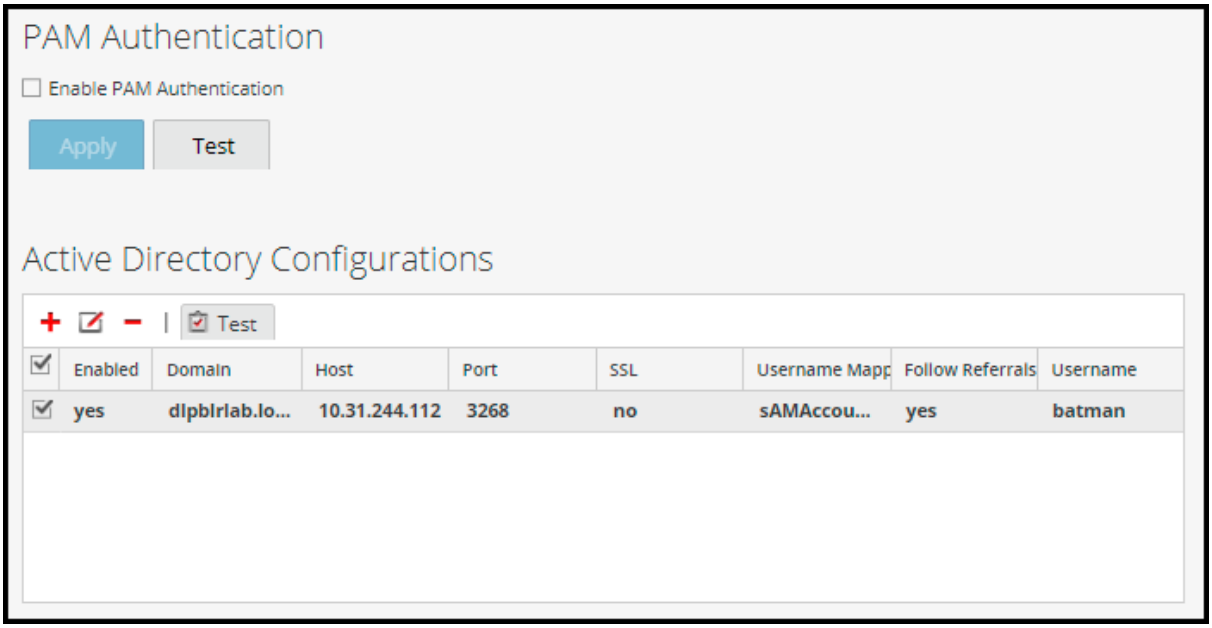
Enable PAM in NetWitness Server

1. Go to  **(Admin) > Security**.

   The Security view is displayed with the Users tab open.

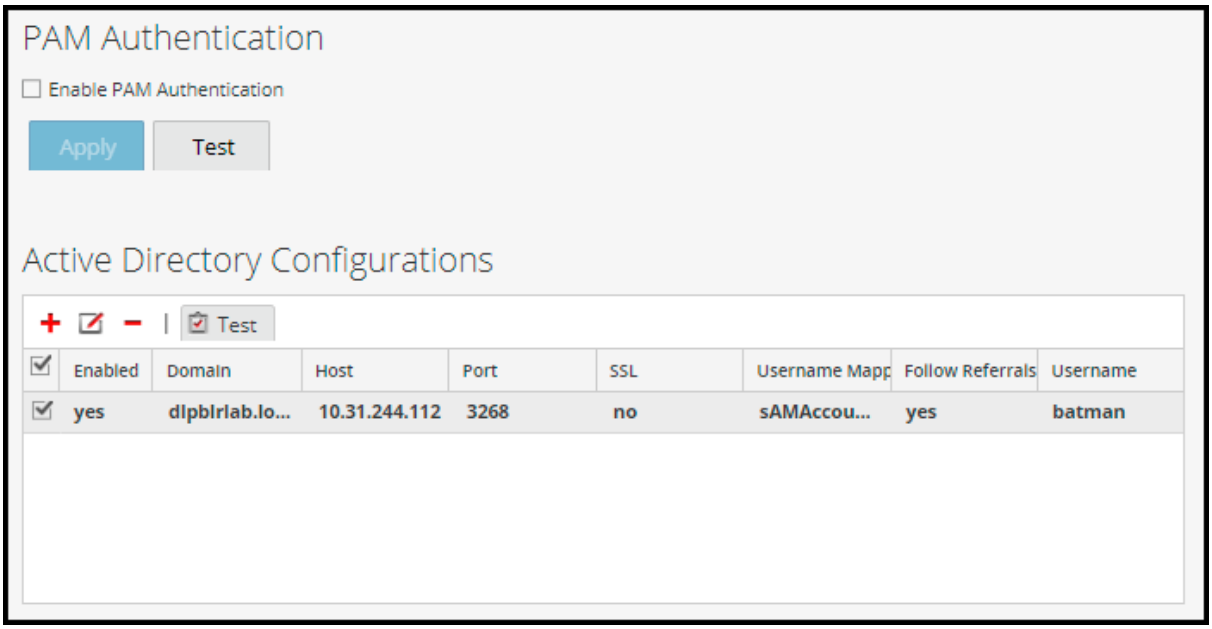
2. Click the **Settings** tab.

3. Under **PAM Authentication**, select **Enable PAM Authentication** and click **Apply**.



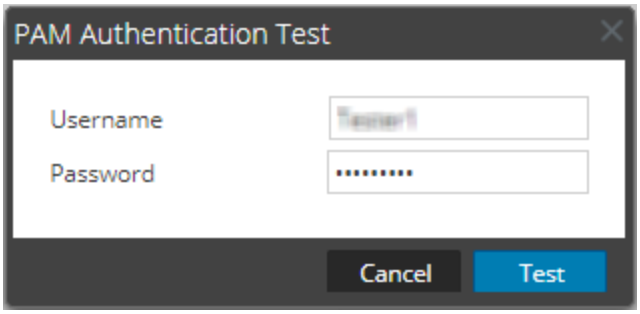
Test External Authentication for PAM

1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.
3. Under **PAM Authentication**, select **Enable PAM Authentication**.



4. Under **PAM Authentication** options, click **Test**.

The PAM Authentication Test dialog is displayed.



5. Type a user name and password that you want to test for authentication using the current PAM configuration.
6. Click **Test**.

   The external authentication method is tested to ensure connectivity.
7. If the test does not succeed, review and edit the configuration.

PAM is enabled, and Active Directory configurations will also remain enabled. PAM configurations are automatically populated in the External Group Mapping tab so that you can map security roles to each group.

Create Group Mappings in NetWitness Server

To configure security roles used for PAM access, see (Optional) Map User Roles to External Groups.

(Optional) Configure PKI Authentication

PKI (Public Key Infrastructure) authentication feature enables the user to securely login to NetWitness Platform using a smart card. The smart card is a hardware device and contains a Certificate and a password protected Private Key corresponding to the Certificate which enables PKI to validate the user. The certificate is provided by the CA and is unique for a user. For more information on how to configure PKI Authentication, see (Optional) Set Up Public Key Infrastructure (PKI) Authentication.

(Optional) Use a Custom Server Certificate

NetWitness also allows you to configure custom web server certificate to be used as NetWitness Server certificate. By default NetWitness Server uses a web server certificate generated by NetWitness for HTTPS connection. You can configure custom web server certificate even if PKI is not enabled.

Supported Keystore Formats

You must select the format that meets your requirement. The following keystore formats are supported:

- For server certificate with its private key:
  - pfx/pkcs/p12 (PKCS8/PKCS12 are the standards)
  - jks (JKS standard)

Note: The .pfx, .p12 and .jks are containers that can contain one or more private keys and its corresponding chains or certificates.

(Optional) Create a Certificate Signing Request (CSR) and Certificate Store for a Server Certificate

Note: The steps provided in this procedure allows you to create a CSR and Certificate Store for a Server Certificate.

If a server certificate is already created along with its private key, you can directly upload the certificate to the NetWitness Server. If the server certificate is not created, based on the CSR created, the CSR can be submitted to the Certificate Authority (CA) server to obtain a server certificate. Once the certificate is created, perform the following steps to package the private key and the signed certificate that must uploaded to the NetWitness Server to be used as a server certificate.

To create a CSR for a Server Certificate:

1. Change the directory to /root:

```
cd /root
```

2. Create a new directory:

```
mkdir nw_pki_server_cert
```

3. Change the directory to the newly created directory:

```
cd nw_pki_server_cert
```

4. Create a Private Key of 2048 Bits:

```
openssl genrsa -out nw_server_pki_private_key.key 2048
```

5. Create a CSR:

```
openssl req -new -sha256 -key nw_server_pki_private_key.key -out server_cert_
request.csr
```

For example, if country: US, location: RT, and unit:

CN: ABCD (Hostname or IP Address of the Machine)

For multiple names, use values such as : CN=ABCD, CN=10.XX.XXX.XX

email: example@rsa.com

6. Check the CSR and Private Key match.

```
openssl req -noout -modulus -in server_cert_request.csr | openssl sha256
openssl rsa -noout -modulus -in nw_server_pki_private_key.key | openssl sha256
```

For example:

```
[root@ABCD open_ssl_test]# openssl rsa -noout -modulus -in server_private.key
| openssl sha256
(stdin)= 88df3d1ea5b2f411712b96d2ed4a72f5
[root@ABCD open_ssl_test]# openssl req -noout -modulus -in server_cert_
request.csr | openssl sha256
(stdin)= 88df3d1ea5b2f411712b96d2ed4a72f5
```

Note: You make a note of both stdin's.

7. Submit the CSR to the CA and get a signed Server Certificate.

8. Copy the certificate in PEM format to the new directory:

```
/root/nw_pki_server_cert/signed_certificate.pem
```

9. Check the certificate for the correct public key.

```
openssl x509 -noout -modulus -in certificate.pem | openssl sha256
```

For example :

```
[root@ABCD open_ssl_test]# mv test.pem certificate.pem
[root@ABCD open_ssl_test]# openssl x509 -noout -modulus -in certificate.pem |
openssl sha256
(stdin)= 3e2f4bbd1f32ae097902afcc1893089e
[root@ABCD open_ssl_test]# openssl rsa -noout -modulus -in sa_server_pki_
private_key.key | openssl sha256
(stdin)= 3e2f4bbd1f32ae097902afcc1893089e
[root@ABCD open_ssl_test]# openssl req -noout -modulus -in server_cert_
request.csr | openssl sha256
(stdin)= 3e2f4bbd1f32ae097902afcc1893089e
```

10. Copy the Private Key and Certificate to a Key Store.

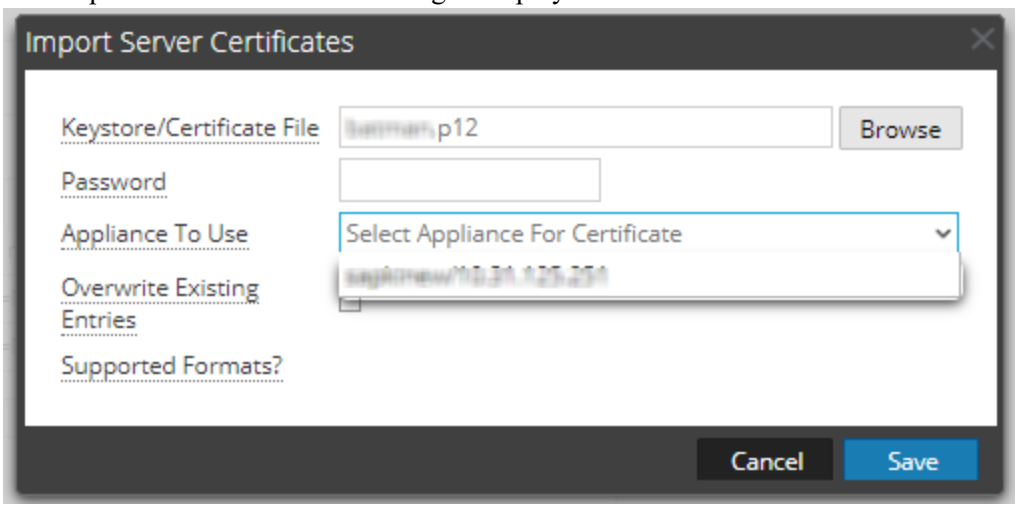
```
openssl pkcs12 -export -descert -name <myservercert> -in signed_
certificate.pem -inkey nw_server_pki_private_key.key -out keystore.p12
```

11. Enter the keystore password, for example **NetWitness@123**, to the Keystore.

Import an NW Server Certificate with its Private Key

Note: .p12, .jks, and .pfx are the supported server certificate formats. Execute the following OpenSSL command to convert certificates to the supported format:
`openssl pkcs12 -export -out cert.p12 -in cert.cer -inkey nw_server_pki_private_key.key`
Only certificates that are configured with an export password can be uploaded to the NetWitness UI.

1. Go to **(Admin) > Security.**
   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.
3. In the **Server Certificates** section, click +.
   The Import Server Certificates dialog is displayed.



4. In the **Keystore/Certificate File** field, click **Browse** and select the keystore.
5. In the **Password** field, enter the keystore password.
6. In the **Appliance To Use** field, select the appliance for which you want to use this certificate.
7. (Optional) Select the **Overwrite Existing Entries** checkbox to overwrite the entries of the certificate that is already added.
8. Click **Save.**
   The NetWitness Server certificate with its private key is successfully added to NetWitness.

Note: When the certificate is being applied on the selected appliance, no other operation on PKI can be performed until the process is completed.
Double-click on the added entries to view the details of the certificate.

9. To apply the server certificate on a server, select a certificate and click .

Note: Uploading a keystore will add the server certificate and its private key locally. To apply a server certificate on a server, you need to select a server certificate and click the synchronization button  . All server certificates are also synchronized on the appliances when PKI is enabled.

Note: To complete the certificate update process, log into the Admin Server (node-0) stop and start the nginx with the command `systemctl restart nginx`.

(Optional) Create a Customized Login Banner

You can create and enable customized login banner that is displayed before users log on to NetWitness asking users to agree the conditions. Users who do not agree are not able to log on.

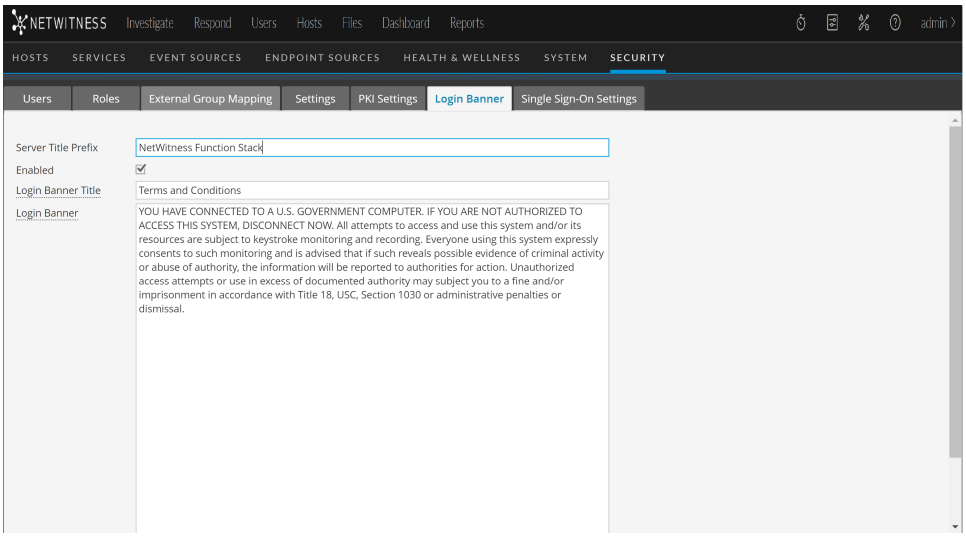
To create and enable a customized login banner:

1. Go to  **(Admin) > Security**.

   The Security view is displayed with the Users tab open.

2. Click the **Login Banner** tab and select the **Enabled** checkbox to toggle between enabling and disabling the banner.

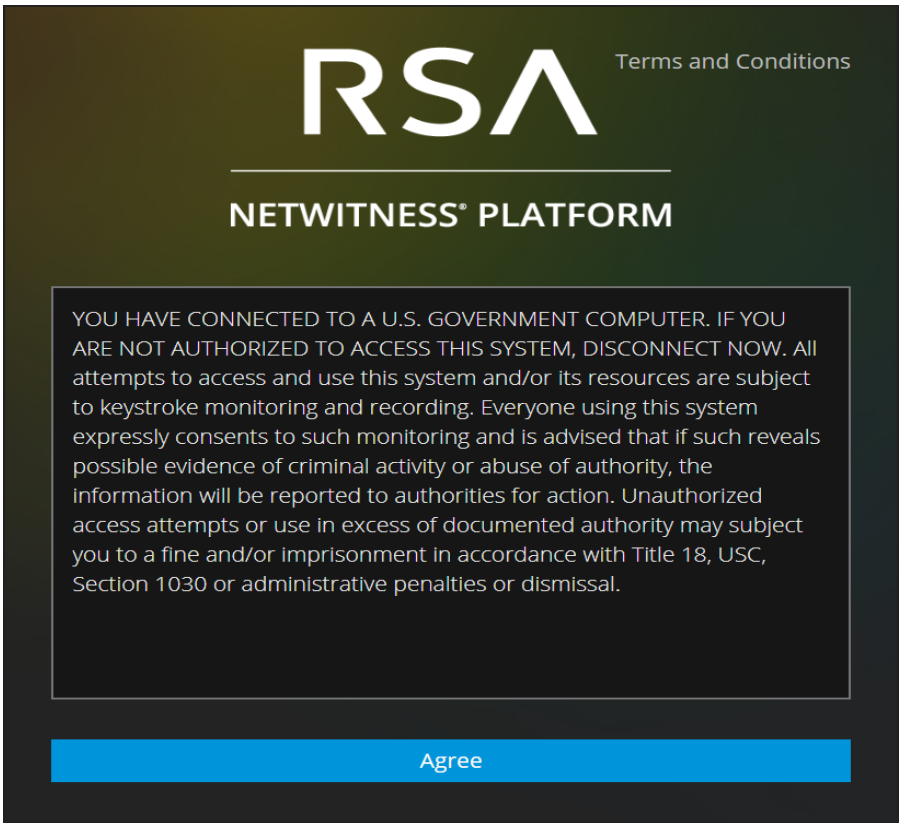
   When Enable is selected, the Login Banner Title and Login Banner fields become active with default content in place.



3. Use the default content or type the custom title and content for your banner and click **Apply**. The banner is enabled and becomes active immediately.

   Note: While both plain text and text with HTML tags are allowed, any suspicious tags will be removed. For example, all links must use HTTPS protocols.

4. To test the banner, log out. The banner is displayed in front of the fields for entering NetWitness credentials.



5. Click **Agree**.

   The banner closes and you can log on.

How Role-Based Access Control Works

In the NetWitness Platform, roles determine what users can do. A role has permissions assigned to it and you must assign a role to each user. The user then has permission to do what the role allows. Role-bsed access control (RBAC) is established when there is a trusted connection between NetWitness Server and a Core service.

Preconfigured Roles

To simplify the process of creating roles and assigning permissions, there are preconfigured roles in NetWitness. You can also add roles customized for your organization.

The following table lists each preconfigured role and the permissions assigned to it. All permissions are assigned to the Administrators role. A subset of permissions is assigned to each of the other roles.

Role	Permission
Administrators	Full system access. The System Administrators persona is granted all permissions by default.
Analysts	Access to meta and session content but not to configurations. The Security Operation Center (SOC) Analysts persona is centered around investigation, ESA Alerting, Reporting, and Respond, but not system configuration.
Reporting_Engine_ Content_Administrators	Access to manage the Live content. Users with the Reporting Engine Content Administrator role can deploy Reporting Engine content (rules, reports, charts, and lists) from Live Content, view and manage permissions to the deployed content in Reporting Engine.
Data_Privacy_Officers	The Data Privacy Officer (DPO) persona is similar to Administrators with additional focus on configuration options that manage obfuscation and viewing of sensitive data within the system (see the *Data Privacy Management Guide*). Users with the DPO role can see which meta keys are flagged for obfuscation, and they also see obfuscated meta keys and values created for the flagged meta keys.
Malware_Analysts	Access to investigations and malware events. The only access granted to the Malware Analysts persona is the Malware Analysis module.
Operators	Access to configurations but not to meta and session content. The System Operators persona is focused on system configuration, but not investigation, ESA, Alerting, Reporting, and Respond.
Respond_Administrator	Access to all Respond permissions. The Respond Administrator persona is focused on system configuration of Respond.
SOC_Managers	Same access as Analysts plus additional permission to handle incidents. The SOC Managers persona is identical to Analysts, but with permissions necessary to configure Respond.

Role	Permission
UEBA_Analysts	Access to the NetWitness UEBA service in the **Investigate** > **Users** view. NetWitness UEBA is an advanced analytics solution for discovering, investigating, and monitoring risky behaviors across all entities in your network environment. **Note:** You do not need to set up specific permissions for this role. You only need to assign this role to a user, and that user will have access to NetWitness UEBA.

Trusted Connections Between Server and Service

In a trusted connection, a service explicitly trusts NetWitness Server to manage and authenticate users. This reduces administration on each service because authenticated users do not have to be defined locally in each Core service.

As the following table shows, you perform all user management tasks on the server.

Task	Location
Add a user	Server
Maintain usernames	Server
Maintain passwords	Server
Authenticate internal NetWitness users	Server
(Optional) Authenticate external users with: - Active Directory - PAM	 Server Server
Install and configure PAM	Server

The benefits of a trusted connection and centralized user management are that:

- You perform all user administration tasks once, on NetWitness Server only.
- You control access to services but do not have to set up and authenticate users on the services.
- Users enter passwords once at NetWitness logon and are authenticated by the server.
- Users, already authenticated by the server, access every Core service in (Admin) > Services without entering a password.

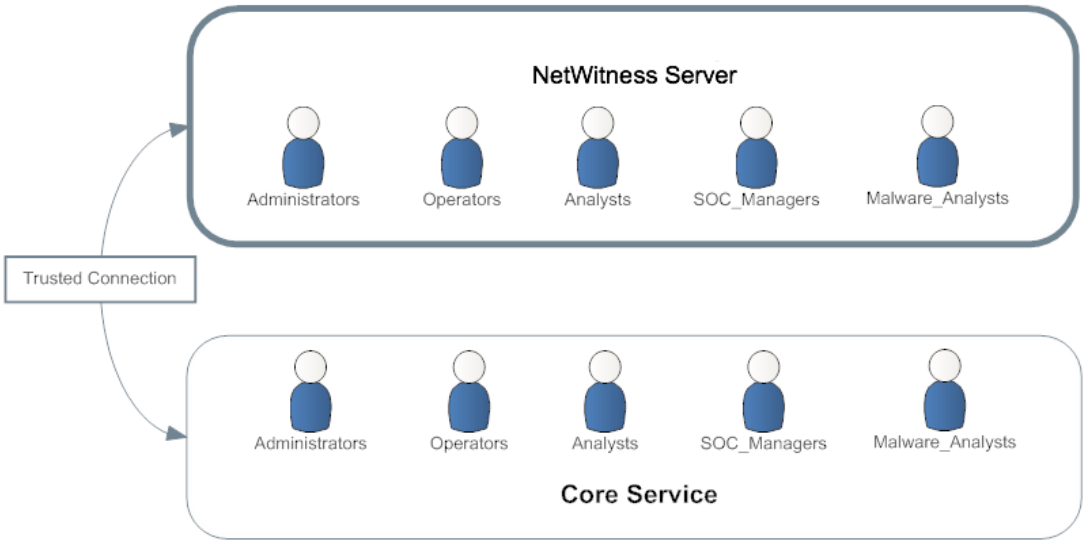
How Trusted Connections Are Established

When you install or upgrade to 11.x, trusted connections are established by default with two settings:

- SSL is enabled.
- The Core service is connected to an encrypted SSL port.

Common Role Names on the Server and Services

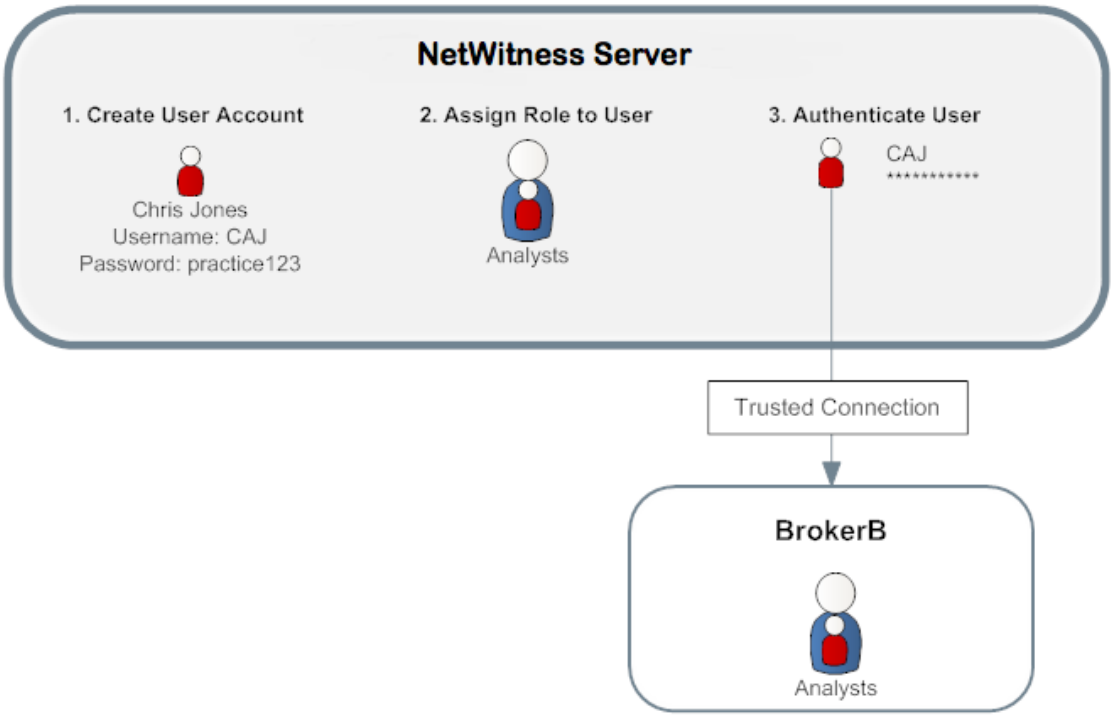
Trusted connections rely on common role names on the server and service. On a fresh installation, NetWitness installs the five preconfigured roles on the server and each Core service.



If you add a custom role, such as JuniorAnalysts, you must add the role to each service, such as ArchiverA and BrokerB. Role names are case-senstive, cannot contain spaces and must be identical. For example, JuniorAnalyst (singular) and JuniorAnalysts (plural) do not meet the requirements for common role names.

End-to-End Workflow for User Setup and Service Access

This workflow shows how role-based access control works when there is a trusted connection between NetWitness Server and the service BrokerB.



1. On NetWitness Server, create an account for a new user:
   Name: Chris Jones
   Username: CAJ
   Password: practice123
2. Determine if you want to assign a preconfigured or custom role to Chris Jones:
   - **Preconfigured role**
     a. Keep or modify the default permissions assigned to the **Analysts role,** which include permissions such as access to the Alerting, Investigation and Malware modules,
     b. Assign the Analysts role to Chris Jones.
   - **Custom role**
     a. Create the custom role, such as JuniorAnalysts.
     b. Assign permissions to the **JuniorAnalysts role**.
     c. Assign the JuniorAnalysts role to Chris Jones.
     d. Add the JuniorAnalysts role to the service, such as BrokerB.
3. The user, Chris Jones, logs on to NetWitness Server:

- Username: CAJ
- Password: practice123

4. The server authenticates Chris.
5. The trusted connection allows the authenticated user, Chris, to access BrokerB without entering another password.

For more detailed descriptions and procedures, see Manage Users with Roles and Permissions.

Role Permissions

InNetWitness, user can access each module, dashlet, and view is restricted based on the assigned permissions. You can locate these role permissions in the Add or Edit Roles dialogs accessible from the  (Admin) > **Security** > **Roles** tab.

In the Add or Edit Role dialogs, the tabs in the Permission section represent different areas of NetWitness and show the available permissions for those areas. For example, the Administration tab shows the permissions available in the Admin view.

Note: There is no Configure tab in the Add/Edit Role dialogs that corresponds to the Configure view. To assign permissions in the Configure view, assign permissions to the views contained within the Configure view: Live Content (Live), Incident Rules (Incidents), Respond Notifications (Incidents, Respond-server, Integration server), ESA Rules (Alerting), Subscriptions (Live), and Custom Feeds (Live).

Note: To the left of the Administration tab is a tab marked with an asterisk (*). This tab indicates access to management of backend services only.

The tables that follow show the default permissions assigned to each NetWitness user role:

- Administrators
- Respond Administrators (RAs)
- Reporting Engine Content Administrators (RE CAs)
- Data Privacy Officers (DPOs)
- SOC Managers (SOC Mgrs)
- Operators
- Malware Analysts (MAs)
- Analysts
- UEBA Analysts

Since the Administrators role has all of the permissions by default, it is not included in the tables.

Service Permissions Format for New Services

The service permissions for some new NetWitness services contain three parts in the following format:

<service name>.<resource>.<action>

For example, for the **investigate-server.metrics.read** permission:

- `service name` = **investigate-server**
- `resource` = **metrics**
- `action` = **read**

Users assigned this permission can read any metrics that the investigate-server service exposes.

Admin-server

The following table describes the permissions in the Admin-server tab.

Permission	Description
admin-server.configuration.manage	Permission to modify all service configuration parameters
admin-server.health.read	Permission to view any health notifications that the service exposes
admin-server.logs.manage	Permission to change log-related configuration
admin-server.metrics.read	Permission to view any metrics that the service exposes
admin-server.process.manage	Permission to start and stop the service
admin-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
admin-server.security.read	Permission to view security-related resources

Administration

The following table describes the list of permissions in Administration tab.

Permission	Description
Access Administration Module	Permission to access all the administration modules
Access Health & Wellness	Permission to access the health and wellness module
Apply System Updates	Permission to update the system
Can Opt In to Live Intelligence Sharing	Permission to opt for Live Intelligence sharing
Manage Advanced Settings	Permission to modify the advanced settings
Manage ATD Settings	Permission to modify the ATD settings
Manage Auditing	Permission to modify the auditing

Permission	Description
Manage Email	Permission to change the email settings
Manage Global Auditing	Permission to modify global auditing
Manage Health & Wellness Policy	Permission to update the health & wellness policy
Manage Jobs	Permission to change the job settings
Manage LLS	Permission to modify LLS
Manage Logs	Permission to modify log related configurations
Manage Notifications	Permission to change notification settings
Manage Plugins	Permission to modify the plugins
Manage Predicates	Permission to modify the predicates
Manage Reconstruction	Permission to change the reconstruction
Manage Security	Permission to update the security settings
Manage Services	Permission to start and stop the services
Manage SSL Security	Permission to manage PKI setting
Manage System Settings	Permission to the modify the system settings
Modify ESA Settings	Permission to modify the ESA settings
Modify Event Sources	Permission to modify the ESA sources
Modify Hosts	Permission to modify the hosts
Modify Services	Permission to modify the services
View Event Sources	Permission to view the event sources
View Health & Wellness Policy	Permission to view the health & wellness policy
View Health & Wellness Stats Browser	Permission to view the health and wellness status in the browser
View Hosts	Permission to view the hosts
View Services	Permission to view the services
View Unified Sources	Permission to view the unified sources

The following table lists the permissions in the Administration tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts	UEBA Analysts
Access Administration Module		Yes	Yes	Yes	Yes	Yes	
Access Health & Wellness		Yes	Yes	Yes	Yes	Yes	
Apply System Updates				Yes			
Can Opt In to Live Intelligence Sharing				Yes			
Manage Advanced Settings				Yes			
Manage ATD Settings	Yes	Yes	Yes	Yes			
Manage Auditing		Yes		Yes			
Manage Email				Yes			
Manage Global Auditing		Yes		Yes			
Manage Health & Wellness Policy				Yes			
Manage Jobs		Yes	Yes	Yes			
Manage LLS				Yes			
Manage Logs		Yes		Yes			
Manage Notifications				Yes			
Manage Plugins		Yes	Yes	Yes		Yes	
Manage Predicates				Yes			
Manage Reconstruction				Yes			

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts	UEBA Analysts
Manage Security		Yes		Yes			
Manage Services		Yes		Yes			
Manage SSL Security							
Manage System Settings		Yes	Yes	Yes		Yes	
Modify ESA Settings				Yes			
Modify Event Sources				Yes			
Modify Hosts				Yes			
Modify Services		Yes		Yes			
View Event Sources			Yes	Yes			
View Health & Wellness Policy			Yes	Yes		Yes	
View Health & Wellness Stats Browser		Yes	Yes	Yes		Yes	
View Hosts		Yes		Yes			
View Services		Yes		Yes			
View Unified Sources		Yes	Yes	Yes		Yes	

Alerting

The following table describes the permissions in the Alerting tab.

Permission	Description
Access Alerting Module	Permission to access the alerting module
Manage Rules	Permission to update the rules

Permission	Description
View Alerts	Permission to view the alerts
View Rules	Permission to view the rules

The following table lists the permissions in the Alerting tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Access Alerting Module	Yes	Yes	Yes	Yes		Yes
Manage Rules	Yes	Yes	Yes	Yes		
View Alerts	Yes	Yes	Yes			Yes
View Rules		Yes	Yes	Yes		

Config-server

The following table describes the permissions in the Config-server tab. The Administrators role has all of the permissions and is the only role granted permissions by default.

Permission	Description
config-server.*	All permissions (everything below)
config-server.configuration.manage	Permission to modify all service configuration parameters
config-server.health.read	Permission to view any health notifications that the service exposes
config-server.logs.manage	Permission to change log-related configuration
config-server.metrics.read	Permission to view any metrics that the service exposes
config-server.process.manage	Permission to start and stop the service
config-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
config-server.security.read	Permission to view security-related resources

Content-server

The following table describes the permissions in the Content-server tab.

Permission	Description
content-server.*	All permissions (everything below)
content-server.collection.read	Permission to read selective collection content
content-server.configuration.manage	Permission to modify all service configuration parameters
content-server.health.read	Permission to view any health notifications that the service exposes
content-server.logparser.manage	Permission to manage log parser configurations
content-server.logparser.read	Permission to view log parser configurations
content-server.logs.manage	Permission to change log-related configuration
content-server.metrics.read	Permission to view any metrics that the service exposes
content-server.policy.read	Permission to read policies
content-server.process.manage	Permission to start and stop the service
content-server.rule.manage	Permission to manage content rules
content-server.rule.read	Permission to view content rules
content-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
content-server.security.read	Permission to view security-related resources

The following table lists the permissions in the Content-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrator role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
content-server.*		Yes		Yes		
content-server.collection.read						
content-server.configuration.manage						
content-server.health.read						
content-server.logparser.manage						
content-server.logparser.read			Yes			Yes
content-server.logs.manage						

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
content-server.metrics.read						
content-server.policy.read						
content-server.process.manage						
content-server.rule.manage						
content-server.rule.read						
content-server.security.manage						
content-server.security.read						

Contexthub-server

The following table describes the permissions in the Contexthub-server tab.

Permission	Description
contexthub-server.*	All permissions (everything below)
contexthub-server.configuration.manage	Permission to modify all service configuration parameters
contexthub-server.connection.manage	Permission to modify all connection settings
contexthub-server.connection.read	Permission to view all connection settings
contexthub-server.connectiontypes.read	Permission to view all configured connection types
contexthub-server.datasource.manage	Permission to modify data source settings
contexthub-server.datasource.read	Permission to view data source settings
contexthub-server.health.read	Permission to view any health notifications that the service exposes
contexthub-server.listentries.manage	Permission to modify list entries
contexthub-server.logs.manage	Permission to change log-related configuration
contexthub-server.metrics.read	Permission to view any metrics that the service exposes
contexthub-server.process.manage	Permission to start and stop the service

Permission	Description
contexthub-server.query.read	Permission to view queries
contexthub-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
contexthub-server.security.read	Permission to view security-related resources
contexthub-server.stix.read	Permission to view stix settings
contexthub-server.taxiidatasource.manage	Permission to modify settings for the taxii data source
contexthub-server.taxiidatasource.read	Permission to view settings for the taxii data source

The following table lists the permissions in the Contexthub-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrator role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
contexthub-server.*		Yes				
contexthub-server.configuration.manage						
contexthub-server.connection.manage						
contexthub-server.connection.read	Yes		Yes		Yes	Yes
contexthub-server.connectiontypes.read			Yes			
contexthub-server.datasource.manage	Yes		Yes		Yes	Yes
contexthub-server.datasource.read	Yes		Yes		Yes	Yes
contexthub-server.health.read						
contexthub-server.listentries.manage	Yes		Yes		Yes	Yes
contexthub-server.logs.manage						
contexthub-server.metrics.read						

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
contexthub-server.process.manage						
contexthub-server.query.read	Yes		Yes		Yes	Yes
contexthub-server.security.manage						
contexthub-server.security.read						
contexthub-server.stix.read			Yes		Yes	Yes
contexthub-server.taxiidatasource.manage			Yes		Yes	Yes
contexthub-server.taxiidatasource.read			Yes		Yes	Yes

Correlation-server

The following table describes the permissions in the Correlation-server tab. These permissions pertain to ESA Correlation.

Permission	Description
correlation-server.*	All permissions (everything below)
correlation-server.configuration.manage	Permission to modify all service configuration parameters
correlation-server.endpoint.manage	Permission to modify all endpoint configuration parameters
correlation-server.endpoint.read	Permission to view all endpoint configuration parameters
correlation-server.engine.manage	Permission to modify all engine configuration parameters
correlation-server.engine.read	Permission to view all engine configuration parameters
correlation-server.esperrule.manage	Permission to modify all esperrule configuration parameters
correlation-server.esperrule.read	Permission to view all esperrule configuration parameters
correlation-server.health.read	Permission to view any health notifications that the service exposes
correlation-server.keyvaluerule.manage	Permission to modify all keyvaluerule configuration parameters
correlation-server.keyvaluerule.read	Permission to view all keyvaluerule configuration parameters

Permission	Description
correlation-server.logs.manage	Permission to change log-related configuration
correlation-server.metrics.read	Permission to view any metrics that the service exposes
correlation-server.module.manage	Permission to modify each module
correlation-server.module.read	Permission to view each module
correlation-server.process.manage	Permission to start and stop the service
correlation-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
correlation-server.security.read	Permission to view security-related resources
correlation-server.stream.manage	Permission to edit stream configuration settings
correlation-server.stream.read	Permission to view stream configuration settings
correlation-server.telemetry.read	Permission to view telemetry configuration settings

The following table lists the permissions in the Correlation-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrator role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
correlation-server.*		Yes				
correlation-server.configuration.manage						
correlation-server.endpoint.manage						
correlation-server.endpoint.read						
correlation-server.engine.manage	Yes		Yes	Yes		
correlation-server.engine.read	Yes		Yes	Yes		
correlation-server.esperrule.manage						
correlation-server.esperrule.read						
correlation-server.health.read						

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
correlation-server.keyvaluerule.manage						
correlation-server.keyvaluerule.read						
correlation-server.logs.manage						
correlation-server.metrics.read						
correlation-server.module.manage	Yes		Yes	Yes		
correlation-server.module.read	Yes		Yes	Yes		
correlation-server.process.manage						
correlation-server.security.manage						
correlation-server.security.read						
correlation-server.stream.manage	Yes		Yes	Yes		
correlation-server.stream.read	Yes		Yes	Yes		
correlation-server.telemetry.read						

Dashboard

The following table describes the permissions in the Dashboard tab.

Permission	Description
Dashlet Access - Admin Device List Dashlet	Permission to access Admin Device List Dashlet
Dashlet Access - Admin Device Monitor Dashlet	Permission to access Admin Device Monitor Dashlet
Dashlet Access - Admin News Dashlet	Permission to access Admin News Dashlet
Dashlet Access - Alert Variance Dashlet	Permission to access Alert Variance Dashlet

Permission	Description
Dashlet Access - Alerting Recent Alerts Dashlet	Permission to access Alerting Recent Alerts Dashlet
Dashlet Access - Investigation Jobs Dashlet	Permission to access Investigation Jobs Dashlet
Dashlet Access - Investigation Top Values Dashlet	Permission to access Investigation Top Values Dashlet
Dashlet Access - Live Featured Resources Dashlet	Permission to access Live Featured Resources Dashlet
Dashlet Access - Live New Resources Dashlet	Permission to access Live New Resources Dashlet
Dashlet Access - Live Subscriptions Dashlet	Permission to access Live Subscriptions Dashlet
Dashlet Access - Live Updated Resources Dashlet	Permission to access Live Updated Resources Dashlet
Dashlet Access - Malware Jobs Dashlet	Permission to access Malware Jobs Dashlet
Dashlet Access - Reporting Recent Report Dashlet	Permission to access Reporting Recent Report Dashlet
Dashlet Access - Reporting Charts Dashlet	Permission to access Reporting Charts Dashlet
Dashlet Access - Top Alerts Dashlet	Permission to access Top Alerts Dashlet
Dashlet Access - Unified First Watch Dashlet	Permission to access Unified First Watch Dashlet
Dashlet Access - Unified Shortcuts Dashlet	Permission to access Unified Shortcuts Dashlet

The following table lists the permissions in the Dashboard tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RA	DPOs	SOC Mgrs	Operators	MAs	Analysts
Dashlet Access - Admin Device List Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Admin Device Monitor Dashlet		Yes				
Dashlet Access - Admin News Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Alert Variance Dashlet	Yes	Yes	Yes			Yes
Dashlet Access - Alerting Recent Alerts Dashlet	Yes	Yes	Yes			Yes

Permission	RA	DPOs	SOC Mgrs	Operators	MAs	Analysts
Dashlet Access - Investigation Jobs Dashlet	Yes	Yes	Yes			Yes
Dashlet Access - Investigation Top Values Dashlet	Yes	Yes	Yes			Yes
Dashlet Access - Live Featured Resources Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Live New Resources Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Live Subscriptions Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Live Updated Resources Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Malware Jobs Dashlet	Yes	Yes	Yes			Yes
Dashlet Access - Reporting Recent Report Dashlet	Yes	Yes	Yes			Yes
Dashlet Access - Reporting Charts Dashlet	Yes	Yes	Yes			Yes
Dashlet Access - Top Alerts Dashlet	Yes	Yes	Yes			Yes
Dashlet Access - Unified First Watch Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Unified Shortcuts Dashlet	Yes	Yes	Yes	Yes		Yes

Endpoint-broker-server

The following table describes the permissions in the Endpoint Broker server tab.

Permission	Description
endpoint-broker-server*	All permissions (everything below)
endpoint-broker-server.agent.manage	Permission to manage the agent, that is start or stop scan, downloading file from host, delete agent data from the Endpoint Log Hybrid and so on.

Permission	Description
endpoint-broker-server.agent.read	Permission to view the endpoint data received from the agent such as host, file, certificate, events and so on.
endpoint-broker-server.configuration.manage	Permission to modify all endpoint broker configuration parameters
endpoint-broker-server.health.read	Permission to view any health notifications that the service exposes
endpoint-broker-server.logs.manage	Permission to change log-related configuration
endpoint-broker-server.metrics.read	Permission to view any metrics that the service exposes
endpoint-broker-server.policy.read	Permission to view existing policy details
endpoint-broker-server.process.manage	Permission to start and stop the service
endpoint-broker-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
endpoint-broker-server.security.read	Permission to view security-related resources

The following table lists the permissions in the Endpoint-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrator role has all of the permissions by default and is not listed.

Permission	RA	DPOs	SOC Mgrs	Operators	MAs	Analysts
endpoint-broker-server*						
endpoint-broker-server.agent.manage				Yes		Yes
endpoint-broker-server.agent.read				Yes		Yes
endpoint-broker-server.configuration.manage						
endpoint-broker-server.health.read						
endpoint-broker-server.logs.manage						
endpoint-broker-server.metrics.read						
endpoint-broker-server.policy.read						Yes

Permission	RA	DPOs	SOC Mgrs	Operators	MAs	Analysts
endpoint-broker-server.process.manage						
endpoint-broker-server.security.manage						
endpoint-broker-server.security.read						

Endpoint-server

The following table describes the permissions in the Endpoint-server tab.

Permission	Description
endpoint-server*	All permissions (everything below)
endpoint-server.agent.manage	Permission to generate and download the agent packager. Permission to manage the agent, that is start or stop scan, downloading files, master file table (MFT), memory dumps from host, isolate host from network, delete agent data from the Endpoint Log Hybrid and so on Note: Analyze file, Scan With OPSWAT, Save Local Copy have been moved to endpoint-server.file.analyze (from version 11.7)
endpoint-server.agent.read	Permission to view the agent packager configuration Permission to view the endpoint data received from the agent such as host, file, certificate, events, and so on
endpoint-server.agentupdate.manage	Permission to upgrade agent and uninstall agent
endpoint-server.ca.manage	Permission to generate and download the agent packager Permission to upgrade agent
endpoint-server.ca.read	Permission to generate and download the agent packager
endpoint-server.configuration.manage	Permission to modify all endpoint configuration parameters
endpoint-server.file.analyze	Permission to analyze file, save local copy, and initiate OPSWAT scans
endpoint-server.filter.manage	Permission to save, modify, and delete filters
endpoint-server.filter.read	Permission to view filters

Permission	Description
endpoint-server.health.read	Permission to view any health notifications that the service exposes
endpoint-server.logs.manage	Permission to change log-related configuration
endpoint-server.metrics.read	Permission to view any metrics that the service exposes
endpoint-server.policy.read	Permission to view existing policy details
endpoint-server.process.manage	Permission to start and stop the service
endpoint-server.relay.manage	Permission to modify Relay Server Configuration
endpoint-server.relay.read	Permissions to view Relay Server details
endpoint-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
endpoint-server.security.read	Permission to view security-related resources
endpoint-server.tag.manage	Permission to manage Tags (Create and Delete)

The following table lists the permissions in the Endpoint-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrator role has all of the permissions by default and is not listed.

Permission	RA	DPOs	SOC Mgrs	Operators	MAs	Analysts
endpoint-server*						
endpoint-server.agent.manage				Yes		Yes
endpoint-server.agent.read				Yes		Yes
endpoint-server.agentupdate.manage						
endpoint-server.ca.manage				Yes		
endpoint-server.ca.read				Yes		
endpoint-server.configuration.manage						
endpoint-server.filter.manage						Yes
endpoint-server.filter.read						Yes
endpoint-server.health.read						
endpoint-server.logs.manage						
endpoint-server.metrics.read						

Permission	RA	DPOs	SOC Mgrs	Operators	MAs	Analysts
endpoint-server.policy.read						Yes
endpoint-server.process.manage						
endpoint-server.rar.manage						
endpoint-server.rar.read						
endpoint-server.relay.manage				Yes		
endpoint-server.relay.read				Yes		
endpoint-server.security.manage						
endpoint-server.security.read						

Incidents

The following table describes the permissions in the Incidents tab.

Permission	Description
Access Incident Module	Permission to access the Incident module
Configure Incident Management Integration	Permission to configure incident management integration
Delete Alerts and incidents	Permission o delete alerts and incidents
Manage Alert Handling Rules	Permission to modify the alert handling rules
View and Manage Incidents	Permission to modify the incidents

The following table lists the permissions in the Incidents tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Access Incident Module	Yes	Yes	Yes		Yes	Yes
Configure Incident Management Integration	Yes	Yes	Yes			

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Delete Alerts and incidents	Yes	Yes				
Manage Alert Handling Rules	Yes	Yes	Yes			
View and Manage Incidents	Yes	Yes	Yes		Yes	Yes

Integration-server

(The Integration-server permissions are available in NetWitness version 11.1 and later.)

The following table describes the permissions in the Integration-server tab.

Permission	Description
integration-server.*	All permissions (everything below)
integration-server.api.access	Permission to authorize external requests from 3rd party applications
integration-server.configuration.manage	Permission to view and modify all service integration configuration parameters
integration-server.health.read	Permission to read any health notifications that the service exposes
integration-server.logs.manage	Permission to change log-related integration configurations
integration-server.metrics.read	Permission to read any metrics that the service exposes
integration-server.notification.manage	Permission to change global notification configurations (for example, SMTP server)
integration-server.notification.read	Permission to read global notification configurations (for example, SMTP server)
integration-server.notification.send	Permission to send notifications (for example, Email)
integration-server.process.manage	Permission to start and stop the service
integration-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
integration-server.security.read	Permission to read security-related resources
integration-server.template.manage	Permission to change notification template
integration-server.template.read	Permission to read notification template

The following table lists the permissions in the Integration-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrator role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
integration-server.*		Yes				
integration-server.api.access						
integration-server.configuration.manage						
integration-server.health.read						
integration-server.logs.manage						
integration-server.metrics.read						
integration-server.notification.manage	Yes		Yes	Yes		
integration-server.notification.read	Yes		Yes	Yes		
integration-server.notification.send	Yes		Yes	Yes		
integration-server.process.manage						
integration-server.security.manage						
integration-server.security.read						
integration-server.template.manage	Yes		Yes	Yes		
integration-server.template.read	Yes		Yes	Yes		

Investigate

The following table describes the permissions in the Investigate tab.

Permission	Description
Access Investigation Module	Permission to access investigation module
Context Lookup	Permission to access context lookup
Create Incidents from Investigation	Permission to create incidents from investigation
Manage List from Investigation	Permission to modify the list of investigation
Navigate Events	Permission to navigate the events
Navigate Values	Permission to navigate the values

The following table lists the permissions in the Investigate tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Access Investigation Module	Yes	Yes	Yes		Yes	Yes
Context Lookup	Yes		Yes		Yes	Yes
Create Incidents from Investigation	Yes		Yes		Yes	Yes
Manage List from Investigation	Yes		Yes		Yes	Yes
Navigate Events	Yes	Yes	Yes		Yes	Yes
Navigate Values	Yes	Yes	Yes		Yes	Yes

Investigate-server

The following table describes the permissions in the Investigate-server tab.

Permission	Description
investigate-server.*	All permissions (everything below) for 11.4 and above Events view, and 11.3 and earlier Event Analysis view.
investigate-server.column group.read	Permission to access column groups

Permission	Description
investigate-server.configuration.manage	Permission to change any configuration properties for the service
investigate-server.content.export	Permission to export content from the service
investigate-server-content.manage	Permission to clear all per service or per user reconstruction cache
investigate-server.content.reconstruct	Permission to view the summary view, the packet, packet map, text, log, and file reconstructions, as well as the packet count
investigate-server.event.filter	Permission to view the Filter Events panel in the Events view
investigate-server.event.read	Permission to view events that the service exposes
investigate-server.health.read	Permission to view any health notifications that the service exposes
investigate-server.incident.manage	Create or update an incident in Respond
investigate-server.logs.manage	Permission to change log-related configuration
investigate-server.metagroup.manage	Permission to manage meta groups
investigate-server.metagroup.read	Permission to view and use meta groups
investigate-server.metrics.read	Permission to view any metrics that the service exposes
investigate-server.predicate.manage	Permission to edit or remove one or more predicates
investigate-server.predicate.read	Permission to filter events in the Navigate view, Legacy EventsEvents view, and Events view. Note: This permission is required with investigate-server.event.read permission to provide access to the and Events view.
investigate-server.process.manage	Permission to start and stop the service
investigate-server.profile.read	Permission to access profiles.
investigate-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
investigate-server.security.read	Permission to view security-related resources

The following table lists the permissions in the Investigate-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed. The UEBA Analysts and Content Administrators roles have none of these permissions by default and are not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
investigate-server.*	Yes	Yes				
investigate-server.columngroup.read			Yes		Yes	Yes
investigate-server.configuration.manage						
investigate-server.content.export			Yes		Yes	Yes
investigate-server.content.manage						
investigate-server.content.reconstruct			Yes		Yes	Yes
investigate-server.event.filter	Yes	Yes	Yes		Yes	Yes
investigate-server.event.read			Yes		Yes	Yes
investigate-server.health.read						
investigate-server.incident.manage						Yes
investigate-server.logs.manage						
investigate-server.metagroup.manage						
investigate-server.metagroup.read			Yes		Yes	Yes
investigate-server.metrics.read						
investigate-server.predicate.manage						
investigate-server.predicate.read			Yes		Yes	Yes
investigate-server.process.manage						
investigate-server.profile.read			Yes		Yes	Yes
investigate-server.security.manage						

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
investigate-server.security.read						

License-server

The following table describes the permissions in the License-server tab. The Administrator and Operator have all of the permissions and are the only roles granted permissions by default.

Permission	Description
license-server.*	All permissions (everything below)
license-server.configuration.manage	Permission to modify all service configuration parameters
license-server.health.read	Permission to view any health notifications that the service exposes
license-server.license.manage	Permission to manage license related configurations
license-server.license.read	Permission to view license related configurations
license-server.logs.manage	Permission to change log-related configuration
license-server.metrics.read	Permission to view any metrics that the service exposes
license-server.process.manage	Permission to start and stop the service
license-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
license-server.security.read	Permission to view security-related resources

Live

The following table describes the permissions in the Live tab.

Permission	Permission
Live	
Access Live Module	Permission to access live module
Manage Live System Settings	Permission to modify the live system settings
Resources	

Permission	Permission
Deploy Live Resources	Permission to deploy live resources
Manage Live Feeds	Permission to modify live feeds
Manage Live Resources	Permission to modify live resources
Search Live Resources	Permission to search live resources
View Live Resource Details	Permission to view live resource details

The following table lists the permissions in the Live tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Live						
Access Live Module		Yes	Yes	Yes		Yes
Manage Live System Settings				Yes		
Resources						
Deploy Live Resources		Yes		Yes		
Manage Live Feeds		Yes		Yes		
Manage Live Resources		Yes		Yes		
Search Live Resources		Yes	Yes	Yes		Yes
View Live Resource Details		Yes	Yes	Yes		

Malware

The following table describes the permissions in the Malware tab.

Permission	Operators
Download Malware File(s)	Permission to donwnload the malware files for investigation
Initiate Malware Analysis Scan	Permission to start the malware analysis scan
View Malware Analysis Events	Permission to view the malware analysis events

The following table lists the permissions in the Malware tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Download Malware File (s)		Yes	Yes		Yes	Yes
Initiate Malware Analysis Scan		Yes	Yes		Yes	Yes
View Malware Analysis Events		Yes	Yes		Yes	Yes

Metrics-server

The following table describes the permissions in the Metrics-server tab. The Administrators role have all of the permissions and are the only roles granted permissions by default.

Permission	Description
metrics-server .*	All permissions (everything below)
metrics-server.configuration.manage	Permission to modify all service configuration parameters
metrics-server-content.manage	Permission to modify configuration parameters in the service
metrics-server-content.read	Permission to view configuration parameters of the service
metrics-server.health.read	Permission to view any health notifications that the service exposes
metrics-server.logs.manage	Permission to change log-related configuration
metrics-server.metric.manage	Permission to modify all the configuration parameters
metrics-server.metric.read	Permission to view configuration of New Health and Wellness
metrics-server.metrics.read	Permission to view any metrics that the service exposes
metrics-server.process.manage	Permission to start and stop the service
metrics-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
metrics-server.security.read	Permission to view security-related resources

The following table lists the permissions in the Metrics-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RA	DPOs	SOC Mgrs	Operator	MAs	Analysts	UEBA Analysts
metrics-server .*							
metrics-server.configuration.manage							
metrics-server-content.manage							
metrics-server-content.read							
metrics-server.health.read							
metrics-server.logs.manage							
metrics-server.metric.manage							
metrics-server.metric.read		Yes	Yes	Yes	Yes	Yes	
metrics-server.metrics.read							
metrics-server.process.manage							
metrics-server.security.manage							
metrics-server.security.read							

Orchestration-server

The following table describes the permissions in the Orchestration-server tab. The Administrators, Operators, and Data Privacy Officers roles have all of the permissions and are the only roles granted permissions by default.

Permission	Description
orchestration-server.*	All permissions (everything below)
orchestration-server.configuration.manage	Permission to modify all service configuration parameters
orchestration-server.file.read	Permission to view files

Permission	Description
orchestration-server.health.read	Permission to view any health notifications that the service exposes
orchestration-server.logs.manage	Permission to change log-related configuration
orchestration-server.metrics.read	Permission to view any metrics that the service exposes
orchestration-server.process.manage	Permission to start and stop the service
orchestration-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
orchestration-server.security.read	Permission to view security-related resources

Reports

The following table describes the permissions in the Reports tab.

Permission	Description
Alert	
Define RE Alert	Permission to define the RE alerts
Export RE Alert Definition	Permission to export the RE alert definistions
Manage RE Alerts	Permission to to modify the RE alerts
View RE Alerts	Permission to view the RE alerts
View Scheduled RE Alerts	Permission to view the scheduled RE alerts
Chart	
Define Chart	Permission to define the charts
Delete Chart	Permission to delete the charts
Export Chart Definition	Permission to export the chart definistions
Manage Charts	Permission to modify the charts
View Charts	Permission to view the charts
List	
Define Lists	Permission to define the lists
Delete List	Permission to delete the lists

Permission	Description
Export List	Permission to export the lists
Manage Lists	Permission to modify the lists
Report	
Define Report	Permission to define the reports
Delete Report	Permission to delete the reports
Export Report	Permission to export the reports
Manage Reports	Permission to modify the reports
View Reports	Permission to view the reports
Reports	
Access Configure	Permission to access Configure module
Access Reporter Module	Permission to access Reporter module
Access Reporter search	Permission to access Reporter search
Access View	Permission to access Reports view
Rule	
Add RE Alert Definition from Rule	Permission to add RE alert definition from the rules
Define Rule	Permission to define the rules
Delete Rule	Permission to delete the rules
Export Rule	Permission to export the rules
Manage Rules	Permission to modify the rules
View Rule Usage	Permission to view the rules usage
Schedules	
Define Schedule	Permission to define the schedules
Delete Schedule	Permission to delete the schedules
View Schedules	Permission to view the schedules
Warehouse Analytics	
Define Jobs	Permission to define the warehouse analytics jobs

Permission	Description
Delete Jobs	Permission to delete the warehouse analytics jobs
Manage Jobs	Permission to modify the warehouse analytics jobs
View Jobs	Permission to view the warehouse analytics jobs

The following table lists the permissions in the Reports tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all of the permissions by default and is not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Alert						
Define RE Alert		Yes	Yes			Yes
Export RE Alert Definition		Yes	Yes			Yes
Manage RE Alerts		Yes	Yes			Yes
View RE Alerts	Yes	Yes	Yes			Yes
View Scheduled RE Alerts		Yes	Yes			Yes
Chart						
Define Chart		Yes	Yes			Yes
Delete Chart		Yes	Yes			Yes
Export Chart Definition		Yes	Yes			Yes
Manage Charts		Yes	Yes			Yes
View Charts		Yes	Yes			Yes
List						
Define Lists		Yes	Yes			Yes
Delete List		Yes	Yes			Yes
Export List		Yes	Yes			Yes
Manage Lists		Yes	Yes			Yes
Report						
Define Report		Yes	Yes			Yes
Delete Report		Yes	Yes			Yes
Export Report		Yes	Yes			Yes

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
Manage Reports		Yes	Yes			Yes
View Reports		Yes	Yes			Yes
Reports						
Access Configure		Yes	Yes			Yes
Access Reporter Module		Yes	Yes			Yes
Access Reporter search		Yes	Yes			Yes
Access View		Yes	Yes			Yes
Rule						
Add RE Alert Definition from Rule		Yes	Yes			Yes
Define Rule		Yes	Yes			Yes
Delete Rule		Yes	Yes			Yes
Export Rule		Yes	Yes			Yes
Manage Rules		Yes	Yes			Yes
View Rule Usage		Yes	Yes			Yes
Schedules						
Define Schedule		Yes	Yes			Yes
Delete Schedule		Yes	Yes			Yes
View Schedules		Yes	Yes			Yes
Warehouse Analytics						
Define Jobs		Yes	Yes			Yes
Delete Jobs		Yes	Yes			Yes
Manage Jobs		Yes	Yes			Yes
View Jobs		Yes	Yes			Yes

Respond-server

The following table describes the permissions in the Respond-server tab.

Note: For viewing and managing the Risk Score feature, users who have installed NetWitness Platform 11.3 or upgraded from NetWitness 10.6.x to 11.3, risk score permissions will be already present for Analysts. For users updating from NetWitness 11.x to NetWitness Platform 11.3, the Administrator has to provide Analysts' permissions to manage and view risk score.

Permission	Description
respond-server.*	All permissions (everything below)
respond-server.alert.delete	Permission to delete alerts
respond-server.alert.manage	Permission to create, update, or delete alerts and alert filters
respond-server.alert.read	Permission to view alerts and alert filters
respond-server.alertrule.manage	Permission to create, update, or delete alert aggregation rules
respond-server.alertrule.read	Permission to view alert aggregation rules
respond-server.configuration.manage	Permission to change any configuration properties for the service
respond-server.health.read	Permission to view any health notifications that the service exposes
respond-server.incident.delete	Permission to delete incidents
respond-server.incident.manage	Permission to create, update, or delete incidents and incident filters including permission to view the Create Incident and Add to Incident options in the Investigate > Events view
respond-server.incident.read	Permission to view incidents and incident filters
respond-server.journal.manage	Permission to create, update, or delete journal entries for an incident
respond-server.journal.read	Permission to view journal entries for an incident
respond-server.logs.manage	Permission to change log-related configuration
respond-server.metrics.read	Permission to view any metrics that the service exposes
respond-server.notification.manage	(This permission is available in NetWitness version 11.1 and later.) Permission to configure incident email notification settings such as the selected email server, SOC Managers, and who will be sent the notifications (Assignee and SOC Managers)
respond-server.notification.read	(This permission is available in NetWitness version 11.1 and later.) Permission to view incident email notification settings
respond-server.process.manage	Permission to start and stop the service
respond-server.remediation.manage	Permission to create, update, or delete remediation tasks

Permission	Description
respond-server.remediation.read	Permission to view remediation tasks
respond-server.risk.manage	Permission to manage risk score
respond-server.risk.read	Permission to view risk score
respond-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
respond-server.security.read	Permission to view security-related resources

The following table lists the permissions in the Respond-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrator has all of the permissions by default and are not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
respond-server.*	Yes	Yes				
respond-server.alert.delete						
respond-server.alert.manage			Yes		Yes	Yes
respond-server.alert.read			Yes		Yes	Yes
respond-server.alertrule.manage			Yes			
respond-server.alertrule.read			Yes			
respond-server.configuration.manage						
respond-server.health.read						
respond-server.incident.delete						
respond-server.incident.manage			Yes		Yes	Yes
respond-server.incident.read			Yes		Yes	Yes
respond-server.journal.manage			Yes		Yes	Yes
respond-server.journal.read			Yes		Yes	Yes
respond-server.logs.manage						
respond-server.metrics.read						

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
respond-server.notification.manage			Yes			
respond-server.notification.read			Yes			
respond-server.process.manage						
respond-server.remediation.manage			Yes		Yes	Yes
respond-server.remediation.read			Yes		Yes	Yes
respond-server.risk.manage						Yes
respond-server.risk.read						Yes
respond-server.security.manage						
respond-server.security.read						

Incident Email Notification Settings Permissions

Note: Incident email notification setting permissions are available in NetWitness version 11.1 and later.
If you are updating from NetWitness version 11.0 to 11.1 or later, you will need to add additional permissions to your existing built-in NetWitness user roles. For all upgrades to 11.1 or later, you will need to add additional permissions to custom roles.

The following permissions are required for Respond Administrators, Data Privacy Officers, and SOC Managers to access Incident Email Notification Settings [(Configure) > Incident Notifications].

Incidents tab:

- Configure Incident Management Integration

Respond-server tab:

- respond-server.notification.manage
- respond-server.notification.read

Integration-server tab:

- integration-server.notification.read
- integration-server.notification.manage

Respond Event Analysis Permissions

Note: The Event Analysis panel in the Respond view is available in NetWitness version 11.2 and later.

The Events panel in the Respond view, formerly known as the Event Analysis panel, shows the Events view from Investigate for specific indicator events. The following permissions are required to view the Events panel in the Respond view. These permissions are provided by default for users with the Analysts role.

Investigate-server tab:

- investigate-server.event.read
- investigate-server.content.reconstruct
- investigate-server.content.export

Administration tab:

- Access Administration Module

Respond Saved Filter Permissions

Note: Saved filters for the incidents and alerts lists in Respond are available in NetWitness version 11.5 and later.

The following permissions are required for the incidents and alerts filters (Respond > Incidents and Respond > Alerts). The Analysts role has the required Respond filter permissions by default.

Respond-server tab:

- respond-server.incident.manage
- respond-server.incident.read
- respond-server.alert.manage
- respond-server.alert.read

Security-server

The following table describes the permissions in the Security-server tab. The Administrators, Operators, and Data Privacy Officers roles have all of the permissions and are the only roles granted permissions by default.

Permission	Description
security-server.*	All permissions (everything below)
security-server.account.manage	Permission to view, create, modify, or remove NetWitness local accounts
security-server.account.read	Permission to view NetWitness local accounts

Permission	Description
security-server.ca.manage	Permission to manage NetWitness deployment PKI parameters (for example, sign certificates, and so on)
security-server.ca.read	Permission to view NetWitness deployment PKI parameters
security-server.configuration.manage	Permission to modify all service configuration parameters
security-server.connection.manage	Permission to modify all connection configuration parameters
security-server.health.read	Permission to view any health notifications that the service exposes
security-server.logs.manage	Permission to change log-related configuration
security-server.metrics.read	Permission to view any metrics that the service exposes
security-server.permission.manage	Permission to create or remove NetWitness permissions
security-server.pki.manage	Permission to modify all pki configuration parameters
security-server.process.manage	Permission to start and stop the service
security-server.role.manage	Permission to create, modify, or remove NetWitness roles (for example, add role permissions)
security-server.role.read	Permission to view NetWitness role definitions
security-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
security-server.security.read	Permission to view security-related resources
security-server.test.manage	Permission to modify all test configuration parameters
security-server.user.manage	Permission to view, create, modify, or remove NetWitness user profiles
security-server.user.read	Permission to view NetWitness user profile details (for example, roles, login times, and so on)

Source-server

The following table describes the permissions in the Source-server tab.

Permission	Description
source-server.*	All permissions (everything below)
source-server.configuration.manage	Permission to change any configuration properties for the service

Permission	Description
source-server.group.manage	Permission to create and manage USM groups
source-server.group.manage.nopolicy	Permission to manage nopolicy
source-server.group.read	Permission to view USM groups
source-server.grouppolicy.read	Permission to view the canonical groups and policies
source-server.health.read	Permission to view any health notifications that the service exposes
source-server.logs.manage	Permission to change log-related configuration
source-server.metrics.read	Permission to view any metrics that the service exposes
source-server.policy.manage	Permission to create and manage USM policies
source-server.policy.read	Permission to view USM policies
source-server.process.manage	Permission to start and stop the service
source-server.security.manage	Permission to edit security-related resources (passwords, keys, and so on)
source-server.security.read	Permission to view security-related resources
source-server.centralgroup.read	Permission to view the Centralized Content Management groups
source-server.centralpolicy.read	Permission to view the Centralized Content Management policies
source-server.centralservice.read	Permission to view the core services and ESA services

The following table lists the permissions in the Source-server tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators and Operators roles have all of the permissions by default and are not listed.

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
source-server.*						
source-server.configuration.manage						
source-server.group.manage						
source-server.group.manage.nopolicy						

Permission	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
source-server.group.read		Yes	Yes			Yes
source-server.grouppolicy.read						
source-server.health.read						
source-server.logs.manage						
source-server.metrics.read						
source-server.policy.manage						
source-server.policy.read		Yes	Yes			Yes
source-server.process.manage						
source-server.security.manage						
source-server.security.read						Yes
source-server.centralgroup.read						Yes
source-server.centralpolicy.read						Yes
source-server.centralservice.read						Yes

Springboard

The following table describes the permissions in Springboard tab.

Permission	Description
springboard.*	All Permissions (everything below)
springboard.manage	Permission to manage the Springboard, that is view, add, delete, and rearrange panels, and also restore system default settings.
springboard.read	Permission to view Springboard.

The following table lists the permissions in the Springboard tab assigned to each role. A blank field indicates that the role does not have the permission. The Administrators role has all the permissions by default and is not listed.

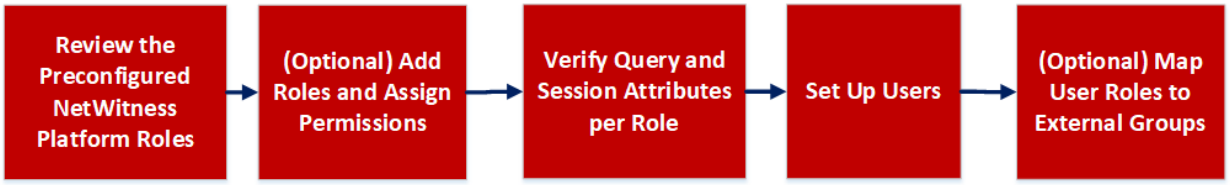
Permissions	RAs	DPOs	SOC Mgrs	Operators	MAs	Analysts
springboard.*						
springboard.manage						
springboard.read	Yes		Yes		Yes	Yes

Manage Users with Roles and Permissions

A set of end-to-end procedures for managing users in NetWitness is described in this section. These steps explain how to add a user in NetWitness and then how to control what the user can do.

Manage Users Workflow

This figure shows the high-level workflow for managing the users in NetWitness.



First, review the preconfigured NetWitness roles such as Administrators, Respond Administrators, Data Privacy Officers, SOC managers, Operators, Malware analysts, Analysts, and UEBA analysts. Determine if you need to make any adjustments to these roles for your environment. You can add new custom roles and assign permissions to each role. After you define the roles, you can verify the query and session attributes that are set for each role. Then you can set up the users by adding new users and assigning roles to them. You can also map external group users to the NetWitness roles.

These are the procedures for setting up and managing users:

- Review the Preconfigured NetWitness Platform Roles
- (Optional) Add a Role and Assign Permissions
- Verify Query and Session Attributes per Role
- Set Up Users
- (Optional) Map User Roles to External Groups

Review the Preconfigured NetWitness Platform Roles

To simplify the process of creating roles and assigning permissions, there are preconfigured roles in NetWitness.

Role	Permission
Administrators	Full system access. The System Administrators persona is granted all permissions by default.
Analysts	Access to meta and session content but not to configurations. The Security Operation Center (SOC) Analysts persona is centered around investigation, ESA Alerting, Reporting, and Respond, but not system configuration.

Role	Permission
Reporting_Engine_ Content_Administrators	Access to manage the Live content. Users with the Reporting Engine Content Administrator role can deploy Reporting Engine content (rules, reports, charts, and lists) from Live Content, view and manage permissions to the deployed content in Reporting Engine.
Data_Privacy_Officers	The Data Privacy Officer (DPO) persona is similar to Administrators with additional focus on configuration options that manage obfuscation and viewing of sensitive data within the system (see the *Data Privacy Management Guide*). Users with the DPO role can see which meta keys are flagged for obfuscation, and they also see obfuscated meta keys and values created for the flagged meta keys.
Malware_Analysts	Access to investigations and malware events. The only access granted to the Malware Analysts persona is the Malware Analysis module.
Operators	Access to configurations but not to meta and session content. The System Operators persona is focused on system configuration, but not investigation, ESA, Alerting, Reporting, and Respond.
Respond_Administrator	Access to all Respond permissions. The Respond Administrator persona is focused on system configuration of Respond.
SOC_Managers	Same access as Analysts plus additional permission to handle incidents. The SOC Managers persona is identical to Analysts, but with permissions necessary to configure Respond.
UEBA_Analysts	Access to the NetWitness UEBA service in the **Investigate** > **Users** view. NetWitness UEBA is an advanced analytics solution for discovering, investigating, and monitoring risky behaviors across all entities in your network environment. **Note:** You do not need to set up specific permissions for this role. You only need to assign this role to a user, and that user will have access to NetWitness UEBA.

The administrator can also add custom roles.

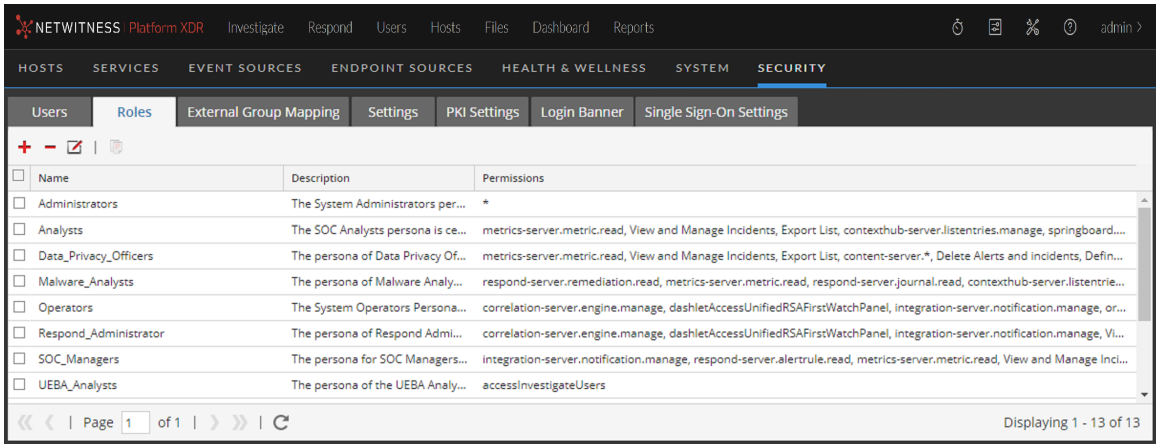
(Optional) Add a Role and Assign Permissions

Although NetWitness has preconfigured roles, you can add custom roles. For example, in addition to the preconfigured Analysts role you could add custom roles for AnalystsEurope and AnalystsAsia. For a detailed list of permissions, see Role Permissions.

Each of the following procedures starts on the **Roles** tab.

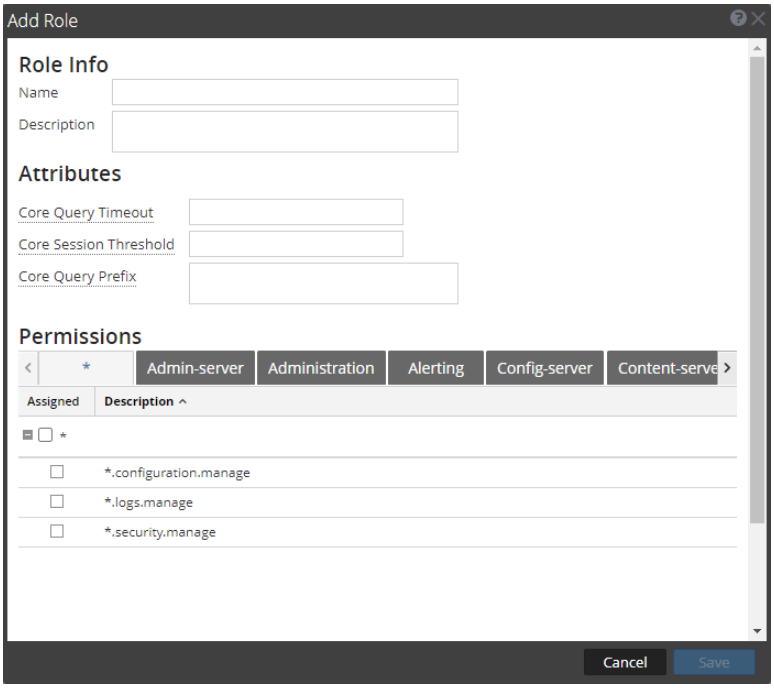
To navigate to the Roles tab:

1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Roles** tab.



Add a Role and Assign Permissions

1. In the **Roles** tab, click ✚ in the toolbar.
2. The **Add Role** dialog is displayed.



3. In the **Role Info** section, type the following information for the role:
   - **Name**
   - (Optional) **Description**
4. In the **Attributes** section, enter the desired values for each attribute. For more information on attributes, see Verify Query and Session Attributes per Role.
5. In the **Permissions** section:
   - Click ‹ and › to scroll through the modules.
   - Select a module the role will access.
   - Select each permission the role will have.
6. Repeat the previous step until you select all permissions to assign to the role.
7. Click **Save** to add the new role, which is effective immediately. You can now assign the new role to users.

Change Permissions Assigned to a Role

1. In the **Roles** tab, select the role and click  .
   The **Edit Role** dialog is displayed.
2. In the **Permissions** section:

- Click  and  to scroll through the modules. Select a module to revise permissions for it. Select or deselect each permission.
- Select a module to revise permissions for it.
- Select or deselect each permission.

3. Repeat the previous step until the role has the required permissions.
4. Click **Save**. The revised permissions are effective immediately.

Duplicate a Role

An efficient way to add a new role is to duplicate a similar role, save it with a new name and revise the permissions that are already assigned.

1. In the **Roles** tab, select the role you want to duplicate and click  .
2. Type a new role name and click **Save**.
3. To change the permissions, follow the steps in the next procedure.

Delete a Role

You can delete a role if it is not assigned to any users.

1. In the **Roles** tab, select the role and click .
2. A dialog requests confirmation that you want to delete the role. Click **Yes**.

Verify Query and Session Attributes per Role

After you define your user roles, it is important to verify the query and session attributes that are set for each role. You can adjust these settings according to your requirements.

You can understand how these role settings impact individual user settings and what happens if a user is a member of multiple roles.

Query and Session Attributes

Query and session attributes determine how to handle the queries that a user runs. These attributes enable you to lock down the information that users can retrieve, and the attributes apply to all sessions of users assigned to a role.

Depending on your requirements, you can specify the following query-handling attributes for a user role:

- **Core Query Timeout** is an optional setting that applies to NetWitness Core services. It specifies the maximum number of minutes that a user can run a query. If this value is set, it must be zero (0) or greater. A value of zero represents no timeout. The default value is 5 minutes.
- **Core Session Threshold** is a required setting. This value must be zero (0) or greater. The default is 100000. The limit you specify here overrides the **Max Session Export** value defined in the Investigate view settings. If the threshold is greater than zero, a query optimization will extrapolate the total session counts that exceed the threshold. When the meta value count returned by the query reaches the threshold, the system will:
  - Stop its determination of the session count.
  - Show the threshold and percentage of query time used to reach the threshold.
- **Core Query Prefix** is an optional filter applied to queries the user runs. The prefix restricts query results that the user sees. For example, the `'service' = 80` query prefix is prepended to any queries run by the user, and the user can only access metadata of HTTP sessions. If you set up data privacy using a whitelist, every meta key specified in the core query prefix must also be whitelisted as described in the *Data Privacy Management Guide*.

Note: In Version 11.1 and later, you can use configured meta entities in a Core Query Prefix. For additional information about configuring meta entities, refer to the *Core Database Tuning Guide*.

The query-handing attribute settings applied for a user depend on the role memberships of the user. It is important to verify the query-handling attribute settings for your roles.

How Query-Handling Attribute Settings Apply to Individual Users

If a user is a member of multiple roles, the following logic applies for the user:

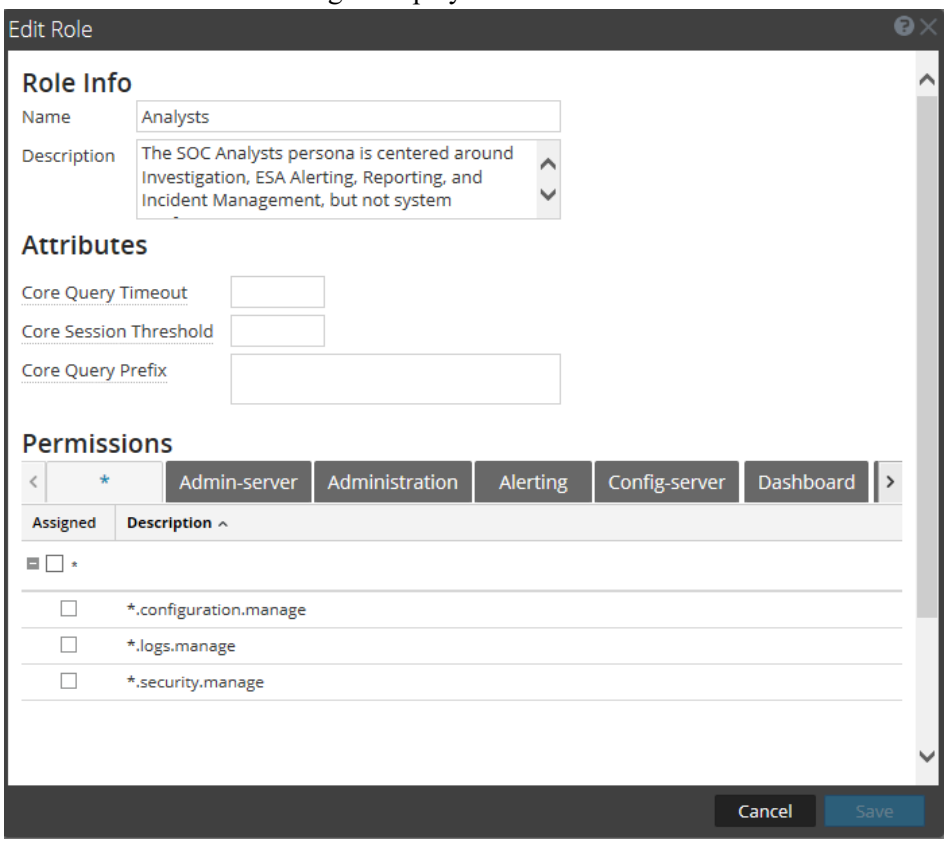
- **Query Timeout:** The most permissive (highest) value of all assigned roles is applied to the user.
- **Query Prefix:** The query prefixes of each of the user roles are AND'd together.

- **Session Threshold:** The highest value of all the assigned roles is applied to the user.

Set Query Handling Attributes for a User Role

1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.

2. Click the **Roles** tab. If you are adding a role, click . If you are editing a role, select the role and click .
   The Add or Edit Role dialog is displayed.



3. To set the attributes for the role, in the **Attributes** section:
   - (Optional) In the **Core Query Timeout** field, type the maximum number of minutes that a user can run a query. This timeout applies to queries performed from Investigate.
   - Type a **Core Session Threshold** for the system to stop its determination of the session count.
   - (Optional) Type a **Core Query Prefix** to filter query results that role members see in the Investigate Navigate view, Events view, and Event Analysis view. You can specify a query that is prepended to all queries executed by users with a specific role. For example, if the `'service' = 80` query prefix is prepended to all queries by users in this role, the users can only access

metadata of HTTP sessions. If users attempt to navigate to non-HTTP event, the view is not displayed.

Caution: If you add or modify a query prefix, and a user who has access to everything falls into a user role that is now restricted by a query prefix, that user will still be able to access cached data and view restricted content. To remove visibility of restricted content and enforce the query prefix in the Navigate or Events view, go to  (Admin) > System > Investigation, and use Reconstruction Cache Settings to clear the cache for all services available to affected users. The user will still be able to access cached data and view restricted content in the Event Analysis view until the analyst restarts the NetWitness Investigate services or the cache is cleared automatically after 24 hours.

4. Click **Save.**

Set Up Users

The procedures to set up a new user are described below.

- Add a User and Assign a Role
- Enable, Unlock, and Delete User Accounts

Add a User and Assign a Role

All NetWitness users must have a local or external user account. You can add a new user to each type of user account, local and external. You can assign role to a local user.

The following considerations are important when managing local and external user accounts.

Local User Account	External User Account
Managed within NetWitness.	Managed externally and outside the scope of this document.
Roles assigned directly.	Roles assigned by external group mapping.
Derives permissions from each role assigned to the user	Derives permissions from each role mapped to the account's external user group, as explained in (Optional) Map User Roles to External Groups.
NetWitness manages all user information.	NetWitness manages user identification only. This includes Username, Full Name and Email.

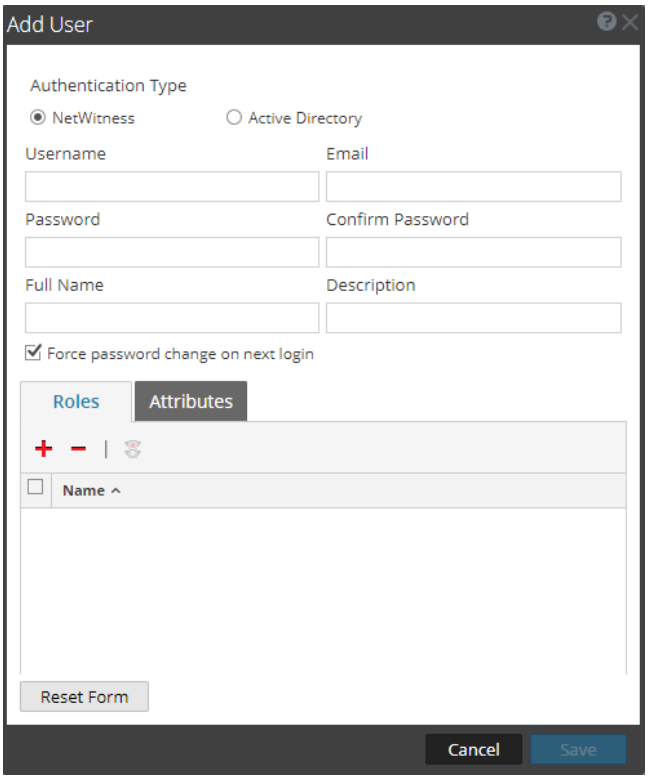
Each of the following procedures starts on the Users tab. To navigate to the Users tab, go to  (Admin) > Security. The Security view is displayed with the Users tab open.

Add a Local User

To add a local user account and assign a role to the user:

1. In the **Users** tab, click  in the toolbar.

   The **Add User** dialog is displayed.

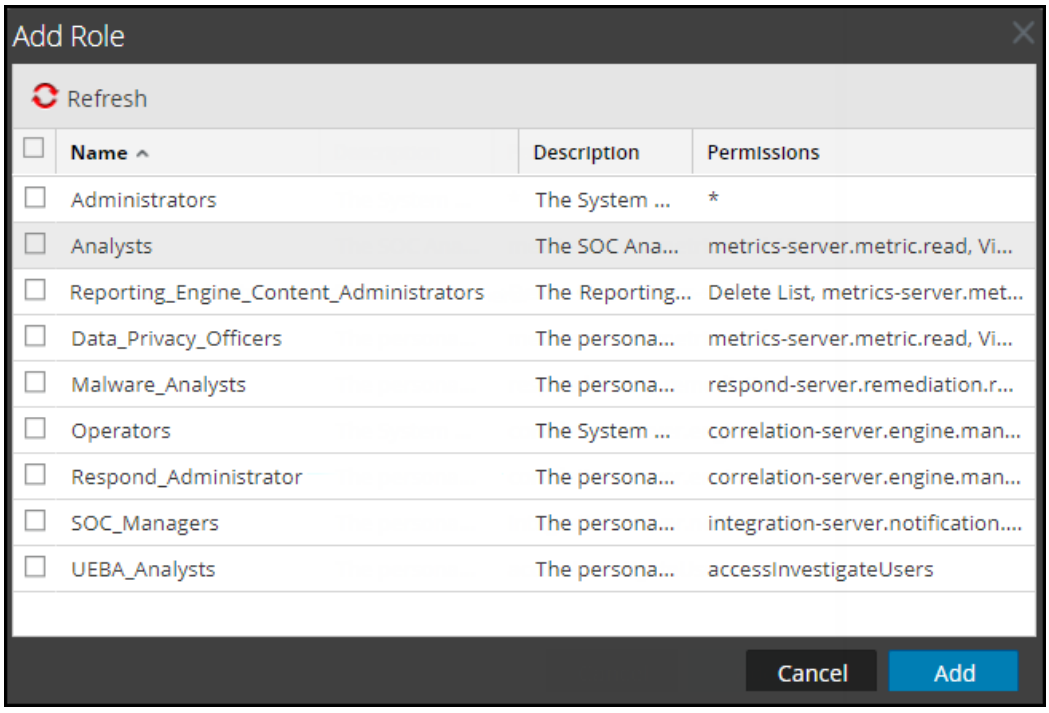


2. Type the following account information for the new user:
   - **Authentication Type**: **NetWitness** is selected by default and is the correct choice when adding a local user. This option is only displayed when there are AD or PAM configurations set up to allow for selecting that authentication type.

     Note: If there are no AD or PAM configurations, the authentication type is set to NetWitness automatically and there are no other options available.
   - **Username** for logging on to NetWitness
   - **Email** address
   - Password for logging on to NetWitness, in the **Password** and **Confirm Password** fields
   - **Full Name** of the new user
   - (Optional) **Description** of the user account
3. To expire the user password the next time the user logs on, select **Force password change on next login**.

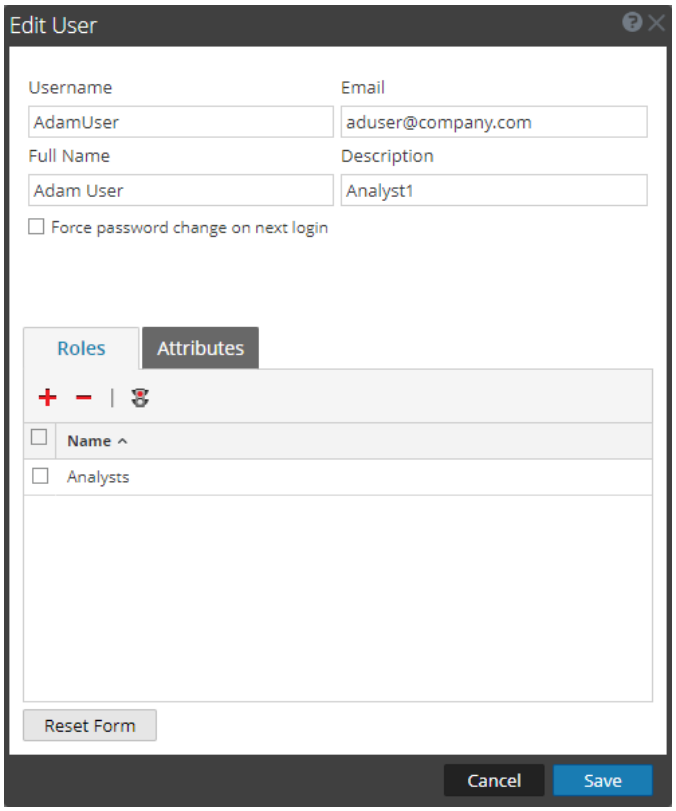
   This does not affect any active user sessions. The  appears in the user row to show that the user password expired. After a password is expired, you cannot undo it. This checkbox is cleared the next time you edit the user account.
4. To assign a role to the user, click + in the **Roles** tab.

   The **Add Role** selection dialog shows the list of available roles.

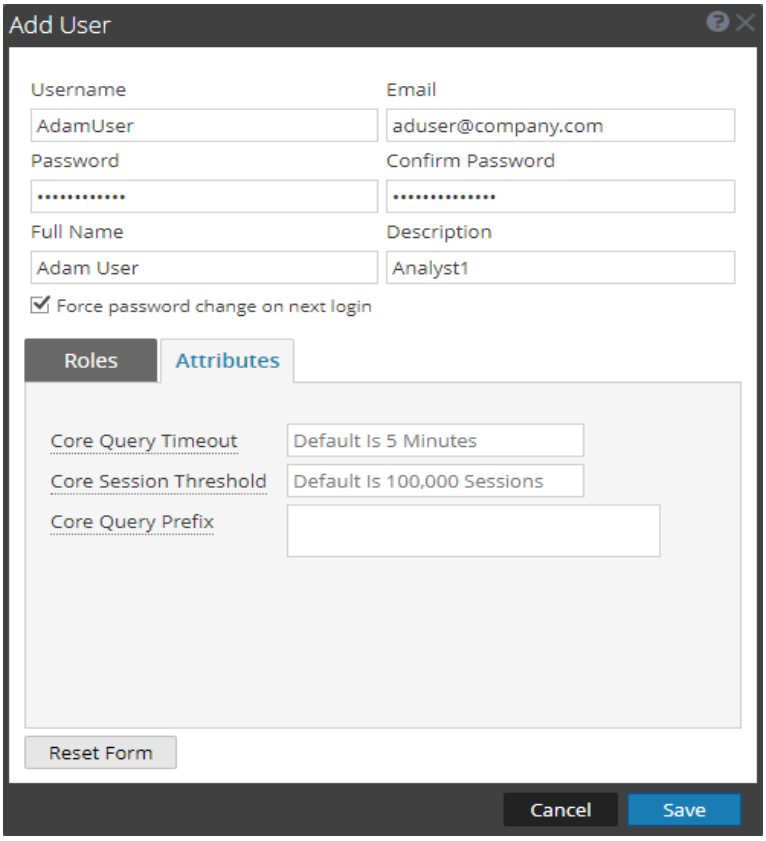


5. Select each role to assign and click **Add**.

   The **Add User** dialog shows each role assigned to the user.

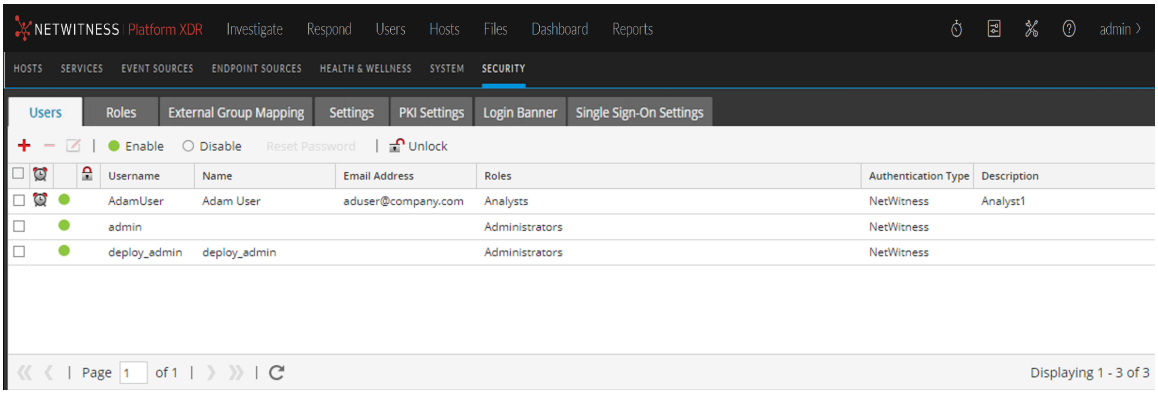


6. (Optional) To assign attributes to a user, go to **Attributes** and modify the appropriate values. These attributes are unique to the user and follow all the same rules for attributes within roles. For more information on attributes, see Query and Session Attributes.



7. (Optional) Select a role and click to **Show all permissions** for the role.
8. Click **Save**.

   The **Users** tab shows the new user and each role assigned to the user. The account is active immediately.



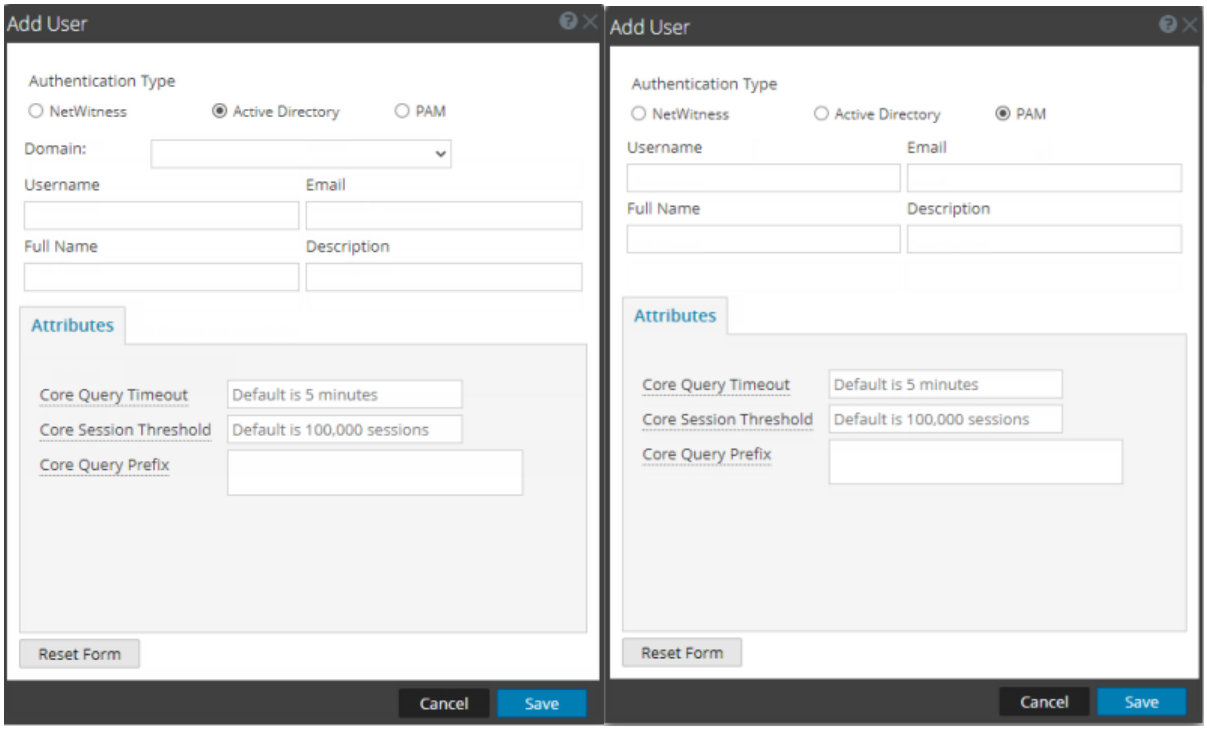
Add a User for External Authentication

To add a user for external authentication:

1. In the **Users** tab, click + in the toolbar.

   The **Add User** dialog is displayed.

2. For **Authentication Type**, select either **Active Directory** or **PAM**. The dialog will update to show the required fields for the selected external authentication type.



3. Type the following information:

   - **Domain** (if select Active Directory authentication only): Select the Active Directory domain for the user from the drop-down list of available domains.
   - **Username** for logging on to NetWitness
   - **Email** address
   - **Full Name** of the new user
   - (Optional) **Description** of the user account

4. In the Attributes section, type the following information.

   a. **Core Query Timeout**- most permissive (highest) value of all assigned roles is applied to the user.

   b. **Core Session Threshold** - query prefixes of each of the user roles are AND'd together.

   c. **Core Query Prefix** - highest value of all the assigned roles is applied to the user.

5. Click **Save**. The Users tab shows the new user account, which still needs a role and permissions.

6. To map a role to the new user, see (Optional) Map User Roles to External Groups.

Change User Information or Roles

To change a user's account information or assigned roles:

1. In the **Users** tab, select a user and click in the toolbar.

   The **Edit User** dialog is displayed.
2. To edit user information, change any of the following fields:
   - **Email**
   - **Full Name**
   - **Description**
3. To expire the **internal** user password the next time the user logs on, select **Force password change on next login**.

   This does not affect any active user sessions. The appears in the user row to show that the user password expired. After a password is expired, you cannot undo it. This checkbox is cleared the next time you edit the user account.
4. In the **Roles** section:
   - To assign another role, click , select a role and click **Add**.
   - To remove an assigned role, select the role and click .
5. Click **Save**.

Delete a User

To delete a user:

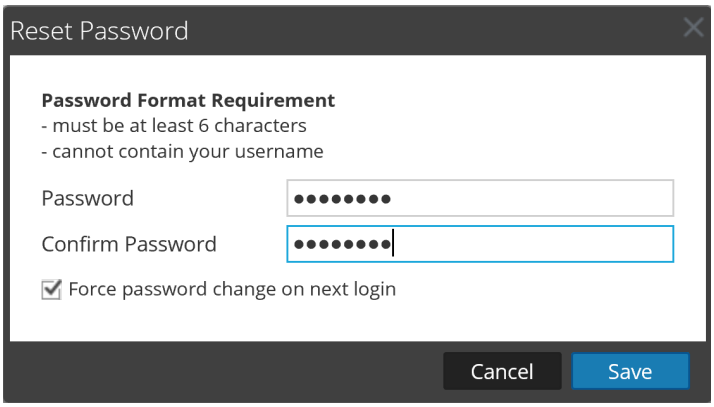
1. In the **Users** tab, select a user.
2. In the toolbar, click .
3. Click **Save**.

Note: To fully delete a user that is externally authenticated by Active Directory, you must also delete the user from the AD Group.

Reset a User Password

To reset a user password:

1. In the **Users** tab, select a user.
2. In the toolbar, click **Reset Password**.



The **Password Format Requirement** section lists the specific requirements for the password. Administrators can adjust these requirements for all internal users in the password policy. See Configure Password Complexity.

3. Choose whether to force a password change the next time the user logs in to NetWitness.
4. Click **Save**.

Enable, Unlock, and Delete User Accounts

All users of NetWitness must either have a local user account with username and password or have an external user account. Within NetWitness, you can enable, disable, and delete local user accounts.

The first time an external user logs into NetWitness, a new user entry is automatically created with NetWitness. NetWitness manages only user identification information; for example, Full Name and Email.

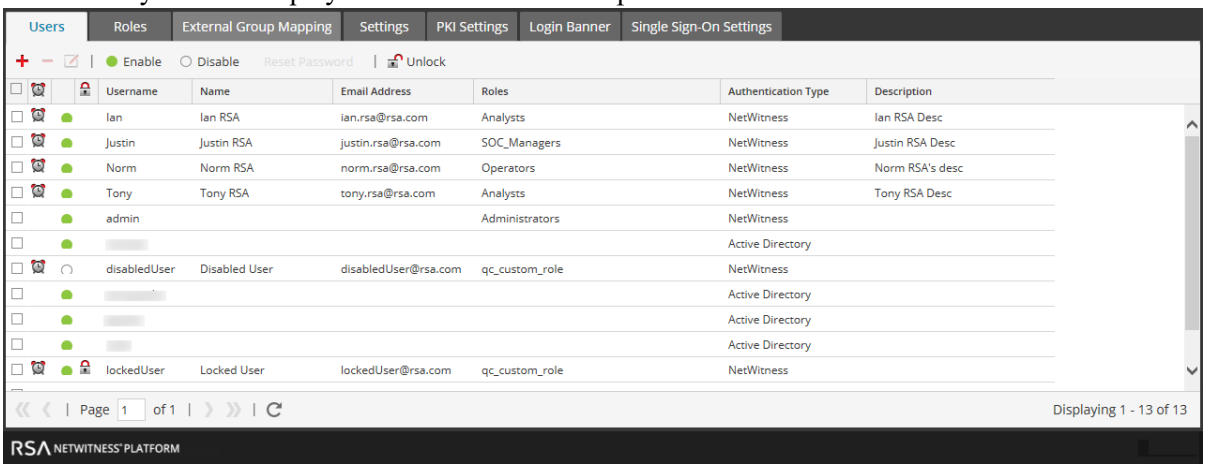
You can unlock locked accounts for both local and external users.

Enable Disabled NetWitness User Accounts

To enable NetWitness user accounts that have been disabled:

1. Go to **(Admin) > Security**.

   The Security view is displayed with the **Users** tab open.



2. In the **Users** grid, select one or more accounts.
3. Click Enable.
   A successful message displays for enabled accounts, and the users can log in to NetWitness.

Disable NetWitness User Accounts

You can block user access by disabling users. Disabling the user does not delete user preferences. This action blocks user access without deleting user preferences so that upon re-enabling users, user preferences are intact. You can re-enable users to restore user access. Disabling users applies only to Local users and not External Users.

To disable NetWitness user accounts:

1. In the **Users** grid, select one or more accounts.
2. Click Disable.
   A successful message displays for disabled accounts, and the users can no longer log in to NetWitness.

Unlock Locked NetWitness User Accounts

A user is locked out for a period of time after a number of failed consecutive login attempts. To unlock NetWitness user accounts that are locked due to excessive failed login attempts:

1. In the **Users** grid, select one or more accounts.
2. Click Unlock.
   A successful message displays for unlocked accounts, and the users can log in to NetWitness.

Delete NetWitness User Accounts

If not using External Authentication, a user can log on to NetWitness using a local account. These local accounts are directly managed using NetWitness. To revoke access to a local user, either disable the account or delete the account completely from the system.

Note: This deletes all user preferences for the account from NetWitness. If this is not the intention, disable the user instead of deleting the user.

To delete NetWitness user accounts:

1. Go to  **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. In the Users list, select one or more accounts.
3. Click .
   A warning dialog requests confirmation.
4. If you want to delete the accounts, click **Yes**.
   The accounts are removed from NetWitness, and the users can no longer log in to NetWitness.

(Optional) Map User Roles to External Groups

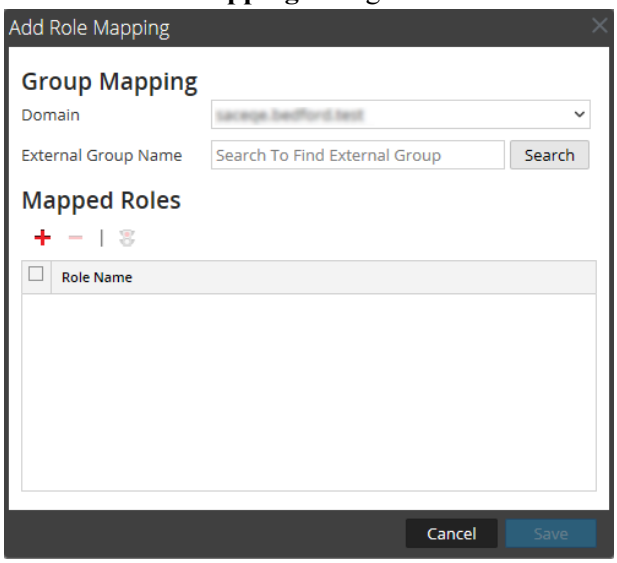
In NetWitness, external groups derive permissions for various modules and views from NetWitness user roles, which have permissions assigned to them. To provide access to an external group, map user roles to it. To modify an external group's access, edit the roles mapped to it. Add and delete roles until the external group has the necessary access. Changes take effect immediately.

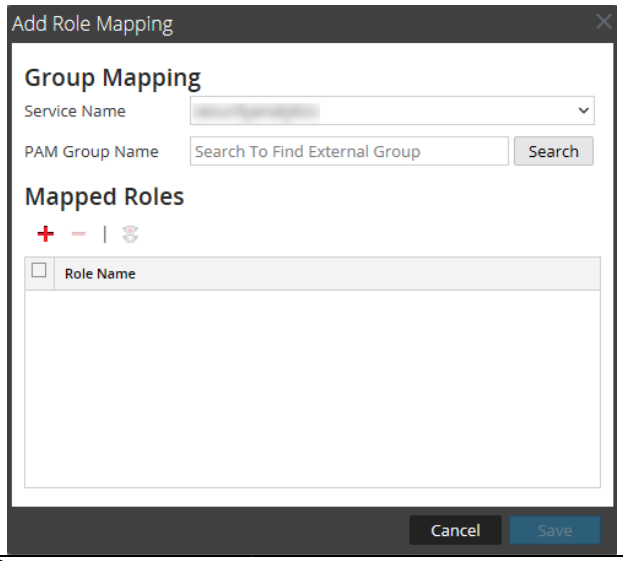
In the Settings tab, you must set up a method for external user authentication to make external groups visible to NetWitness.

Add Role Mapping for an External Group

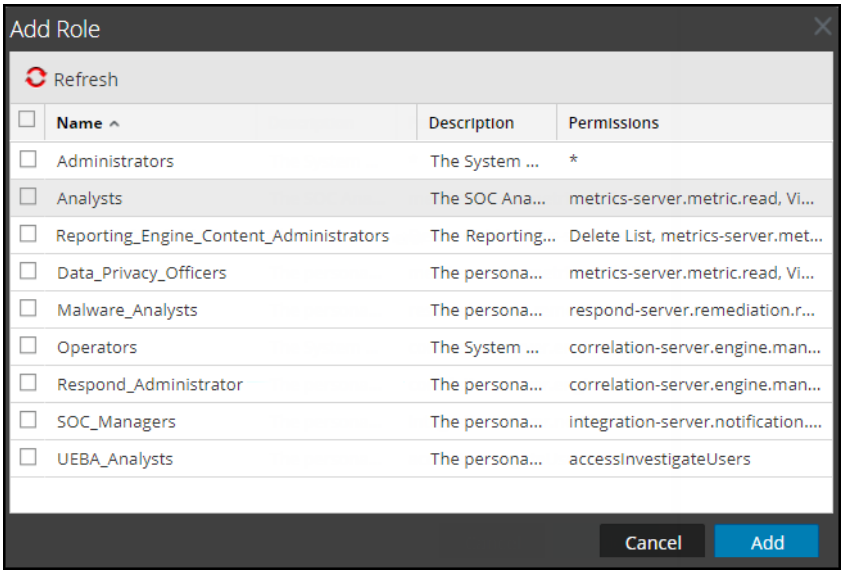
To add role mapping for an external group:

1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click +.
   The **Add Role Mapping** dialog for the external authentication method you selected is displayed.





4. Click **Search** and search for an external group name in the Search for External Groups, then select an external group name.
5. To add roles to the group mapping, click + in the **Mapped Roles** section.
   The **Add Role** dialog is displayed.



6. Select the checkbox in the title bar to select all roles, or select roles individually.
7. To add the roles to the **Mapped Roles** section in the Add Role Mapping dialog, click **Add**.
   The dialog closes and the selected roles are displayed in the Mapped Roles section.
8. If you want to delete roles from the **Mapped Roles** section, select the roles and click − .
9. When the **Add Role Mapping** dialog reflects the role mapping that you want to define for the group, click **Save**.
   The Add Role Mapping dialog closes, and the new role mapping is listed in the External Group Mapping tab list.

Edit Role Mapping for a Group

To edit role mapping in a group:

1. In the **External Group Mapping** action bar, click **Edit**.
   The **Edit Role Mapping** dialog is displayed with the group name in the **External Group Name** field.
2. To add roles to the mapping, click + in the **Mapped Roles** section.
   The Add Role dialog is displayed.
3. Select the checkbox in the title bar to select all roles, or select roles individually.
4. To add the roles to the **Mapped Roles** section in the **Add Role Mapping** dialog, click **Add**.
   The dialog closes, and the selected roles are displayed in the Mapped Roles section.

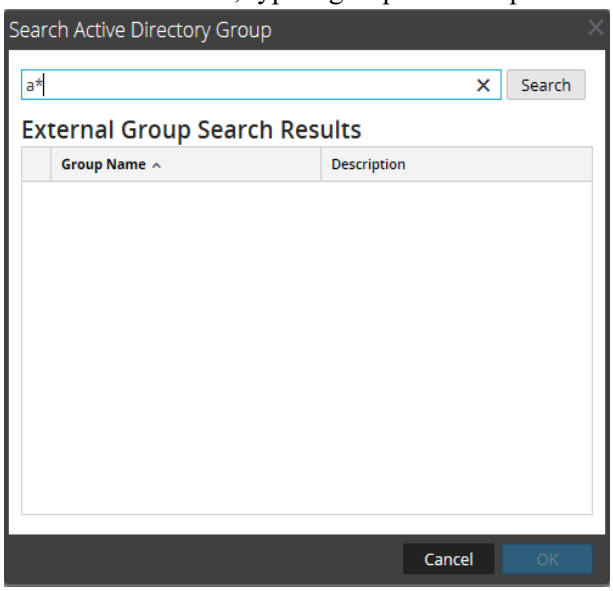
5. If you want to delete roles from the **Mapped Roles** section, select the roles and click .
6. When the **Edit Role Mapping** dialog reflects the role mapping that you want to define for the group, click **Save**.
   The dialog closes, and the edited role mapping is listed in the External Group Mapping tab.

Search for External Groups

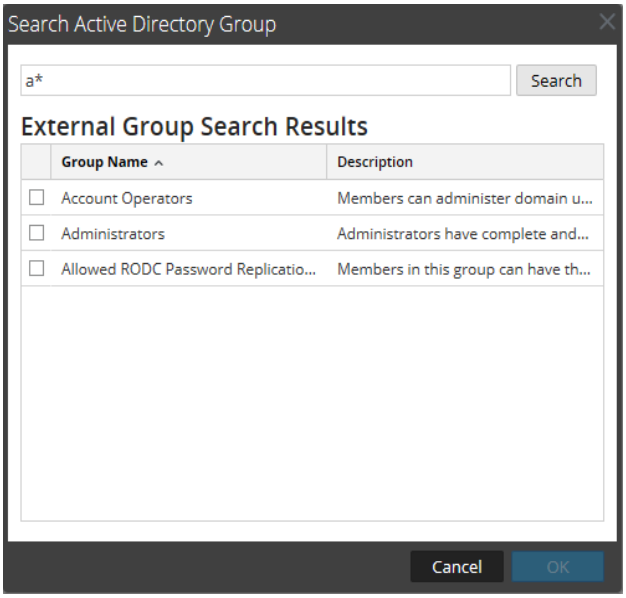
The instructions for searching for external groups that have NetWitness user roles mapped to them.

To search for an external group:

1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click or .
   The **Add Role Mapping** dialog for the external authentication method you selected is displayed.
4. The **Group Mapping** section is dependent on the selected external authentication method.
   - For **Active Directory**, select a **Domain**. Then click **Search** next to **External Group Name**.
   - For **PAM**, click **Search** next to **PAM Group Name**.
     The **Search External Groups** dialog is displayed.
5. In **Common Name**, type a group name or part of a group name with the wild card character (*).



6. Click **Search**.
   The results are displayed in the **External Group Search Results** section.



7. Select the group to which you want to assign roles and click **OK**.

Set Up Multi-Factor Authentication

You can set up Multi-Factor Authentication (MFA) for NetWitness using one of the following methods:

- ADFS Log in to NetWitness with SecurID Passcode.
- PAM SecurID Log in to NetWitness for AD Users.

ADFS Log in to NetWitness with SecurID Passcode

Single Sign-On (SSO) functionality of NetWitness can be leveraged where the user authenticates using ADFS log in user interface with AD user credentials followed by the SecurID passcode.

Note: This method is suitable only for single AD users.

Prerequisites

- NetWitness Platform (NW) version 11.4 or later
- MS Active Directory Federation Services (ADFS) - MS Windows Server 2012 R2 or later
- MS Active Directory (AD) – MS Windows Server 2008 R2 or later
- Authentication Manager (AM) 8.4 or later
- Authentication Agent for ADFS 1.0 or later

Perform the following configurations:

1. Configure Authentication Manager.
2. Configure NetWitness.
3. Configure ADFS.

Configure Authentication Manager

Configure Active Directory as an Identity Source in Authentication Manager using the steps described in the section Add an Identity Source.

Configure NetWitness

1. Configure Active Directory for External Authentication to NetWitness using the steps described in the section Configure Active Directory.
2. NetWitness must be configured for SSO using the steps described in the section Configure Single Sign-On.

Configure ADFS

ADFS must be configured for SSO in NetWitness. You must copy the exported metadata (see step 9 in Configure Single Sign-On) to ADFS and perform the following steps:

1. Go to **Server Manager > Tools > ADFS management > Trust Relationships**.
2. On the right-side, click **Add Relying Part Trust > Start**.
3. Click **Import data about the relying party from a file** and select the metadata file.
4. Click **Next**, and enter a display name.
5. Click **Next** until the **Close** button is displayed.
6. Ensure the **Open the Edit Claim Rules** option is selected.
7. Click **Close**.
8. In the **Edit Claim Rules** dialog, click **Add Rule**.
9. In the **Add Transform Claim Wizard** dialog, click **Next**.
10. Enter a claim rule name.
11. In the **Attribute Store** drop-down menu, select **Active Directory**.
12. In the Mapping of LDAP attributes table, on the left-side select **SAM-Account-Name** and on right-side, select **Name ID**.

    Note: Only one mapping is required.

13. Click **Finish**.
14. Click **Apply**.
15. Click **OK**.

    Next you need to configure MFA using Authentication Agent in ADFS. The agent is freely available at (https://community.securid.com/t5/securid-authentication-agent-for/tkb-p/auth-agent-ad-fs-documentation) and for more information on configuration, see ® Authentication Agent 2.0.3 for Microsoft® AD FS Administrator's Guide.

PAM SecurID Log in to NetWitness for AD Users

In this method only SecurID Passcode is required for authenticating to NetWitness. Authentication Manager takes care of the authentication to AD without requiring the password from the user.

After the configuration, the user registered in the Active Directory can log in to NetWitness using the SecurID passcode.

Prerequisites

- NetWitness Platform (NW) version 11.0 or later
- MS Active Directory (AD) – MS Windows Server 2008 R2 or later
- Authentication Manager (AM) 8.2 or later

Perform the following configurations:

1. Configure Authentication Manager.
2. Configure NetWitness.

Configure Authentication Manager

Configure Active Directory as a Identity Source in Authentication Manager using the steps described in the section Add an Identity Source.

Configure NetWitness

Complete the additional configuration for Authentication Manager and NetWitness configuration as described in the section Configure PAM Login Capability.

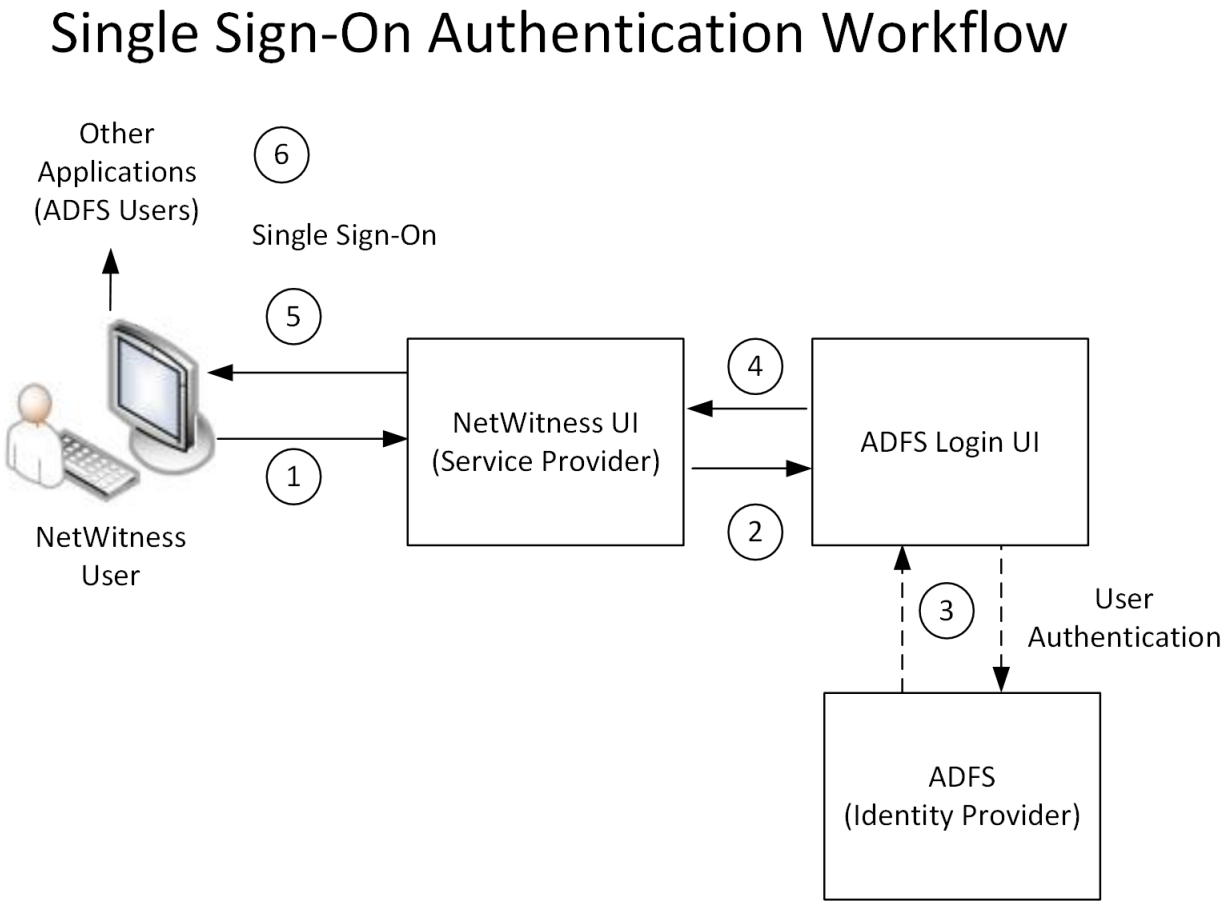
Set Up Single Sign-On Authentication

Note: In 11.4 or later, Single Sign-On (SSO) authentication can be used to access the UI however only one Active Directory is supported. SSO authentication is not supported on an Analyst UI Deployment.

Single Sign-On authentication enables the user to log in to NetWitness or any other application if the user is authenticated by the same Identity Provider (IDP). The Active Directory Federation Services (ADFS) is the only supported IDP and the protocol used for SSO is SAML 2.0.

NetWitness Single Sign-On Authentication Workflow

The following workflow shows how the user can access NetWitness using Single Sign-On authentication.



The workflow of SSO authentication shows the following:

1. User tries to access the NetWitness UI using the web browser. For example, https://nw-host/login.
2. The user is prompted to login into the IDP (ADFS) login page.

3. The user enters the credentials for authentication.
4. If the authentication is successful, NetWitness authorizes the user based on the user groups configured on the Active Directory Server and External Role Mapping in NetWitness.
5. If the authorization is successful, the user is logged into the NetWitness.

Note: If the single sign-on authentication fails, the user cannot access the NetWitness. For more information, see Troubleshooting.

Configure Single Sign-On

The following workflow describes the tasks to be performed in sequence to configure Single Sign-On authentication on NetWitness.

Configure ADFS as IDP for NetWitness

For instructions on how to configure ADFS as IDP for NetWitness, see the *Configure SAML 2.0 provider settings for portals* topic in Microsoft documentation.

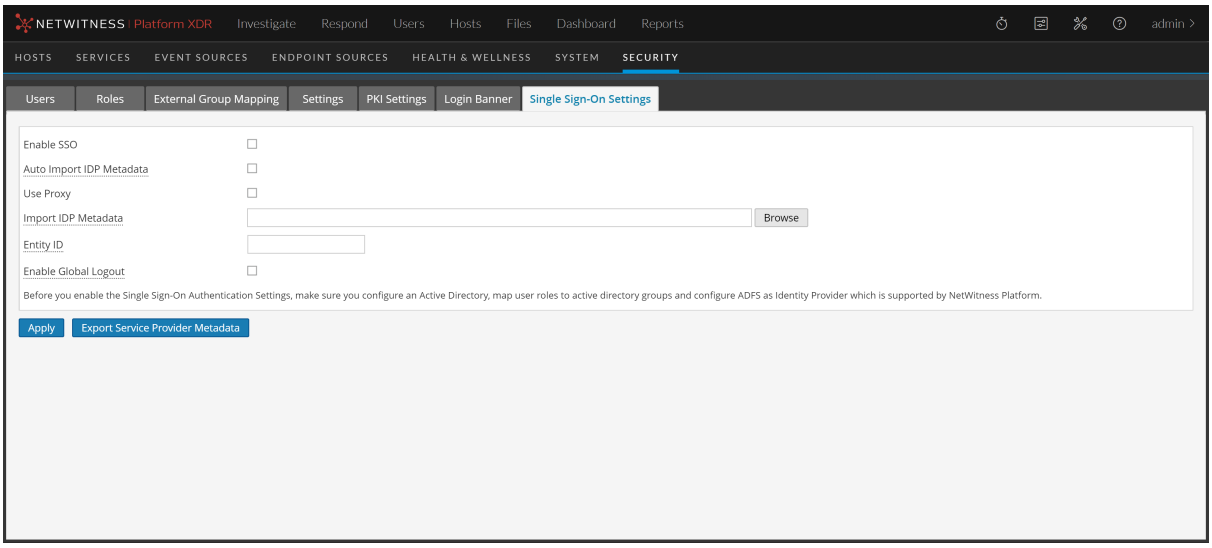
Map User Roles to External Groups

Atleast one Active Directory group should be mapped to an administrator role in NetWitness. For instructions on how to map user roles to Active Directory groups, see (Optional) Map User Roles to External Groups.

Enable Single Sign-On

1. Go to  **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Single Sign-On Settings** tab.

3. Select the **Enable SSO** checkbox.



4. Select the **Auto Import IDP Metadata** if you want the latest IDP metadata to be automatically downloaded at regular intervals.
   When you select this check box, a **Metadata URL** field will be displayed where you must enter the IDP metadata URL.

5. Select **Use proxy** checkbox for the requests to IDP tobe routed through the proxy configured in **(Admin)** > **System** > **HTTP Proxy settings**.

6. Select **Import IDP Metadata** to manually import the meta data and enter the IDP metadata URL.
   Note: Make sure you update the link every time the IDP metadata is updated.

7. Enter a unique entity ID to identify the NetWitness instance in the Identity Provider.

8. (Optional) Select the **Enable Global Logout** checkbox if you want to be logged out of NetWitness along with all the other associated sessions authenticated by IDP.

9. Click **Apply**.
   This may take some time however we recommend you to restart the admin-server immediately. To export the metadata in an XML format either click the link in the notification tray and download the metadata or click **Export Service Provider Metadata** .

Note: The exported Service Provider metadata must be imported to IDP. For more information, see the *Configure SAML 2.0 provider settings for portals* topic in Microsoft documentation.

(Optional) Set Up Public Key Infrastructure (PKI) Authentication

Note: In 11.3 or later, PKI authentication can be used to access the NetWitness UI.

PKI is an authentication method which allows the users to access the NetWitness User Interface (UI) using digital certificates.

The certificates are issued by a Third-Party Certificate Authority (CA) which is external to NetWitness. The following categories of certificates are required for PKI authentication:

- Trusted CA Certificates
- User Certificate (issued by the CA)
- NetWitness Server Certificate (private key and its certificate chain) - Optional

Trusted CA Certificates

Trusted CA certificates are a collection of certificates used by NetWitness as trusted authorities to validate the certificate provided by the user. If the user does not have a certificate signed by one of these CA(s), the user cannot access the NetWitness Platform UI.

User Certificate

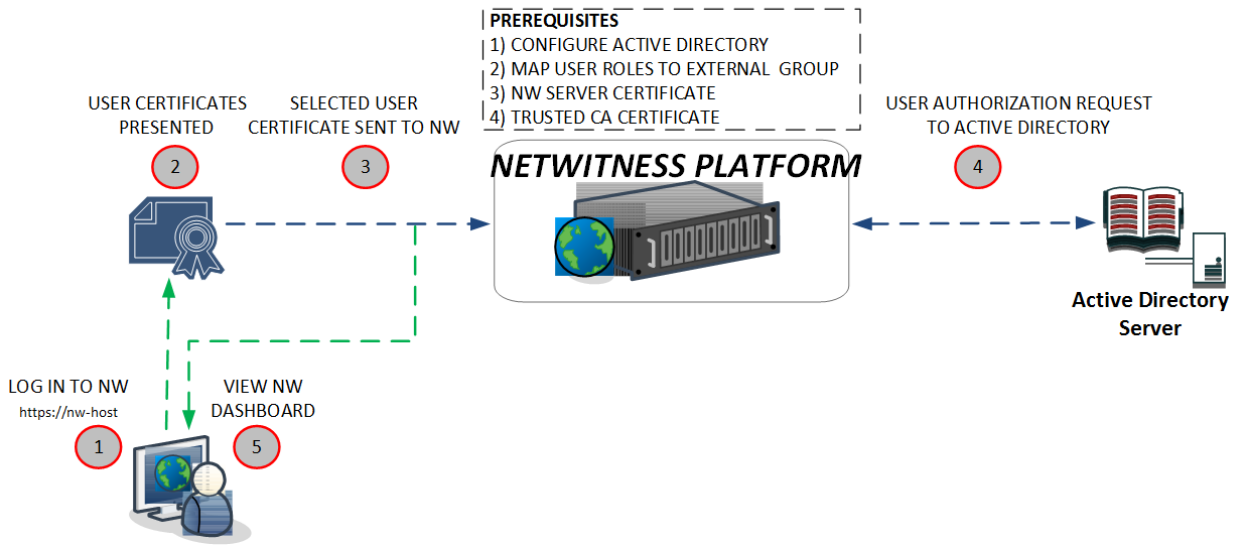
A user certificate is issued by a CA that is trusted by NetWitness and is used by the NetWitness Platform user to present the user identity. By default, user certificates are identified by most browsers. If the certificates are not displayed, you must import the certificates into the browser certificates store.

NetWitness Server Certificate (Optional)

A NetWitness Server certificate is issued by a trusted CA and is used by NetWitness Server to present its identity. If you access the NetWitness Platform UI using HTTPS, the certificate is displayed in the web browser.

NetWitness PKI Authentication Workflow

The following workflow shows how the user can access NetWitness using PKI authentication.



The workflow of PKI authentication shows the following:

1. Access the NetWitness UI using the web browser. For example, https://nw-host/login.
2. The user is prompted to select the user certificate.

Note: The certificate prompt appears differently depending on the browser.

3. The user selects the certificate. The browser sends the selected certificate to the NetWitness for authentication.
4. If the authentication is successful, the NetWitness authorizes the user based on the user groups configured on the Active Directory Server and External Role Mapping in NetWitness.
5. If the authorization is successful, the user is logged into the NetWitness.

Note: If the certificate validation fails, the user cannot access the NetWitness.

Configure PKI Authentication

Perform the following tasks in sequence to configure PKI authentication on NetWitness.

1. Configure Active Directory
2. Map User Roles to External Groups
3. Import Server Certificate and Trusted CA Certificate
4. Enable PKI Authentication

Note: Only Active Directory is supported for PKI Authentication.

Configure Active Directory

For instructions on how to use Active Directory to authenticate external user logins, see Configure Active Directory.

Map User Roles to External Groups

To enable PKI based authentication, a minimum of one external group should be mapped to administrator role in NetWitness. For instructions on how to map user roles to external groups to provide necessary access, see (Optional) Map User Roles to External Groups.

Import Server Certificate and Trusted CA Certificate

To enable PKI authentication, you must import the Trusted CA certificate into the NetWitness. You can import the server certificate and the trusted CA certificate in the  (Admin) > Security view > PKI Settings tab.

Certificate Revocation List

A Certificate Revocation List (CRL) is a file that contains a list of revoked certificates with details such as the serial number and revocation date of each certificate. When a certificate validity is expired, it must be revoked to avoid any compromise of the certificate by unauthorized users. For example, if a NetWitness user resigns from an organization, then the user's certificate must be revoked by the issuing CA.

You can import the CRL or specify the HTTP URL issued by your trusted CA, so that NetWitness can validate with the CRL to block unauthorized users from accessing NetWitness.

To import the CRL or specify a HTTP URL into NetWitness, choose one of the following methods:

- **HTTP server** - This is the most common CRL location where the CA publishes the CRL to external applications using an HTTP server. The NetWitness reads the CRL using the HTTP URL.
- **Local CRL** - This allows the users to manually download the CRL from the CA and upload it to the NetWitness.
- **OCSP (Online Certificate Status Protocol) Responder** - This allows NetWitness to verify the revocation status of a particular certificate instead of validating the complete CRL. To specify a OCSP Responder, you need to provide the HTTP URL and optionally the OCSP Responder's Signing certificate. Make sure the OCSP Responder is online while adding the entry. When the OCSP Responder Signing Certificate is updated, you need to manually update the certificate in NetWitness.

Note: You can configure the CRL when you import the CA certificate or after importing the CA certificate.

User Principal Settings

User Principal Settings allow NetWitness to uniquely identify the user from the user certificate for PKI authentication. To identify the user, you must specify an attribute in the user certificate to extract the user name or user id. NetWitness must be configured to read the value of this attribute. NetWitness uses the extracted value of this attribute as username or user id for authorization and retrieves the user groups from an Active Directory (AD) server. By default, NetWitness extracts the entire value of the selected attribute, without filtering any characters. You can apply regular expression (RegEx) to refine the value extracted.

Note: The conversion of Distinguished Names (attribute in Subject Name or Subject Alternative Name) to a human readable format is done based on RFC2253 (LDAPv3). Therefore, any Relative Distinguished Name apart from the one defined in RFC2253 (LDAPv3) may display in hex format. For example, email attribute value may display #1160bcghryy637bchs774. You can apply RegEX to extract the value. NetWitness tries its best to extract values for such attributes.

User Principal settings can be configured when you import the Trusted CA certificate.

Lookup Query

A Lookup Query sends a specific query to Active Directory to retrieve the user object. Here is an example of a sample query for retrieving a user object from the Active Directory.

```
Sample Query:(&(objectCategory=Person)(objectClass=User)(CN=${nw-pki-user}))
nw-pki-user is replaced with the value extracted from the user certificate.
```

Caution: Make sure that the AD user account is active. AD does not return the user account expiry (accountExpires) information to NetWitness along with user details. Therefore, the NetWitness cannot validate the AD user account is expired or not.

Note: NetWitness does not validate the syntax of the lookup query. You must ensure proper query syntax is used to retrieve the user object from Active Directory.

Import NW Server Certificate with its Private Key

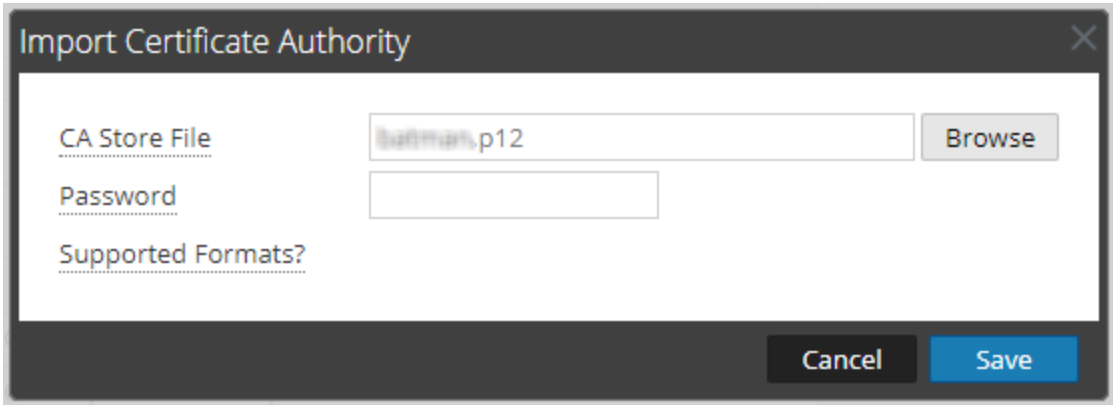
For instructions on how to import the NetWitness Server Certificate with its private key, see (Optional) Use a Custom Server Certificate.

Import Trusted CAs, Configuring CRL and User Principal Settings

To import a trusted CA:

1. Go to  **(Admin) > Security.**
   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.

3. In the **Trusted CAs** section, click  .
   The Import Certificate Authority dialog is displayed.

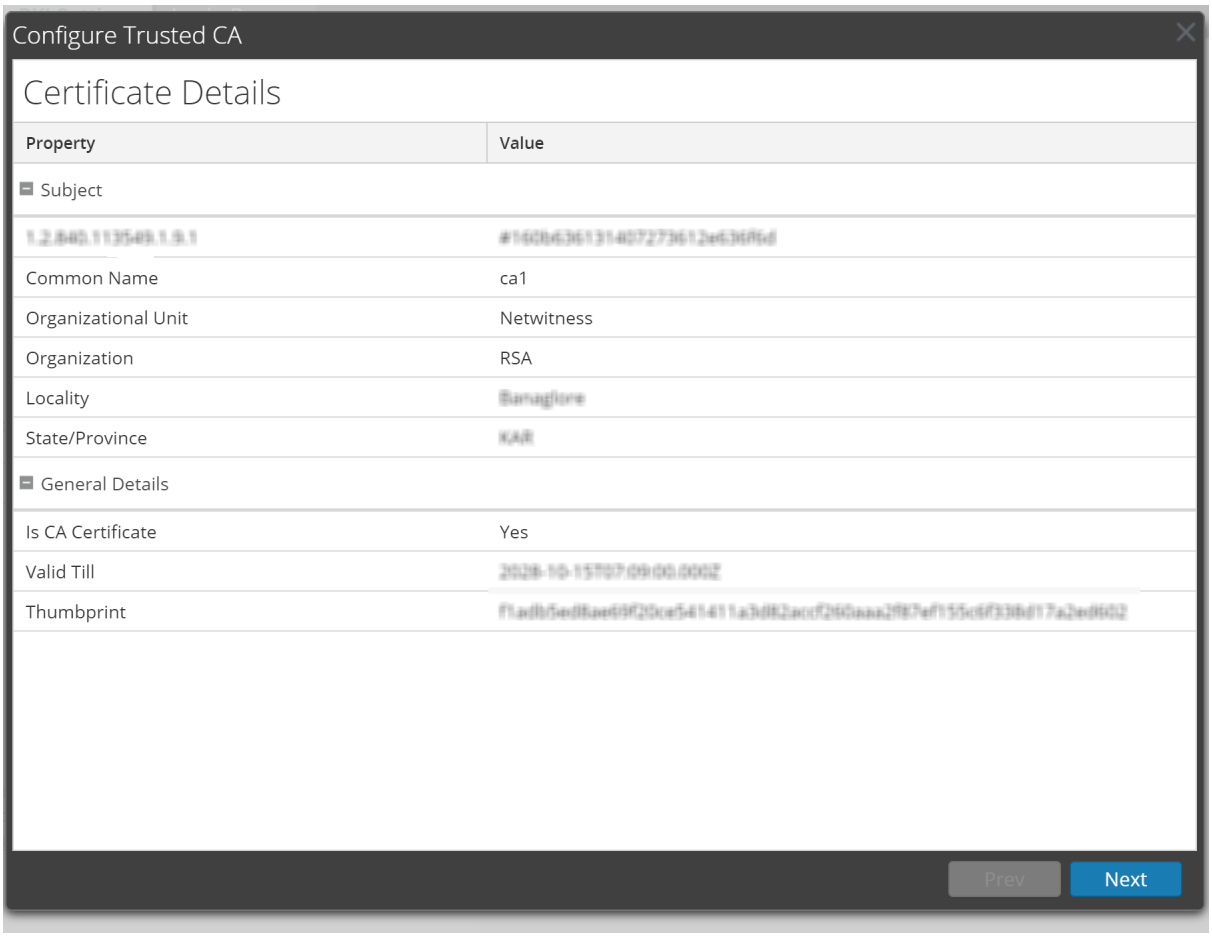


Note: The supported formats are .p12, .jks, .pfx, .pem, .crt, .der, and .cer

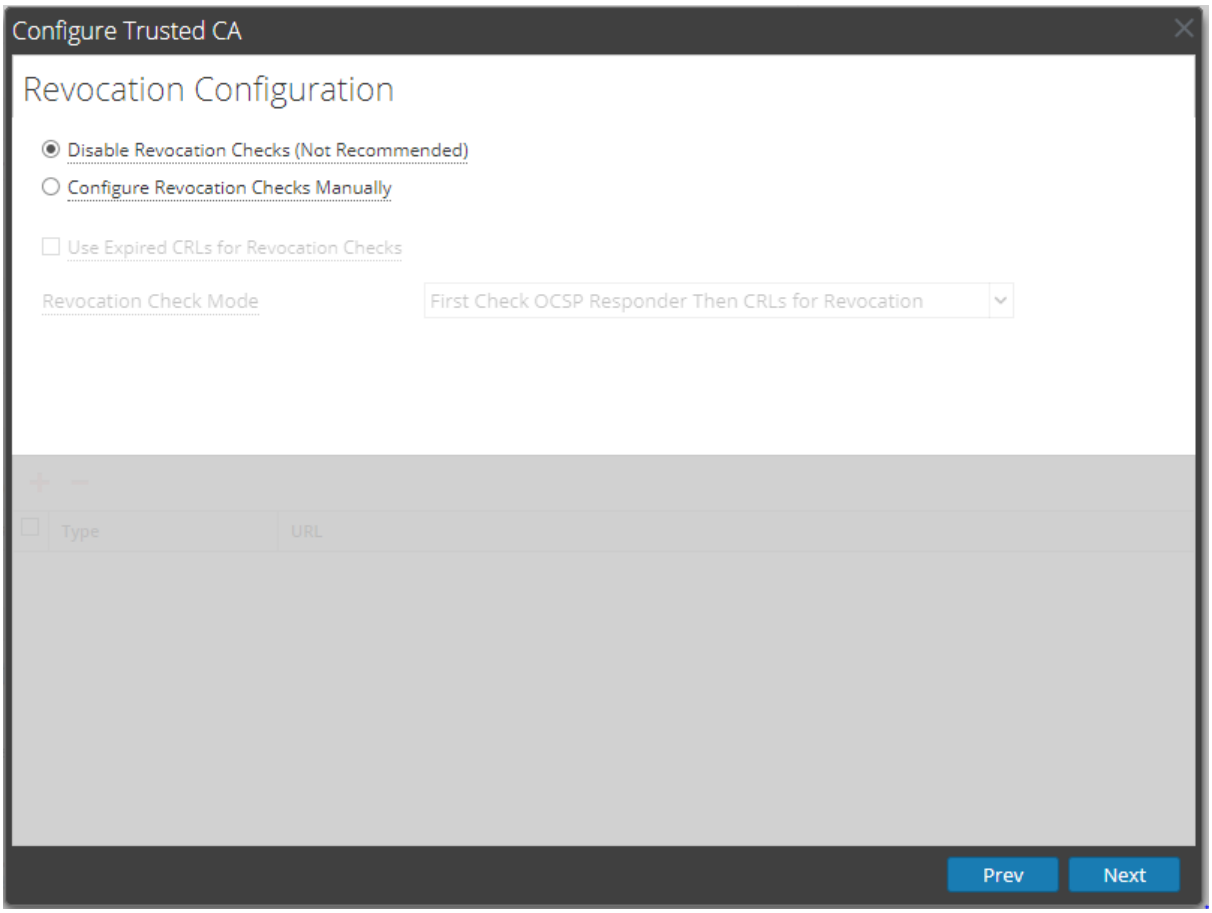
4. In the **CA Store File** field, click **Browse** and select a certificate.
5. In the **Password** field, enter the password of the certificate.

Note: The password is applicable only for .p12, .pfx and .jks certificate formats.

6. Click **Save**.
   A Configure Trusted CA dialog is displayed with Certificate Details.


Configure Trusted CA
Certificate Details
Property
Value
Subject
1.2.840.113549.1.9.1
#160b6361314027273612e636f6d
Common Name
ca1
Organizational Unit
Netwitness
Organization
RSA
Locality
Banaglore
State/Province
KAR
General Details
Is CA Certificate
Yes
Valid Till
2028-10-15T07:09:00.000Z
Thumbprint
f1adb5ed8ae69f20ce541411a3d82accf260aaa2f87ef155c6f338d17a2ed602
Prev
Next

7. Click **Next**.



8. In the Revocation Configuration section, do one of the following to configure the CRL revocation check.

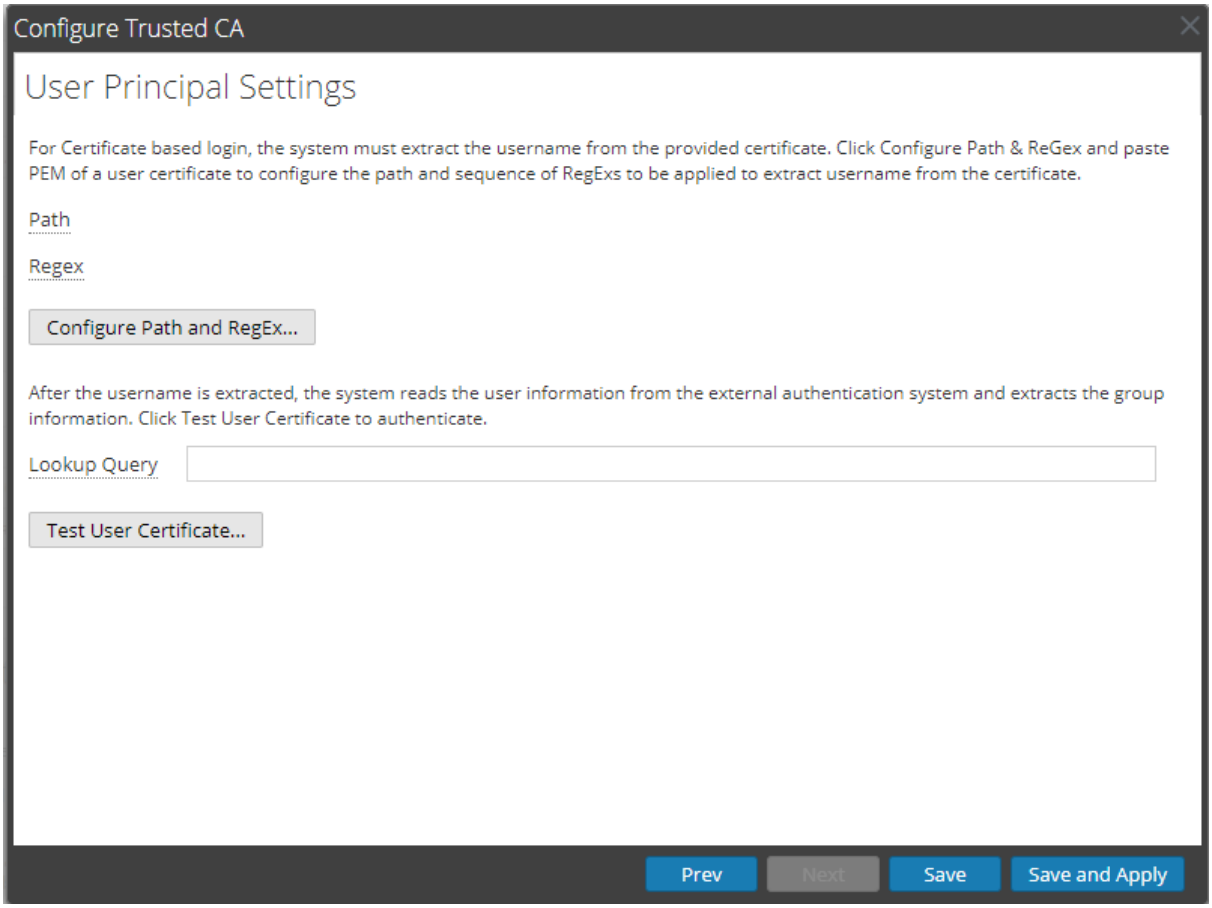
   - Select **Disable Revocation Checks** to disable the CRL revocation check.

   Warning: Disabling the revocation check may increase the risk of unauthorized users logging in to NetWitness.

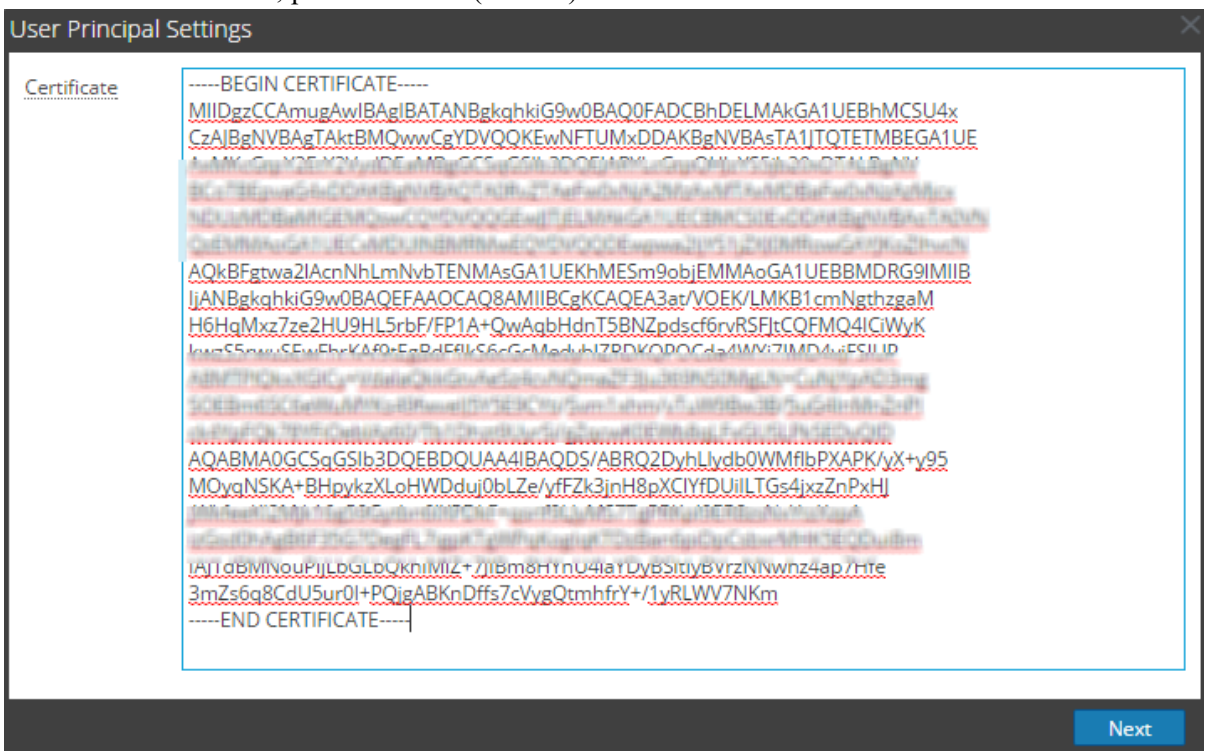
   - Select **Configure Revocation Checks Manually** to manually configure the CRL revocation check.
     For more information, see (Optional) Configure the CRL Manually.

9. Click **Next**.

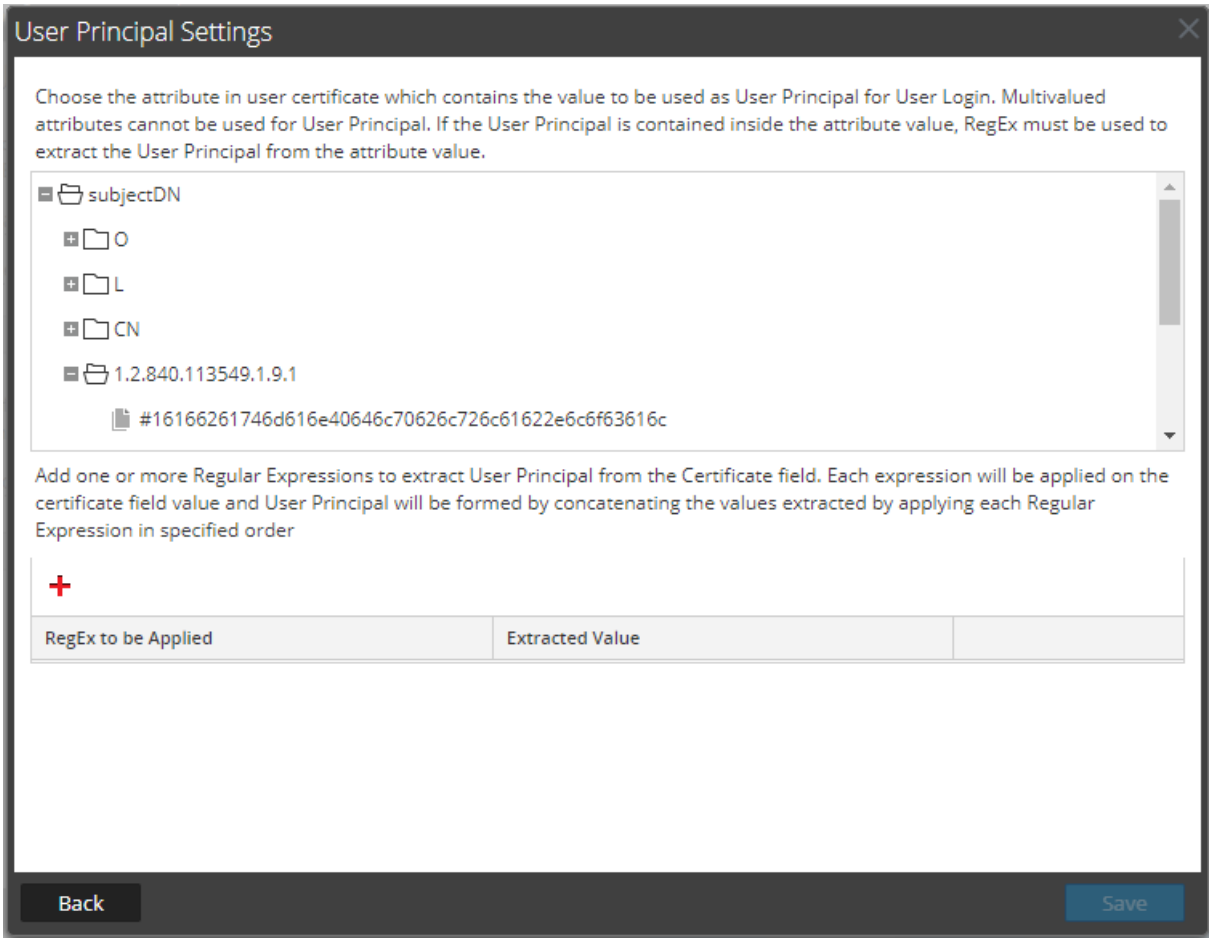
10. To configure user principal settings, in the User Principal Settings section, click **Configure Path and RegEx**.



11. In the **Certificate** field, paste the PEM (Base64) encoded user certificate.



12. Click **Next**.
    The **subjectDN**, **subjectAltnames**, and **extenstions** attributes are displayed.

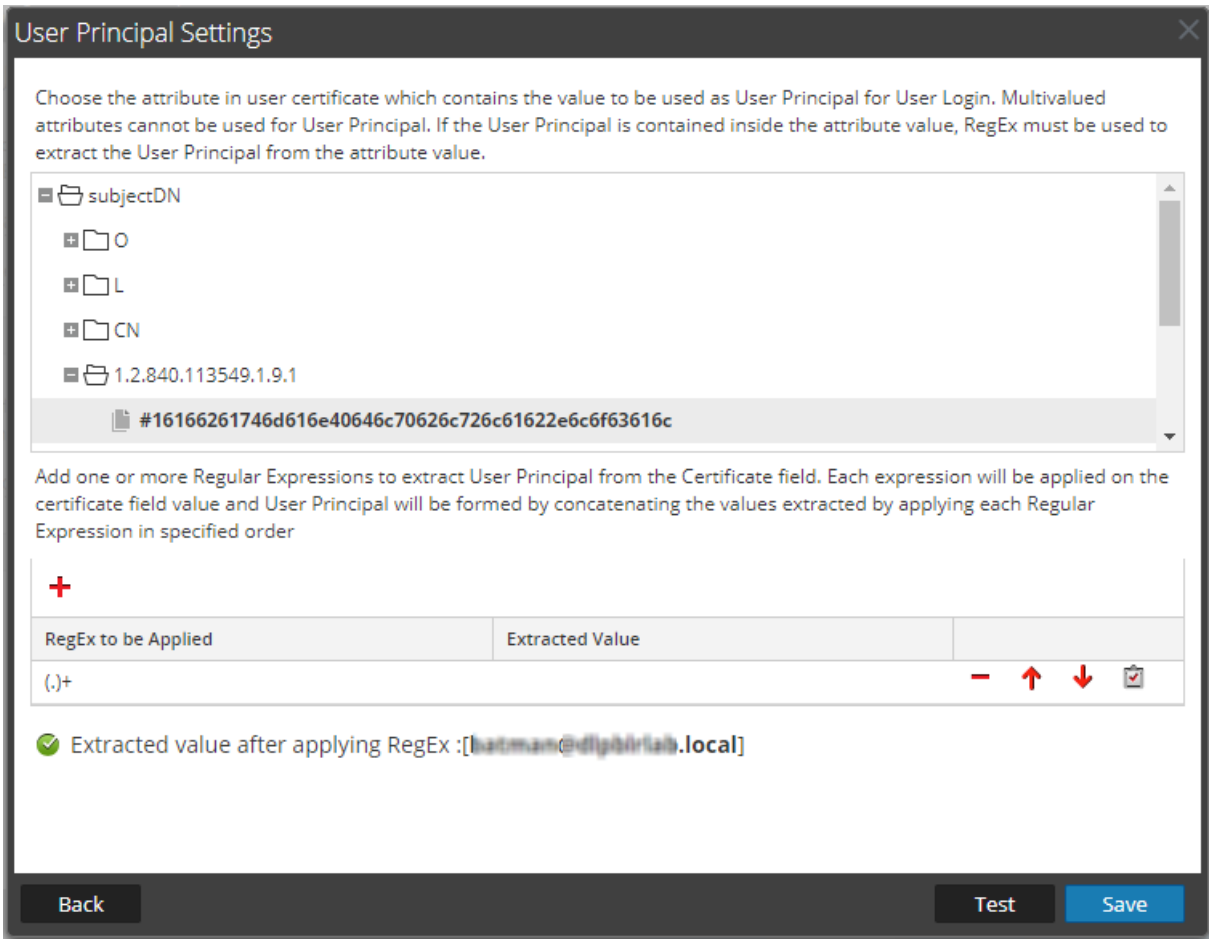


13. Select a unique attribute value to extract the username or user id.

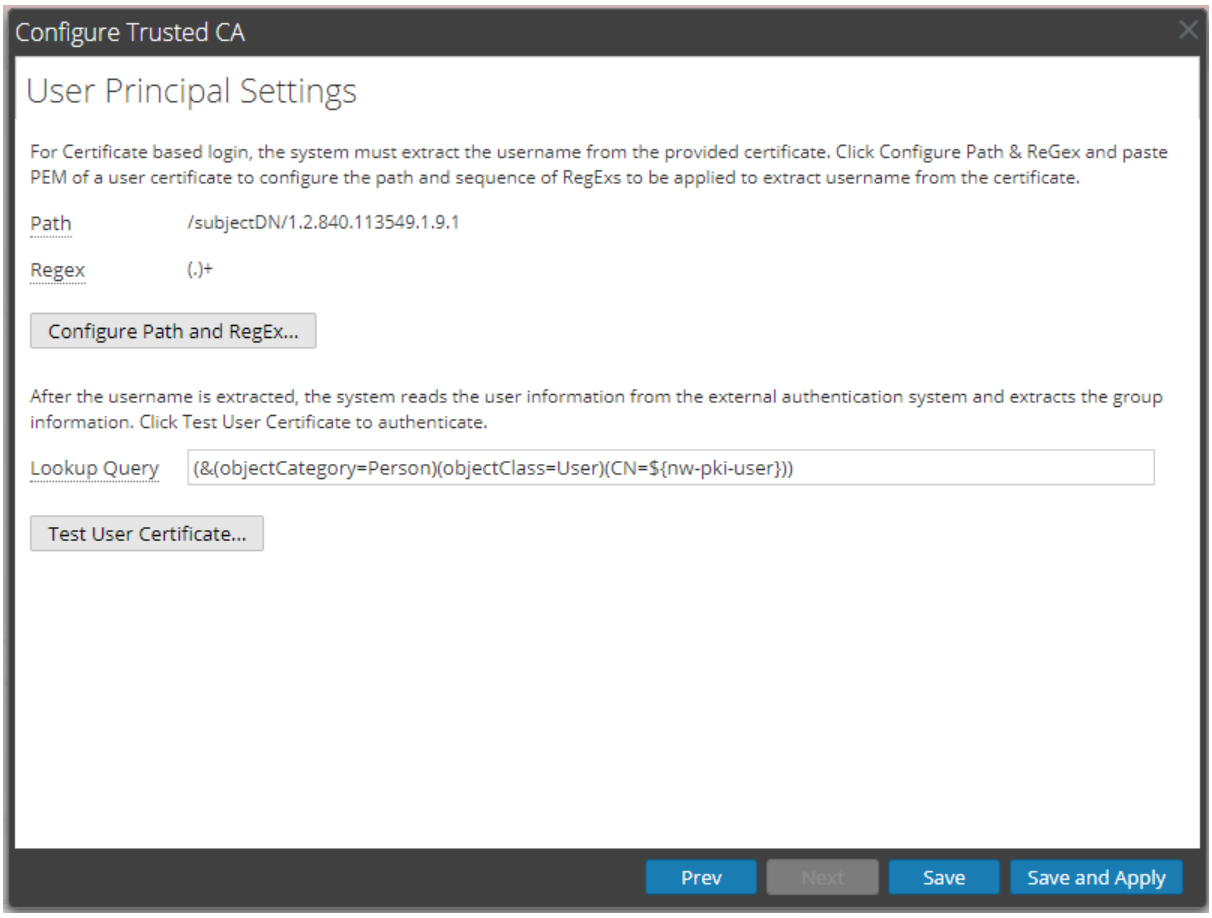
14. To apply RegEx, click  .

> **Note:** You can apply multiple RegEx to extract a username or user id. All of the extracted values are concatenated to generate the final username or user id.

15. Click **Test**.
    The final user name or user id after applying RegEx is extracted and displayed.

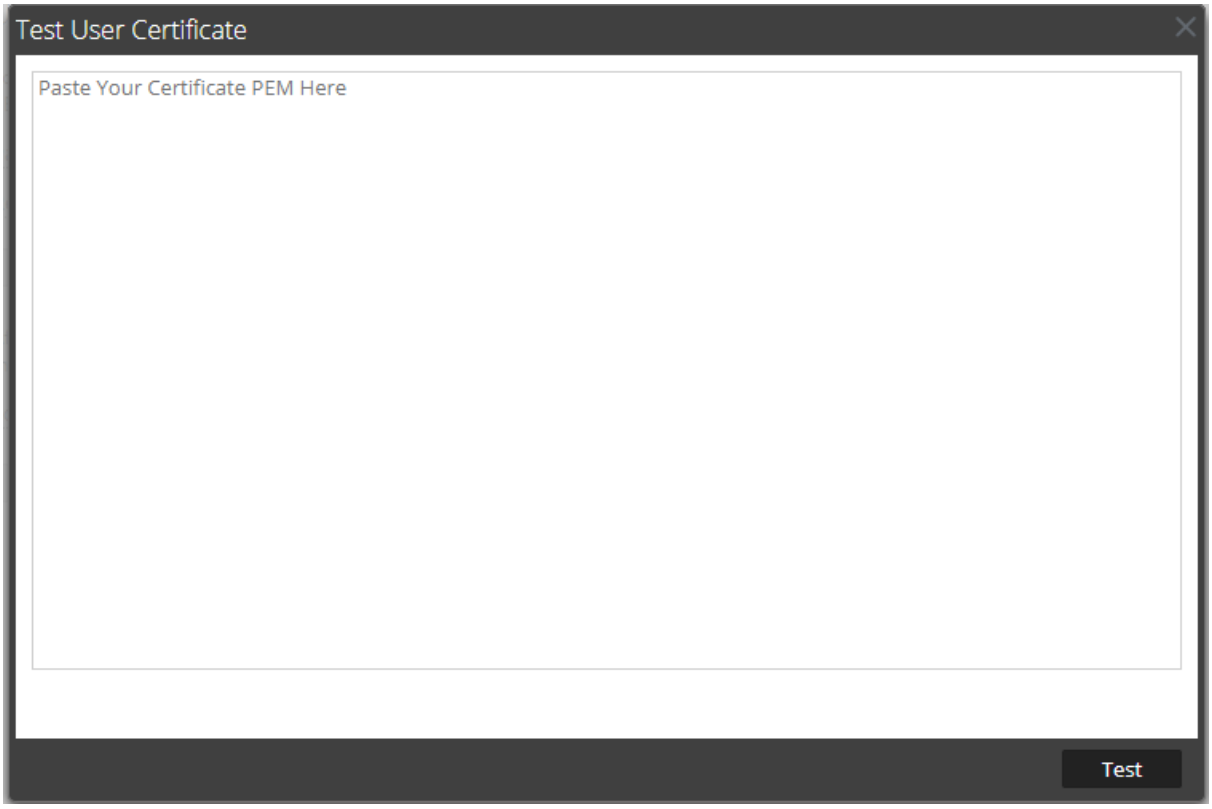

User Principal Settings
Choose the attribute in user certificate which contains the value to be used as User Principal for User Login. Multivalued attributes cannot be used for User Principal. If the User Principal is contained inside the attribute value, RegEx must be used to extract the User Principal from the attribute value.
subjectDN
O
L
CN
1.2.840.113549.1.9.1
#16166261746d616e40646c70626c726c61622e6c6f63616c
Add one or more Regular Expressions to extract User Principal from the Certificate field. Each expression will be applied on the certificate field value and User Principal will be formed by concatenating the values extracted by applying each Regular Expression in specified order
RegEx to be Applied
Extracted Value
(.)+
Extracted value after applying RegEx :[[redacted].local]
Back
Test
Save

16. Click **Save**.



17. Enter the query in the **Lookup Query** field to query the external authentication system for retrieving the user objects.

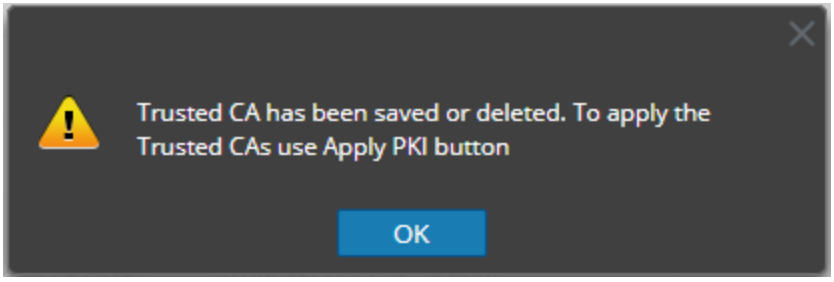
18. Click **Test User Certificate**.
    The Test User Certificate dialog is displayed.



19. Paste the PEM of the user certificate and click **Test**.

Note: The user Certificate is used by NetWitness for a dry-run of the trusted CA configuration. If the user certificate validation and the user id extraction from the certificate is successful, a confirmation message is displayed.

20. After the certificate is validated, click **Save**.
    The following message is displayed.



21. Click **OK**.
    The Trusted CA certificate is added to the NetWitness.

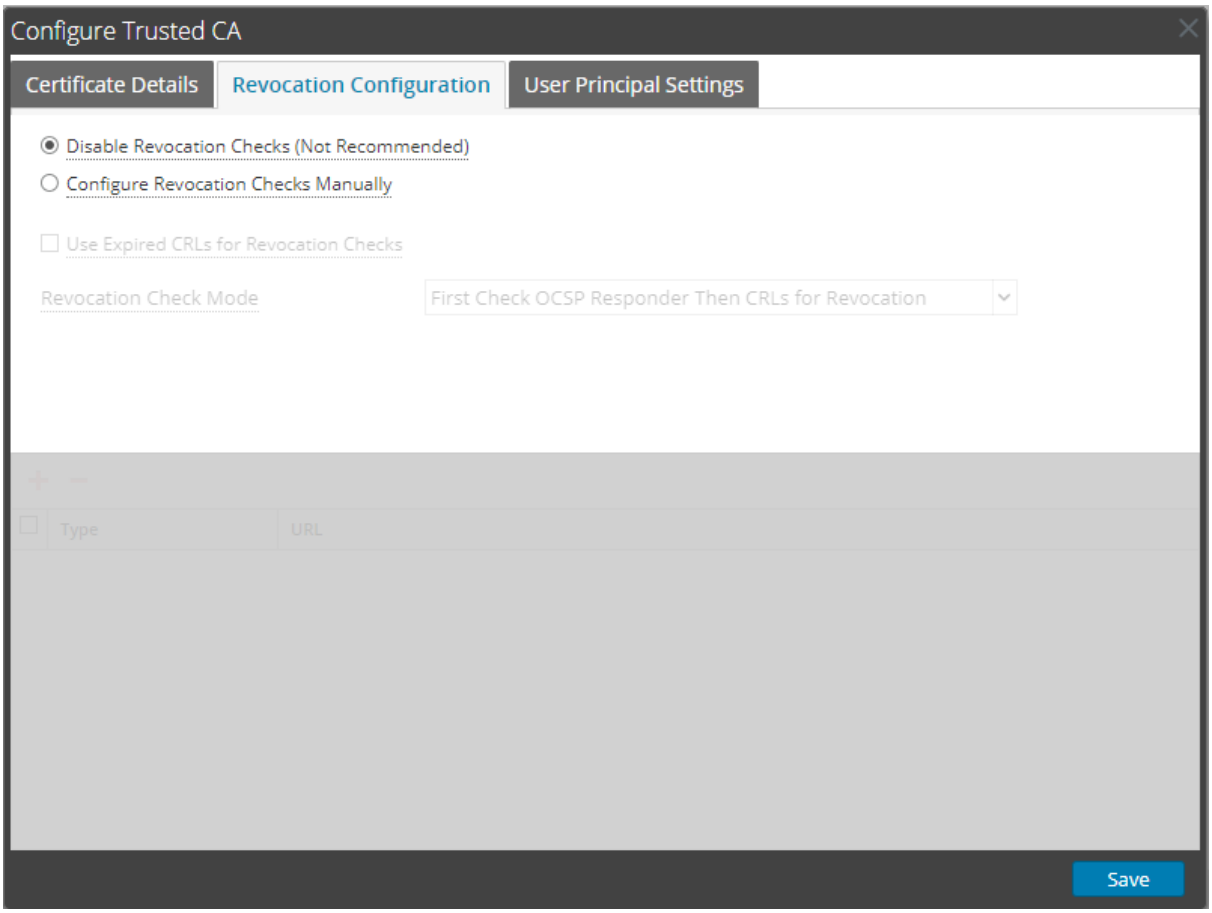
Note: You can add multiple Trusted CA certificates.

(Optional) Configure the CRL Manually

To configure the CRL manually:

1. Double click on the imported CA certificate.

   The Configure Trusted CA dialog is displayed.



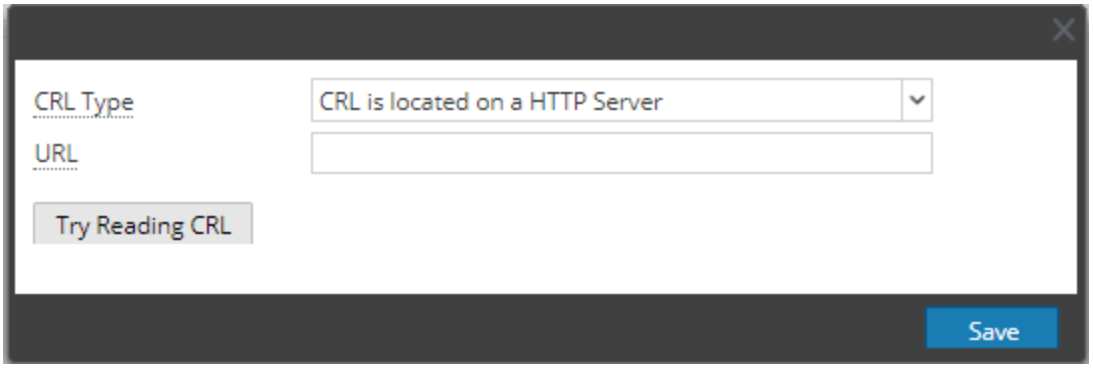
2. In the Revocation Configuration section, select **Configure Revocation Checks Manually**.
3. If the latest CRL is not available, select **Use Expired CRLs for Revocation Checks** to use the expired CRL for revocation.

   Caution: If the above option is enabled, the first CRL in the sequence will be used. This option is useful when you want the NetWitness to work even if PKI system is not available. Make note that first CRL in the sequence is always valid and it will not expire.

4. In the **Revocation Check Mode** field, do one of the following to validate the user certificate.
   - Select **Check only CRLs for Revocation** to use only the CRLs.
   - Select **Check only OCSP Responder for Revocation** to use only the OCSP Responders.
   - Select **First Check CRLs then OCSP Responder for Revocation** to use the CRL. If all the CRLs are expired, use the OCSP Responders.

- Select **First Check OCSP Responder Then CRLs for Revocation** to use the OCSP Responders. If all the Responders are offline or unavailable, use the CRLs.

5. Click  to add the CRL.



6. To add a CRL published on a HTTP server:
   a. In the **CRL Type** field, select **CRL is located on a HTTP server**.
   b. In the **URL** field, specify the HTTP URL to access the CRL

Note: Make sure that the CRL is available and HTTP server is accessible from NetWitness.

7. To upload a CRL file downloaded from the CA:
   a. In the **CRL Type** field, select **CRL is available as a File**.
   b. In the **CRL file** field, click **Browse** to upload the CRL file.

Note: Make sure that the CRL is downloaded from CDP location.

8. To add a OCSP Responder:
   a. In the **CRL Type** field, select **HTTP URL for OCSP Responder.**
   b. In the **URL** field, specify the HTTP URL.
   c. In the **Certificate** field, click **Browse** to upload the OCSP Responder Signing Certificate.

Note: Make sure that the OCSP Responder is accessible from NetWitness.

9. Click **Try Reading CRL**.

   The NetWitness UI displays the extracted information from the CRL.

Note: The CRL revocation check is done in the sequence that the CRL is added.
For example:
- If there are two CRLs configured and both are valid, only the first CRL is considered for revocation. The second CRL is considered for revocation only after the first CRL expires.
- If there are two CRLs configured, if the first CRL is expired and you select **Use Expired CRLs for Revocation Checks**, the first CRL is only considered for revocation check and second CRL is ignored.

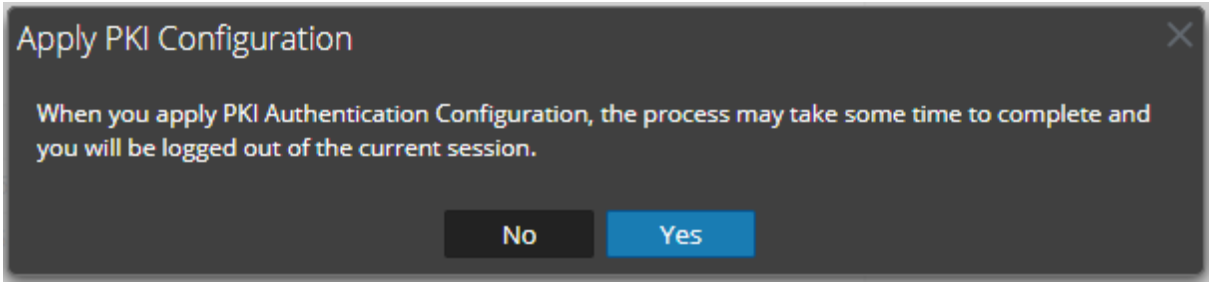
If the HTTP URL is located on the HTTPS location, the NetWitness does not validate the web server certificate of the HTTP server on which the CRL is located.

10. Click **Save**.

    The CRL file is added to the NetWitness.

Enable PKI Authentication

1. Go to  **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.
3. In the PKI Based Authentication Status section, select **Enabled**.
4. Click **Apply PKI Configuration**.
   The PKI Based Authentication Enabled dialog is displayed.



5. Click **Yes**.

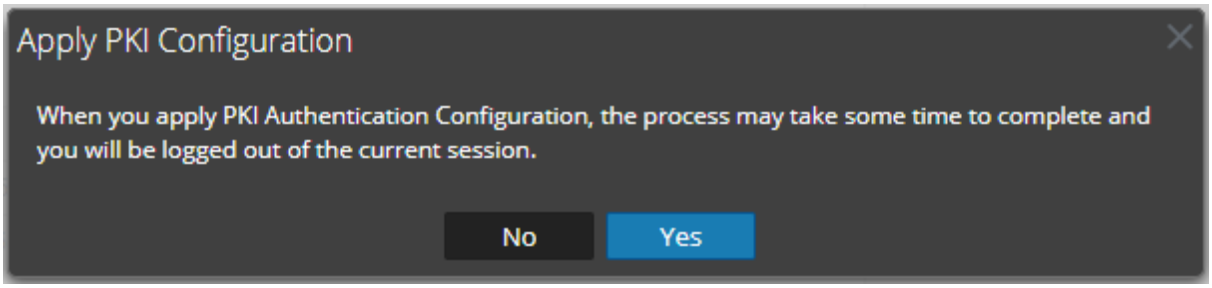
Note: After you enable PKI,
- Do not delete the AD configuration and external group mapping that corresponds to the user certificate's domain.
- Log out from a PKI based session by closing the browser used to access NetWitness.
- If audit log is enabled, the user login and activity is logged using the user DN.

Disable PKI

Note: If NetWitness users or Administrators are unable to access the NetWitness UI and want to use user name and password based authentication, you must disable PKI using the command line. See, Disable PKI using command line.

Disable PKI Authentication

1. Go to  **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.
3. In the PKI Based Authentication Status section, select **Disabled**.
   The PKI Based Authentication Disabled dialog is displayed.



4. Click **Yes**.

Note: After disabling the PKI, wait for some time, close the browser, and open NetWitness in a new browser.

Disable PKI using command line

1. SSH to access root@node-0.
2. Run the following command:
   a. `nw-shell`.
   b. `login` {Enter the username and password to login}
   c. `connect --service orchestration-server`
   d. `cd /rsa/orchestration/userpki/disable-pki-on-hosts`
   e. `invoke`
   f. `connect --service admin-server`
   g. `cd /rsa/security/authentication/web/pki-enabled`
   h. `set false`
   i. `cd/rsa/security/pki/client-auth`
   j. `set WANT`
   k. `exit`
   l. `systemctl reset rsa-nw-admin-server`
   m. `systemctl reset-nw-security-server`

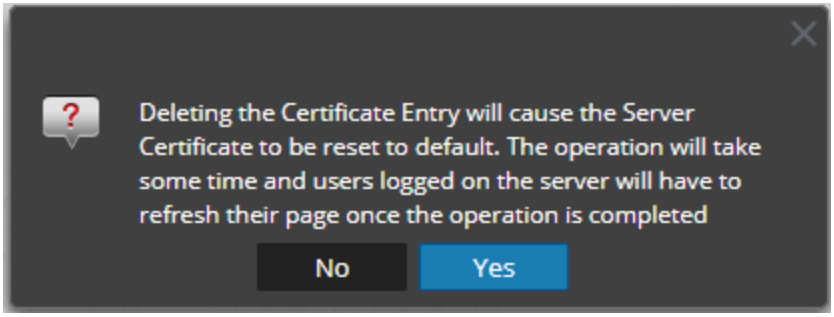
Note: The command `systemctl restart rsa-nw-admin-server` restarts the admin server and `systemctl restart rsa-nw-security-server` restarts the security server.

Delete Server Certificate and Trusted CA Certificate

Note: Deleting the server certificate may cause NetWitness to apply the default server certificate on the selected appliance.

To delete a NetWitness Server Certificate with its Private Key:

1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.
3. In the **Server Certificates** section, select the certificate to delete.
4. Click .
   The following message is displayed.

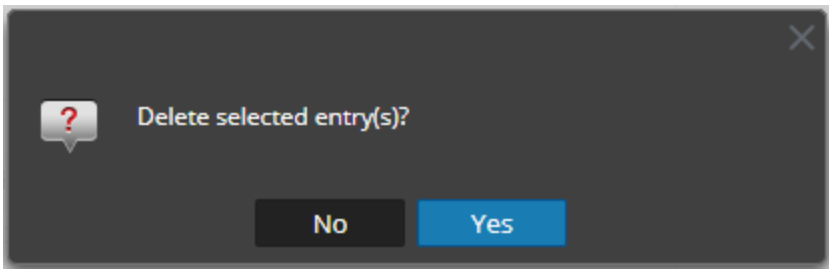


5. Click **Yes**.

Note: When the certificate is being applied on the selected appliance, no other operation on PKI can be performed until the process is completed.

To delete a Trusted CA Certificate:

1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.
3. In the **Trusted CAs** section, select the certificate to delete.
4. Click .
   The following message is displayed.



5. Click **Yes**.

Note: Make sure you apply the PKI configuration again after deleting the Trusted CA certificate.

Troubleshooting

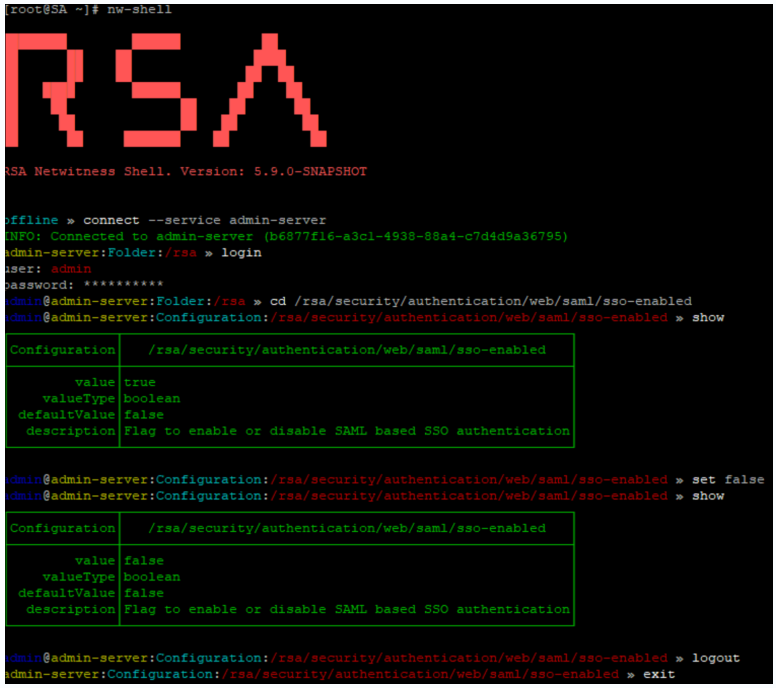
This topic provides information about possible issues that NetWitness users may encounter when configuring the System Security and User Management settings in NetWitness. You can look up explanations of issues and their solutions.

Users are able to create a password of 8-chracters or less despite the configured minimum password length of 9 characters in Version 11.3

Problem	Solutions
When NetWitness was upgraded from 11.2 and previous versions to Version 11.3, the administrator did not set the minimum password length to 9 characters.	In 11.2 and earlier versions, the minimum password length is 8. The minimum password length changed to 9, in Versions 11.3. If you upgrade or update from earlier versions to 11.3, users can still create a password of 8 characters until you explicitly set the minimum password length to 9 characters as described in Configure Password Complexity.

Unable to log in to NetWitness Platform using SSO

Problem	Solutions
When the Administrator configures the SSO incorrectly and is unable to log in to NetWitness.	**Manual Steps to Disable SSO** To resolve this issue you must disable SSO manually, using the following commands: 1. SSH to `admin server node`. 2. Connect to `nw-shell`. 3. Connect to admin server service using the `connect --service admin-server` command. 4. Log in to admin server using the `login` command. 5. Enter the admin username and password. 6. Execute the following commands: • `cd /rsa/security/authentication/web/saml/sso-enabled` • `set false` • `logout` • `exit` • `systemctl restart rsa-nw-admin-server`



Problem	Solutions
Unable to connect to IDP and request session has timed out	• Check if the admin server is able to reach the specific IDP metadata URL. • Check if the IDP can be to accessed over the internet, if not configure the proxy and try again.
SSL handshake failed as the certificate is not verified	• Enable the `trust-all-certs-for-idp-metadata` flag in the explorer view of admin-server by navigating to RSA>Security>Authentication>Web>SAML. • Import the SSL certificate of the IDP metadata server to the JVM trust store, run the command `keytool -import -trustcacerts -file /root/selfsignedadfs.cer -alias selfsignedcert -keystore /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.222.b10-0.el7_6.x86_64/jre/lib/security/cacerts` on the Admin node.
SSL handshake failed as the hostname is not verified	• Check the IDP metadata server's SSL certificate has a valid DN and matches the server hostname. • Enable the `trust-all-certs-for-idp-metadata` flag in the explorer view of admin-server by navigating to RSA>Security>Authentication>Web>SAML.
Fail over IP address changed	Perform the following manual steps to configure the new IP address. 1. Disable SSO using nw-shell after failover from new IP. For more information, see Manual Steps to Disable SSO 2. Generate the new metadata and reupload it in ADFS. For more information, see see the *Configure SAML 2.0 provider settings for portals* topic in Microsoft documentation.

References

This section is a collection of references for system security and user management in NetWitness.

- Admin Security View
- Users Tab
- Add or Edit User Dialog
- Roles Tab
- Add or Edit Role Dialog
- External Group Mapping Tab
- Add Role Mapping Dialog
- Search External Groups Dialog
- Settings Tab
- PKI Settings Tab
- Login Banner Tab

Admin Security View

The Admin Security view provides the capability to manage user accounts, manage user roles, map external groups to NetWitness roles, and modify other security-related system parameters. These apply to the NetWitness system and are used in conjunction with the security settings for individual services.

What do you want to do?

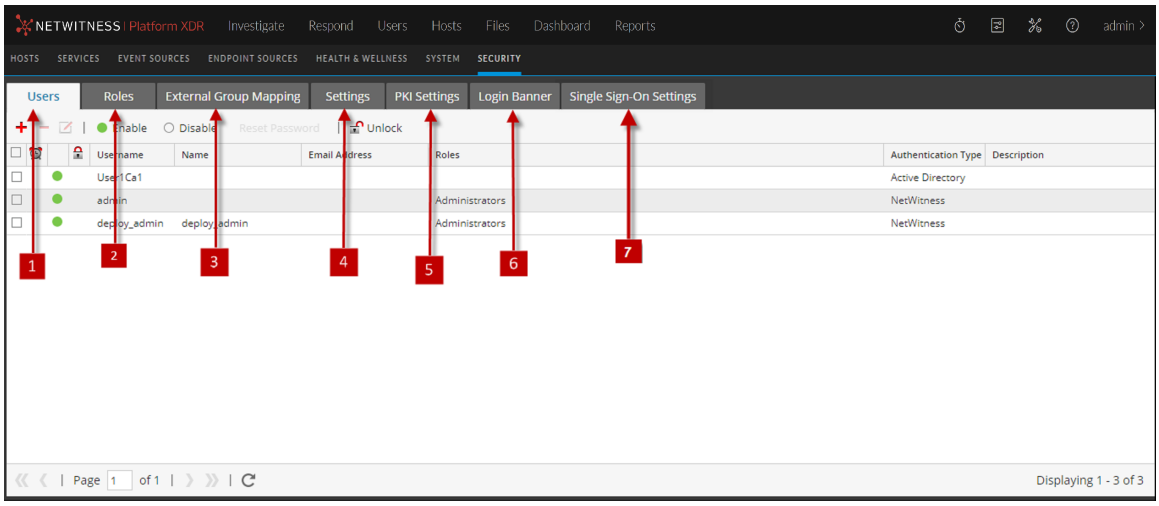
Role	I want to ...	Show me how
Admin	Manage users	Set Up Users
Admin	Manage roles	Review the Preconfigured NetWitness Platform Roles (Optional) Add a Role and Assign Permissions
Admin	Configure settings	Configure System-Level Security Settings
Admin	(Optional) Configure external group mappings	(Optional) Map User Roles to External Groups
Admin	(Optional) Set login conditions	(Optional) Create a Customized Login Banner
Admin	(Optional) Set up PKI	Configure PKI Authentication

Related Topics

- Users Tab
- Roles Tab
- External Group Mapping Tab
- Settings Tab
- PKI Settings Tab
- Login Banner Tab

Quick Look

To display the Admin Security view, go to  **(Admin) > Security**.

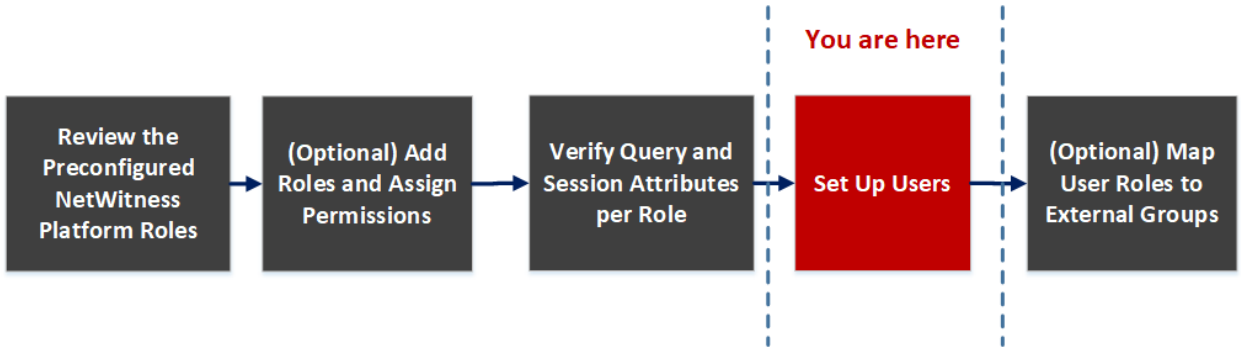


1. **Users** tab allows you to manage user accounts.
2. **Roles** tab allows you to define security roles and assign roles to user accounts.
3. **External Group Mapping** tab allows you to manage access parameters for LDAP groups.
4. **Settings** tab allows you to configure password complexity and expiration for internal NetWitness users and to configure system behavior due to failed logins and inactivity. It also allows you to configure external authentication.
5. **PKI Settings** allows you to enable and disable the PKI authentication.
6. **Login Banner** tab allows you to set conditions which must be agreed to before gaining access to the login screen.
7. **Single Sign-On Settings** tab allows you to enable and disable the SSO authentication.

Users Tab

The Users tab in the Admin Security view allows you to set up user accounts. Each NetWitness user must have a user account. In the Users tab, you can create, edit, delete, enable, disable, and unlock a user account.

Workflow



What do you want to do?

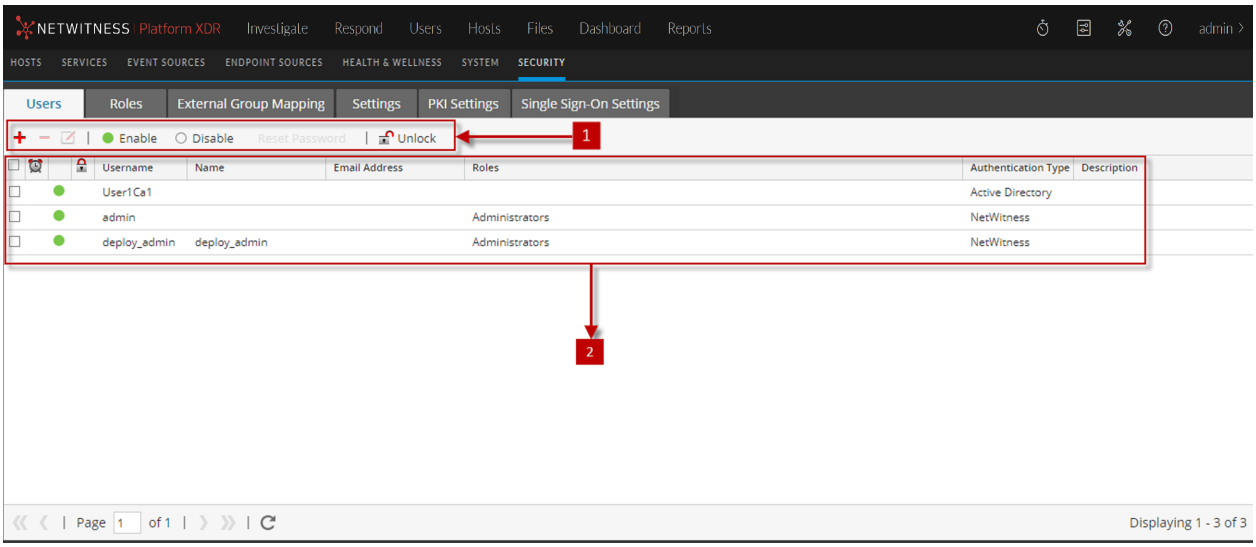
Role	I want to ...	Show me how
Admin	Set up a new user	Set Up Users
Admin	Manage user accounts	

Related Topics

- Add or Edit User Dialog

Quick Look

To access this view, go to  **(Admin) > Security**. The Security view displayed with **Users** tab open.



The Users tab includes the following panels.

1 **Users** toolbar
2 **Users** list

Users Toolbar

The following table describes the Users toolbar.

Feature	Description
+	Opens the Add User dialog.
−	Deletes the selected user.
	Opens the Edit User dialog for the selected user.
Enable	Enables a disabled user account with all user preferences intact.
Disable	Blocks user access without deleting user preferences so that upon re-enabling users, user preferences are intact.
Reset Password	Opens the Reset Password dialog, which enables you to change the password of the selected user. This dialog lists the password format requirements necessary to change the password and allows you to force the user to change their password on the next login.
Unlock	Unlocks a user account that has been locked due to too many failed login attempts.

Users List

The following table describes the columns in the Users list.

Column	Description
	If this icon appears in a user row, it indicates that the user password has expired.
Username	Username to log on to NetWitness.
Name	Name of the user to whom the account belongs.
Email Address	Email address of the user.
Roles	Role assigned to the user.
Authentication Type	Authentication method, which could be external by Active Directory or PAM or internal by NetWitness.
Description	Description of the user account.

Add or Edit User Dialog

All users must either have a local user account with a username and password or an external user account that is mapped to NetWitness.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Add a User and Assign a Role	
Administrator	Change User Information	
Administrator	Reset a User Password	
Administrator	Add a User for External Authentication	

Related Topics

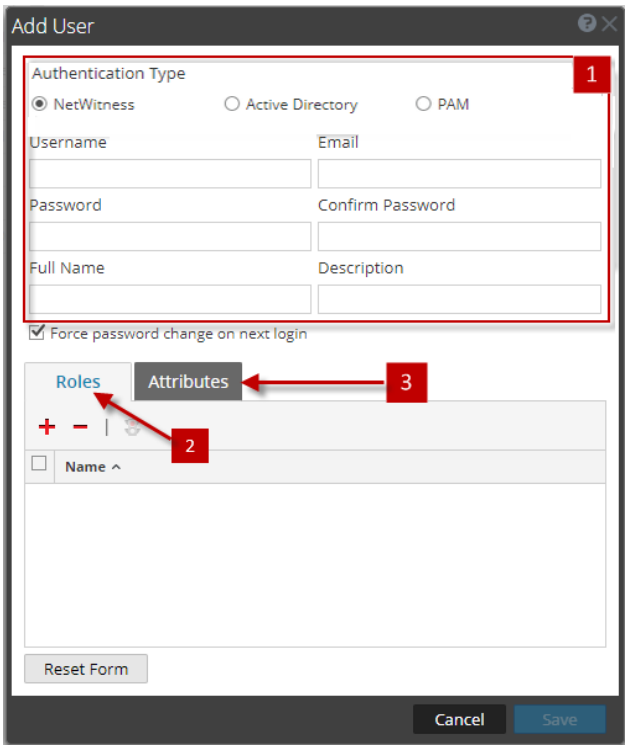
- Manage Users with Roles and Permissions

Quick Look

To access Add or Edit User dialog, go to  **(Admin) > Security > Users** tab and in the toolbar, click  , or select a user and click .

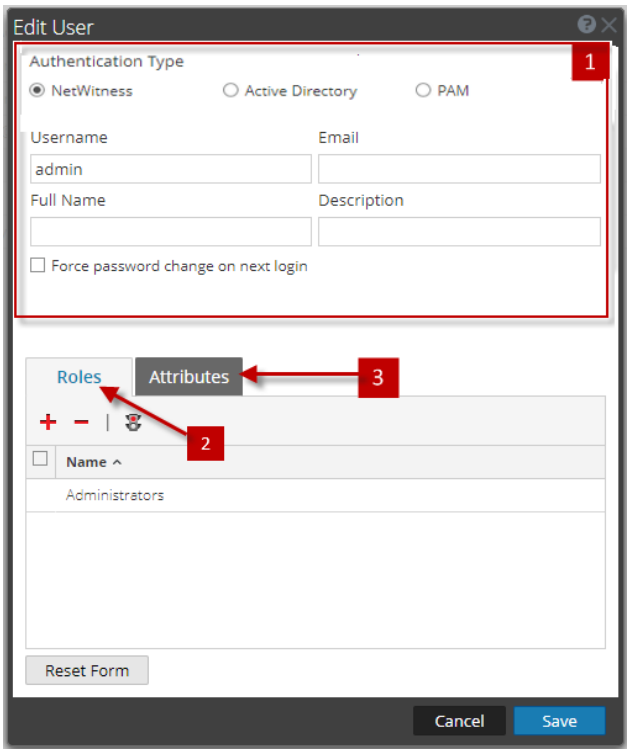
Add User Dialog

This is the Add User dialog for an internal user.



Edit User Dialog

This is the Edit User dialog for an internal user.



The Add User and Edit User dialogs are the same except that the Add User dialog contains additional **Password** and **Confirm Password** fields. You can add a password for a new user in the Add User dialog. Users can change their own passwords in the user preferences. You can reset a password for a user directly from the Users tab.

The Add User and Edit User dialogs have following sections:

1. User information
2. **Roles** tab
3. **Attributes** tab

User Information

The following table provides descriptions of the user information.

Field	Description
NetWitness	Authenticate with NetWitness.
Active Directory	Authenticate with Active Directory.
PAM	Authenticate with PAM.
Username	Username for the NetWitness user account.
Email	Email address of the user.
Password	(Add User dialog only) Password to log on to NetWitness.
Confirm Password	(Add User dialog only) Password confirmation for adding the user password.
Full Name	Name of the user.
Description	(Optional) Description of the user.
Force password change on next login	Expires the user password the next time the user logs on to NetWitness. This field applies only to internal users. This does not affect any active user sessions. The ⏰ appears in the user row to show that the user password expired. After a password is expired, you cannot undo it. This checkbox is cleared the next time you edit the user account.
Reset Form	Removes any changes in process.

Roles Tab

The following table provides descriptions of the **Roles** tab options. The Roles tab shows the roles that are assigned to the user.

Option	Description
+	Opens the Add Role dialog that lists roles you could assign to the user.

Option	Description
	Removes the selected role from being assigned to the user.
	Shows permissions for the selected role.
Name	Lists each role assigned to the user.

Attributes Tab

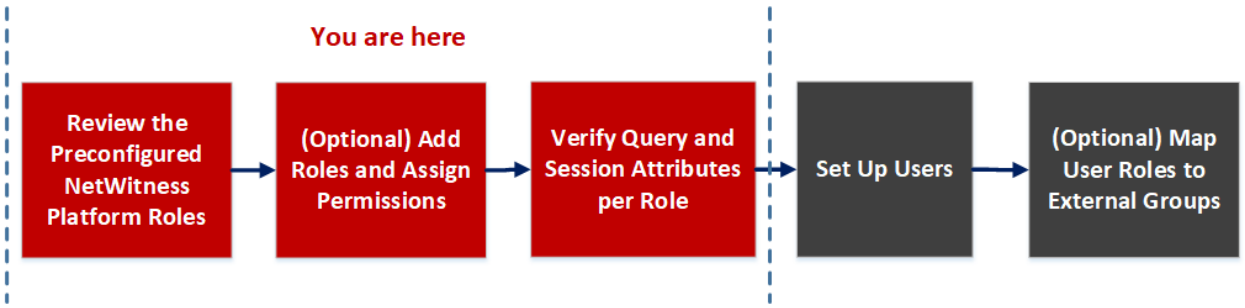
The following table lists the descriptions of the **Attributes** tab options. The **Attributes** tab shows the attributes that are assigned to the user.

Option	Description
Core Query Timeout	(Optional) Specifies the maximum number of minutes that a user can run a query. The default value is 5 minutes. This timeout only applies to queries performed from Investigation. If this value is set, it must be zero (0) or greater. A value of zero represents no timeout.
Core Session Threshold	Controls how the service scans meta values to determine session counts. This value must be zero (0) or greater. If this value is greater than zero, a query optimization will extrapolate the total session counts that exceed the threshold. When the meta value returned by the query reaches the threshold, the system will: • Stop its determination of the session count • Show the threshold and percentage of query time used to reach the threshold The default value is `100000`. The limit you specify here overrides the **Max Session Export** value defined in the Investigate view settings.
Core Query Prefix	(Optional) Filters query results to restrict what the role members see. By default, this is blank. For example, the `'service' = 80` query prefix prepends to any queries run by the user and the user can only access meta of HTTP sessions.

Roles Tab

Roles are assigned to all NetWitness users. Users receive the permissions the roles allow. In the Roles tab you can create, duplicate, edit and delete a role. You can also see a list of all roles and their respective permissions.

Workflow



Related Topics

- Add or Edit Role Dialog

What do you want to do?

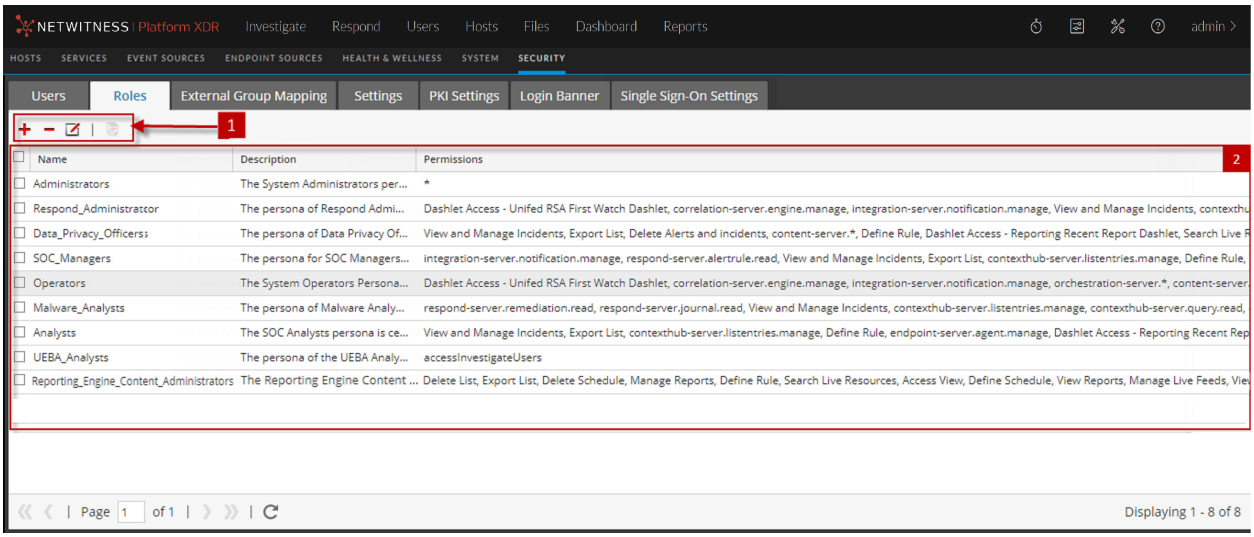
Role	I want to ...	Show me how
Admin	View preconfigured roles	Review the Preconfigured NetWitness Platform Roles
Admin	Create a new role	(Optional) Add a Role and Assign Permissions

Related Topics

- Add or Edit Role Dialog

Quick Look

To access **Roles** tab view, go to  **(Admin) > Security** and click the **Roles** tab.



The Roles tab has the following sections.

1 **Roles** toolbar
2 **Roles** list

Roles Toolbar

The following table describes the **Roles** toolbar.

Icon	Description
	Displays the Add Role dialog.
	Displays the Edit Role dialog.
	Displays a warning message, and asks for confirmation that you want to delete a role.
	Duplicates a role to save with a different name.

Roles list

The following table describes the columns in the **Roles** list.

Column	Description
Name	Displays the name of a role that can be given to a user.
Description	Displays a description of the role.
Permissions	Displays the permissions assigned to the role.

Add or Edit Role Dialog

In the Add Role and Edit Role dialogs, you can add or edit a role and the permissions assigned to it. You can also specify the query-handling attributes for role members to lock down the information that they can retrieve. The structure of these dialogs is the same. The only difference is that you either add a new role or modify an existing role.

When you change permissions for a role, the change is immediately applied to users who are assigned the particular role after the role is saved.

What do you want to do?

Role	I want to ...	Show me how
Admin	View preconfigured roles	Review the Preconfigured NetWitness Platform Roles
Admin	Create a new role	(Optional) Add a Role and Assign Permissions
Admin	Edit a role	(Optional) Add a Role and Assign Permissions
Admin	Delete a role	(Optional) Add a Role and Assign Permissions

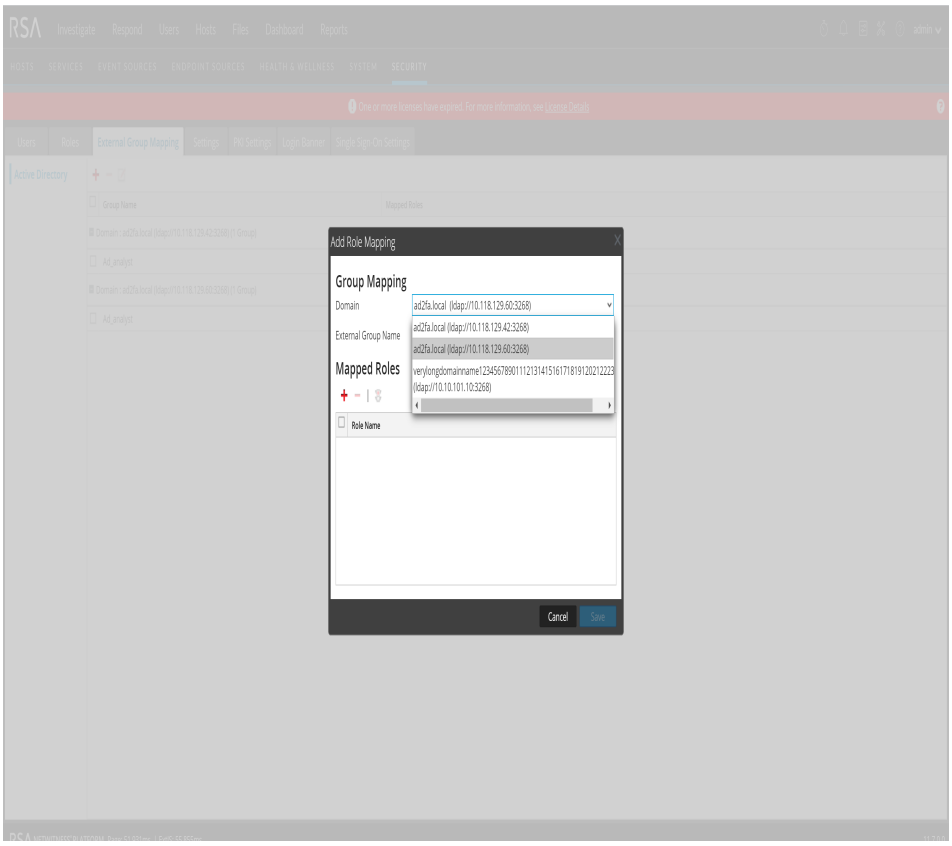
Related Topics

Verify Query and Session Attributes per Role

Role Permissions

Quick Look

To access this view, go to  **(Admin) > Security > Roles** tab and in the toolbar, click  , or select a role and click  .



The Add Role and Edit Role dialogs include three sections.

1. **Role info**
2. **Attributes**
3. **Permissions**

Role Info

This is the information in the **Role Info** section.

Feature	Description
Name	The name of the user role.
Description	An optional description of the user role.

Attributes

The following table describes the fields in the **Attributes** section..

Field	Description
Core Query Timeout	(Optional) Specifies the maximum number of minutes that a user can run a query. The default value is 5 minutes. This timeout only applies to queries performed from Investigation. If this value is set, it must be zero (0) or greater. A value of zero represents no timeout.
Core Session Threshold	Controls how the service scans meta values to determine session counts. This value must be zero (0) or greater. If this value is greater than zero, a query optimization will extrapolate the total session counts that exceed the threshold. When the meta value returned by the query reaches the threshold, the system will: • Stop its determination of the session count • Show the threshold and percentage of query time used to reach the threshold The default value is `100000`. The limit you specify here overrides the **Max Session Export** value defined in the Investigate view settings.
Core Query Prefix	(Optional) Filters query results to restrict what the role members see. By default, this is blank. For example, the `'service' = 80` query prefix prepends to any queries run by the user and the user can only access meta of HTTP sessions.

Permissions

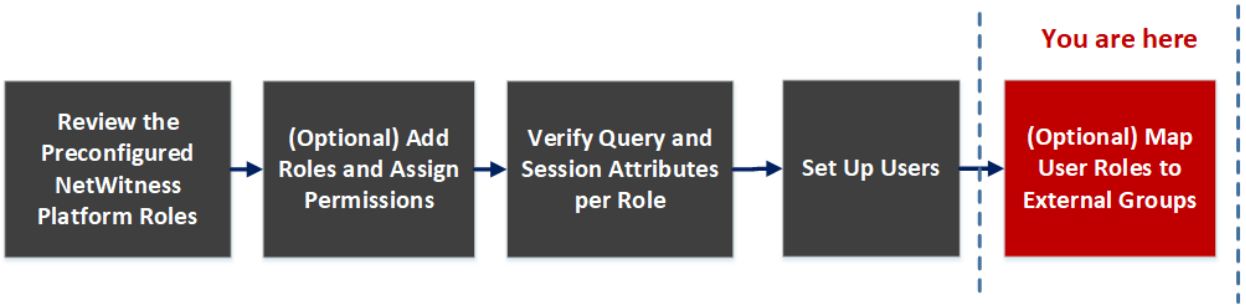
The following table describes the features in the **Permission** section.

Feature	Description
Module tabs	There are fifteen default tabs, one for each module: Administration, Admin-server, Alerting, Config-server, Incidents, Investigation, Investigation-server, Integration-server, Live, Malware, Orchestration-server, Reports, Response-server, Security-server and Dashboard. Additional tabs may be available based on the installation. Each tab lists the permissions for a module.
Assigned column	Checkbox that indicates if a module permission is assigned to the role.
Description column	List of all permissions for the module.
Save	Saves the role with the selected permissions assigned to it.
Cancel	Cancels any work and closes the dialog.

External Group Mapping Tab

If you set up external user authentication, you can map NetWitness user roles to an external group. The External Group Mapping tab provides information about each external group to which you have mapped roles.

Workflow



What do you want to do?

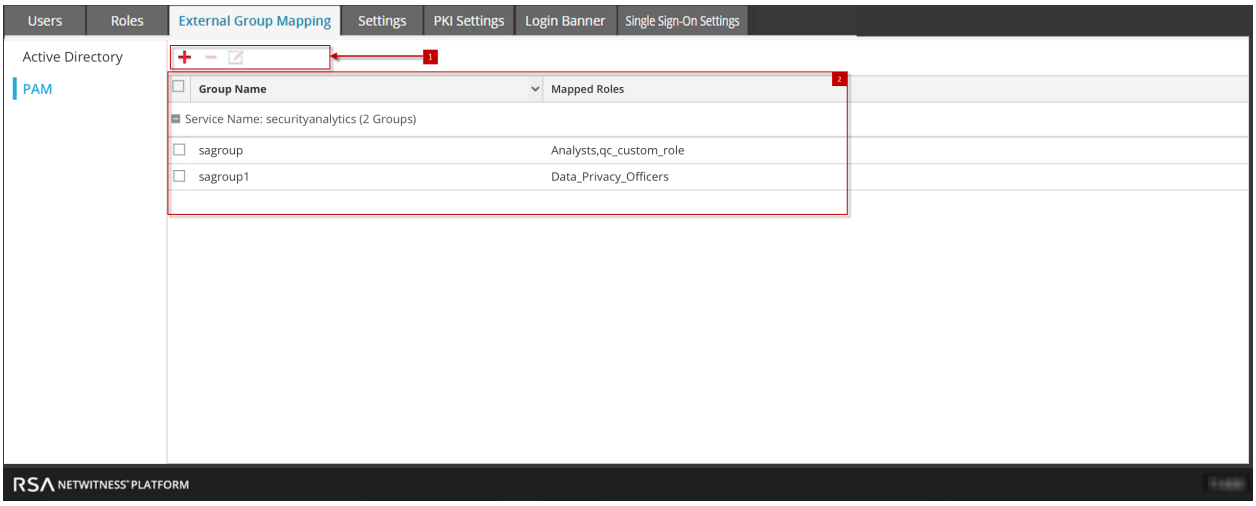
Role	I want to ...	Show me how
Admin	Map a role to an external group	(Optional) Map User Roles to External Groups
Admin	Search for an external group	Search for External Groups

Related Topics

- Add Role Mapping Dialog
- Search External Groups Dialog

Quick Look

To access this view, go to **(Admin) > Security** and click the **External Group Mapping** tab.



The External Group Mapping includes the following sections.

1 Toolbar
2 List

Toolbar

The following table describes the **External Group Mapping** toolbar.

Icon	Description
	Displays the Add Role Mapping dialog in which you can select an external group and map it to a NetWitness role.
	Displays a warning message and asks for confirmation to remove all NetWitness roles mapped to the external group.
	Displays the Edit Role Mapping dialog in which you can add or remove NetWitness roles from the external group.

List

The following table describes the **External Group Mapping** list.

Feature	Description
Group type	In the column on the left, click either **Active Directory** or **PAM** to show groups for the selected type.
Selection box	In a row, toggles selection of a group name. In the title bar, toggles selection of all group names.
Group Name	Displays the name of the external group that has access to NetWitness.
Mapped Roles	Displays the NetWitness roles mapped to the external group.

Add Role Mapping Dialog

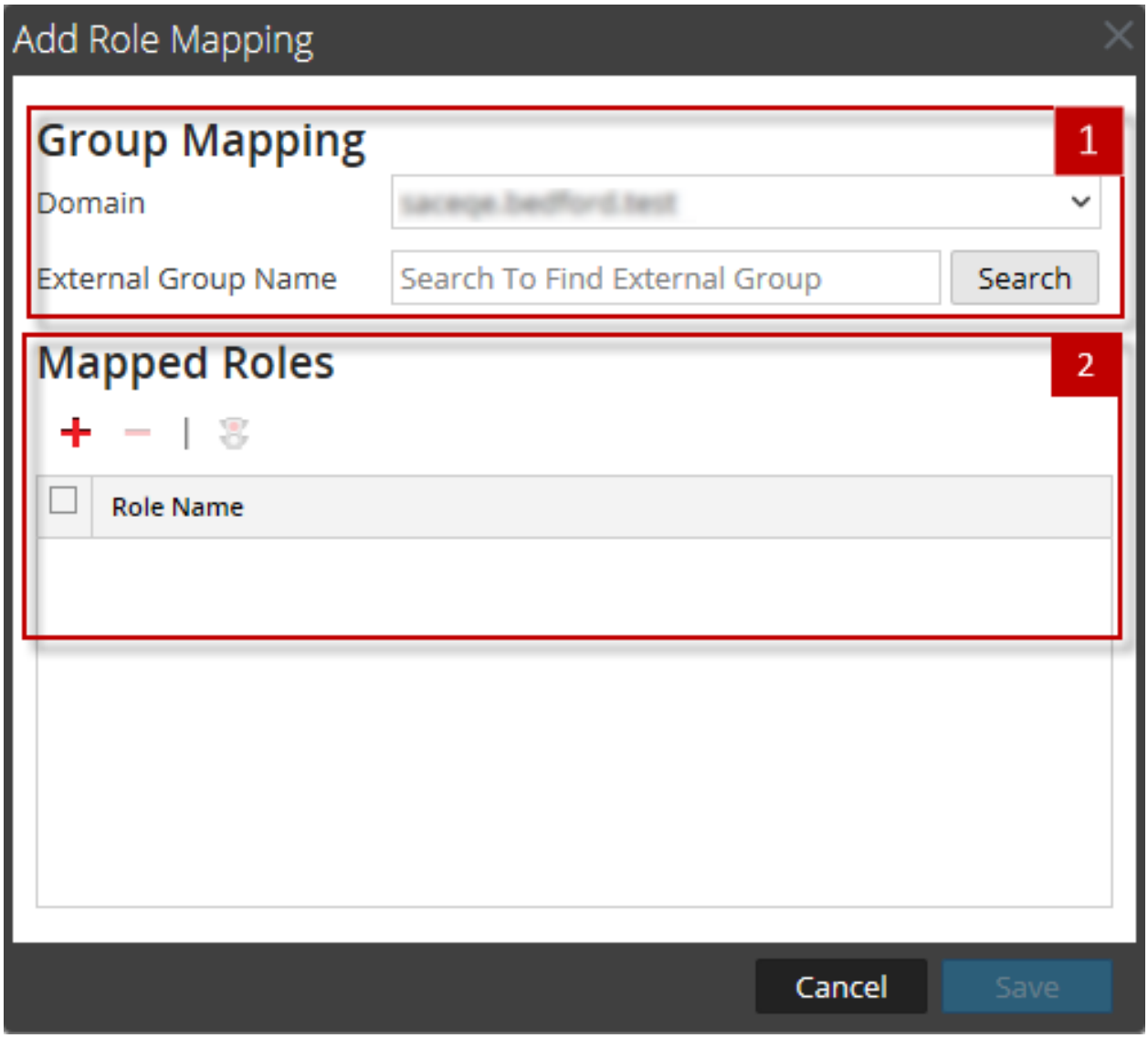
In NetWitness each user role has its own set of permissions. You can map one or more NetWitness roles to an external group, which grants the group the same set of permissions that each role has.

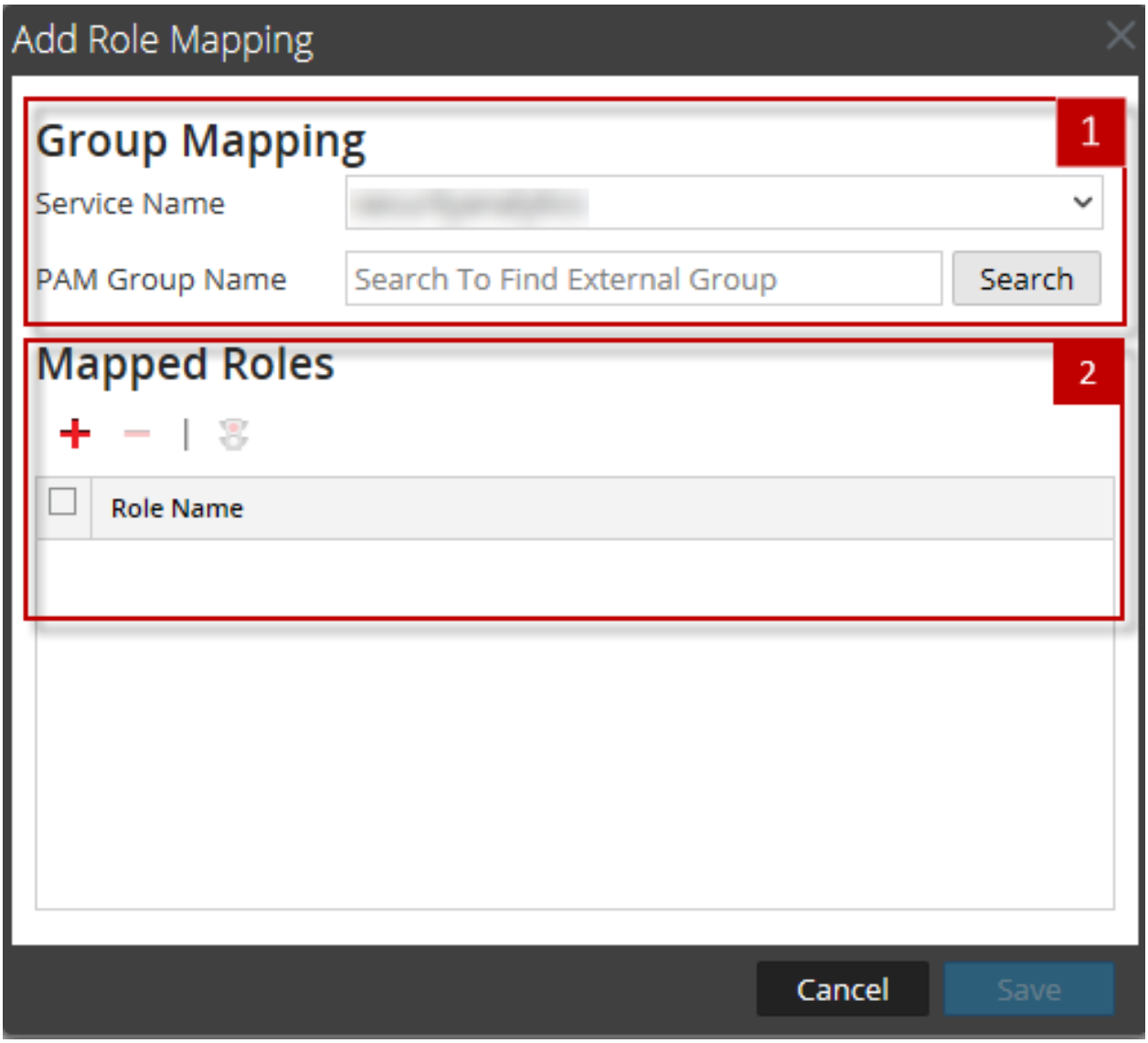
What do you want to do?

Role	I want to ...	Show me how
Admin	Map a role to an external group	(Optional) Map User Roles to External Groups
Admin	Search for an external group	Search for External Groups

Quick Look

To access this dialog, go to  **(Admin) > Security**, click the **External Group Mapping** tab, and in the toolbar, click +. The **Add Role Mapping** dialog for the external authentication method that you set up is displayed.


Add Role Mapping
Group Mapping
1
Domain
External Group Name
Search To Find External Group
Search
Mapped Roles
2
Role Name
Cancel
Save



Note: The Add Role Mapping and the Edit Role Mapping dialogs are nearly identical. The only difference is that you cannot search in the Edit Role Mapping dialog.

The **Add Role Mapping** tab includes the following sections.

1 **Group Mapping**
2 **Mapped Roles**

Group Mapping

The following table describes the **Group Mapping** section features.

Feature	Description
Domain	Displayed if you set up Active Directory for external user authentication. The domain name of the external AD group to which roles are mapped.
External Group Name	Displayed if you set up Active Directory for external user authentication. The external group to which roles are mapped.
PAM Group Name	Displayed if you configured PAM for external user authentication. The name of the external group to which roles are mapped.
Search	Displays a search dialog in which you can search for external groups using domain name and host. Search is not available in the Edit Role Mapping dialog.

Mapped Roles

The following table describes the **Mapped Roles** section features.

Feature	Description
	Opens the Add Role dialog, in which configured NetWitness user roles to add are listed.
	Removes selected roles from the Mapped Roles grid.
Name	Displays the name of the NetWitness user role.
Permissions	Displays the permissions associated with the NetWitness user role.
Cancel	Cancels the new group mapping or changed group mapping and closes the dialog.
Save	Saves the new group mapping or changed group mapping and closes the dialog.

Search External Groups Dialog

If you set up external user authentication, you can map NetWitness user roles to external groups. You search for external groups to select the groups to which you want to map NetWitness roles.

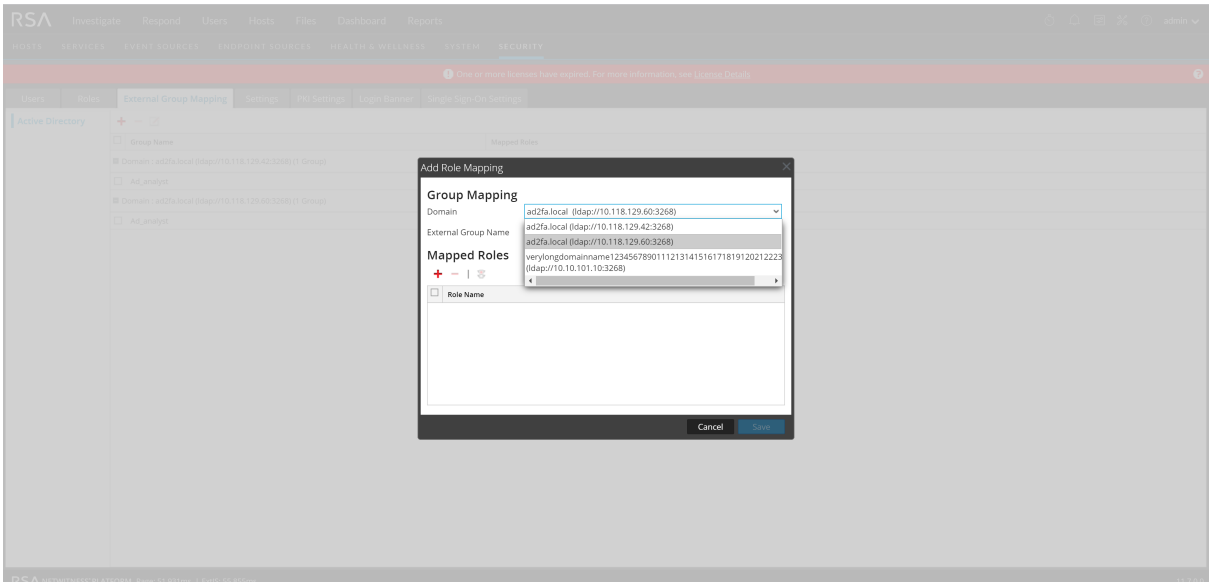
What do you want to do?

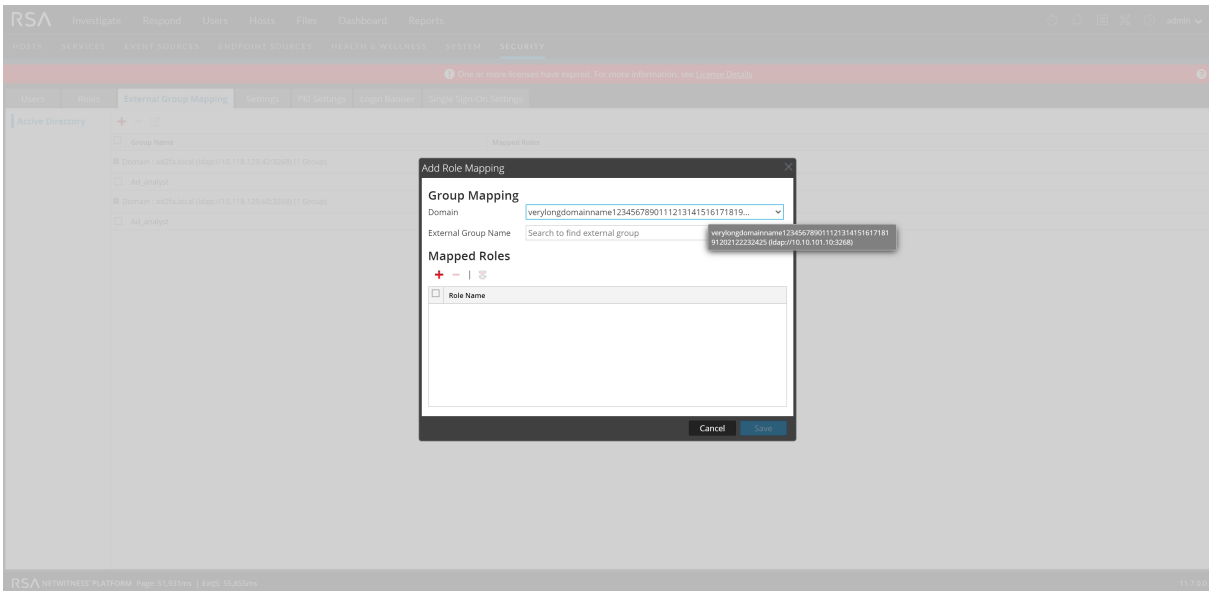
Role	I want to ...	Show me how
Admin	Map a role to an external group	(Optional) Map User Roles to External Groups
Admin	View external group mappings	External Group Mapping Tab
Admin	Search for external groups	Search for External Groups

Quick Look

To access this dialog:

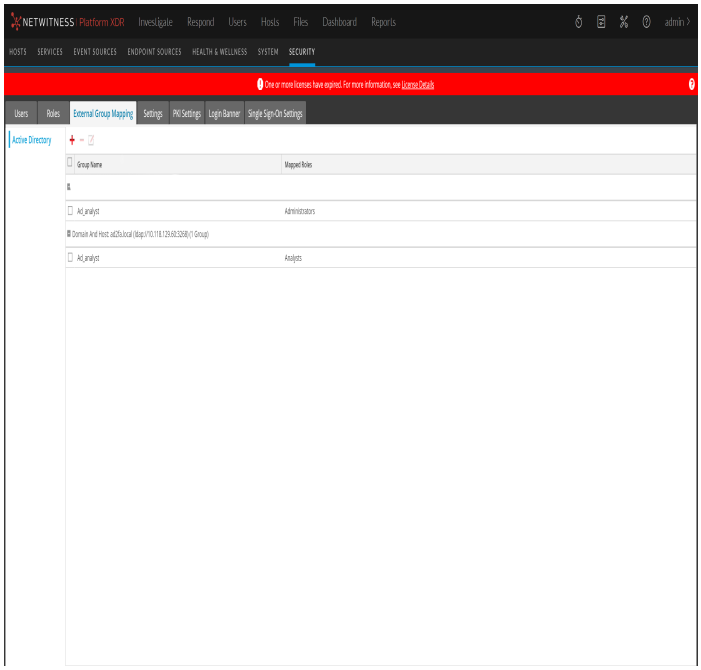
1. Go to **(Admin) > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click +.
   The Add Role Mapping dialog for the external authentication method you set up is displayed.





4. In the Group Mapping section, select a **Domain**.

5. In the Group Mapping section, click **Search** next to **External Group Name** field.
   The **Search External Groups** dialog is displayed.



The following table describes the features of the **Search External Group** dialog.

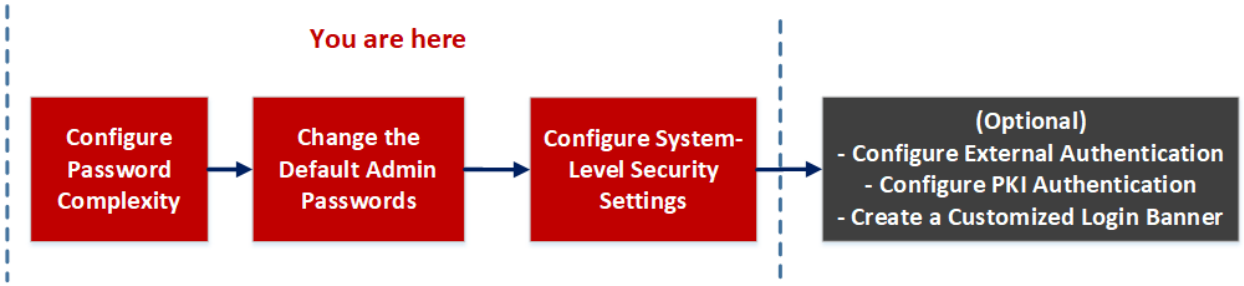
Feature	Description
Retrieve all groups or enter a search criteria	Group name for which you are searching. Can be the exact name or can contain the wild card character (*) to match any character.
Group Name	External group to which you could map roles.
Description	Optional text about the group.
OK	Displays the Add Role Mapping dialog, showing the external group you selected.
Cancel	Closes the dialog.

Settings Tab

In the Settings tab, you can configure password complexity for internal NetWitness users and set system-wide security parameters. You can also restrict access to incidents in the Respond view.

Password complexity requirements apply only to internal users and are not enforced for external users. External users rely on their own methods and systems to enforce password complexity.

Workflow



What do you want to do?

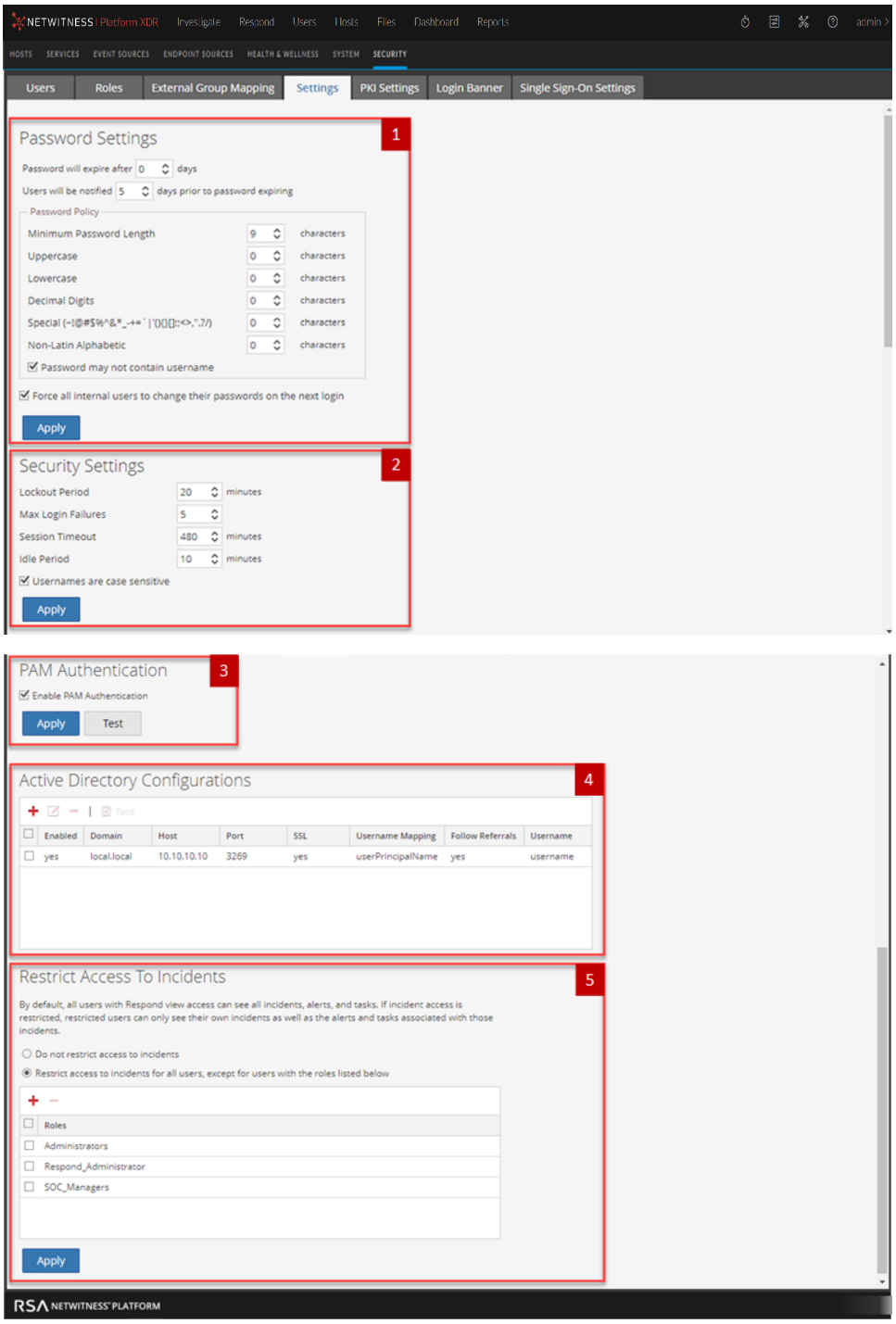
Role	I want to ...	Show me how
Admin	Configure password complexity	Configure Password Complexity
Admin	Configure system-level security settings	Configure System-Level Security Settings
Admin	Restrict access to incidents.	Configure System-Level Security Settings
Admin	(Optional) Configure external authentication	(Optional) Configure External Authentication

Related Topics

- Set Up System Security

Quick Look

To access this view, go to  **(Admin) > Security** and click the **Settings** tab.



The **Settings** tab includes the following sections.

1 **Password Settings**
2 **Security Settings**
3 **PAM Authentication**
4 **Active Directory Configurations**
5 **Restrict Access To Incidents**

Password Settings

The Password Policy section enables you to configure password complexity requirements for internal NetWitness users when they set their passwords.

Option	Description
Password will expire after <n> days	The default number of days before a password expires for all internal NetWitness users. A value of zero (0) disables password expiration. For new installations, the default value is 30. For upgrades, the previous value will migrate automatically to the upgraded installation.
Users will be notified <n> days prior to password expiring	The number of days before the password expiration date, to notify a user that their password is about to expire. Users receive a one-time email on the specified date before their passwords expire. They also see a Password Expiration Message dialog when they log on to NetWitness. The minimum value is 1 day.
Minimum Password Length	Specifies a minimum password length requirement for NetWitness user passwords. A minimum password length prevents users from using short passwords that are easy to guess.
Uppercase	Specifies a minimum number of uppercase characters for the password. This includes European language characters A through Z, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic uppercase: Д Ц • Greek uppercase: Π Λ
Lowercase	Specifies a minimum number of lowercase characters for the password. This includes European language characters a through z, sharp-s, with diacritic marks, Greek characters, and Cyrillic characters. For example: • Cyrillic lowercase: д ц • Greek lowercase: π λ
Decimal Digits	Specifies a minimum number of decimal characters (0 through 9) for the password.
Special (~!@#$%^&*_-+=`|'(){}[]:;<>,".?/)	Specifies a minimum number of special characters for the password: `~!@#$%^&*_-+=`|'(){}[]:;<>,".?/`
Non-Latin Alphabetic	Specifies a minimum number of Unicode alphabetic characters that are not uppercase or lowercase. This includes Unicode characters from Asian languages. For example: • Kanji (Japanese): 頁 (leaf) 枒 (tree)
Password May Not Contain Username	Specifies that a password cannot contain the case-insensitive username of the user.

Option	Description
Force all internal users to change their passwords on the next login	Forces all internal users to change their passwords the next time they log on to NetWitness instead of when they create or change their passwords. Note that this setting is checked by default.
Apply	Password strength settings take effect when NetWitness users create or change their passwords. If **Force all internal users to change their passwords on the next login** is selected, all internal users must change their password the next time they log on to NetWitness.

Security Settings

The Security Settings section enables you to configure global security settings for NetWitness users.

Option	Description
Lockout Period	Number of minutes to lock a user out of NetWitness after the configured number of failed logins is exceeded. The default value is 20 minutes.
Max Login Failures	The maximum number of unsuccessful login attempts before a user is locked out. The default value is 5
Session Timeout	The maximum duration of a user session before timing out in minutes. The default value is 600. If the value is 0, there is no maximum time for a session. If the value is a positive integer, the session times out when the configured time has elapsed. The user must log in again.
Idle Period	Number of minutes of inactivity before a session times out. The default value is 10. If the value is 0, the session will not timeout.
Usernames are case sensitive	Select this option if you want the Username field on the NetWitness login screen to be case sensitive. For example, if usernames are case sensitive, you could use admin to log on to NetWitness, but you could not use Admin. This is a mandatory field.
Password	Enter the password if you want to add or edit the Active Directory Security Settings. This is a mandatory field.
Apply	Makes the settings become effective immediately.

PAM Authentication

The PAM Authentication section enables you to configure NetWitness to use Active Directory or PAM to authenticate and test external user logins.

Option	Description
Enable PAM Authentication	Allows NetWitness to use Pluggable Authentication Modules (PAM) to authenticate external user logons.
Apply	Makes the PAM configuration settings become effective in the next logon.
Test	Prompts for a username and password, then tests the currently enabled PAM authentication method.

Active Directory Configurations

The Active Directory Configuration section enables you to configure NetWitness to use Active Directory to authenticate external user logins.

Option	Description
Enabled	Enables Active Directory authentication for NetWitness users.
Domain	Domain name where the Active Directory Service is located.
Host	Host name or IP address where the Active Directory Service is located.
Port	Port on the host that is used for Active Directory Service authentication.
SSL	Indicates whether the Active Directory Service uses Secure Sockets Layer (SSL). To enable SSL so that your Active Directory Service can communicate with NetWitness version 11.1 and later, you must upload an Active Directory server certificate.
Username Mapping	Indicates the Active Directory search field to use for username mapping. You can specify userPrincipalName (UPN) or sAMAccountName.
Follow Referrals	Indicates whether NetWitness will follow LDAP referrals made by Active Directory.
Username	Username of the user that binds to the Active Directory Service while searching Active Directory groups. This is usually a service account that has permissions to query the domain and validate user accounts and group membership. This credential is not used for any other purpose.
Password	Password of the user that binds to the Active Directory Service while searching Active Directory groups. This is usually a service account that has permissions to query the domain and validate user accounts and group membership. This credential is not used for any other purpose.

Restrict Access to Incidents

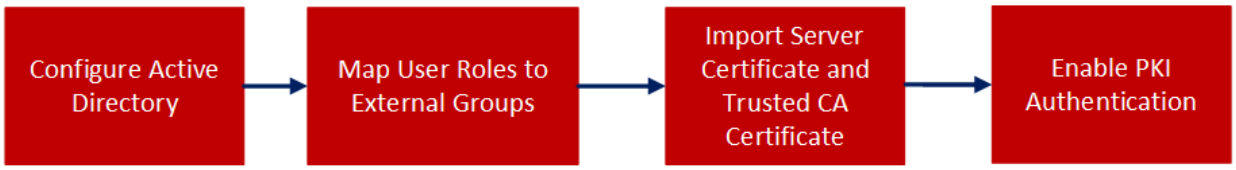
By default, analysts can view all of the incidents, alerts, and tasks in the Respond view. If you have sensitive or restricted information that should not be shared, you can restrict what analysts and other users can see in the Respond view.

Option	Description
Do not restrict access to incidents	Enables analysts to view all of the incidents, alerts, and tasks in the Respond view. This is the default setting.
Restrict access to incidents for all users, except for users with the roles listed below	Restricts what analysts and other users can see in the Respond view. Analysts can only see incidents assigned to them as well as the alerts and tasks associated with those incidents.
(List of user roles whose access to incidents is not restricted.)	When you select to restrict access to incidents, this list shows the user roles that do not have restricted access to incidents. You can adjust this list of user roles independently from your restriction selection. For example, you can add and adjust the list of non-restricted user roles before you make the selection to restrict access to incidents.
Apply	Changes take effect on the next log in to NetWitness Platform.

PKI Settings Tab

The Public Key Infrastructure (PKI) Settings tab enables you to configure PKI authentication for NetWitness.

Workflow

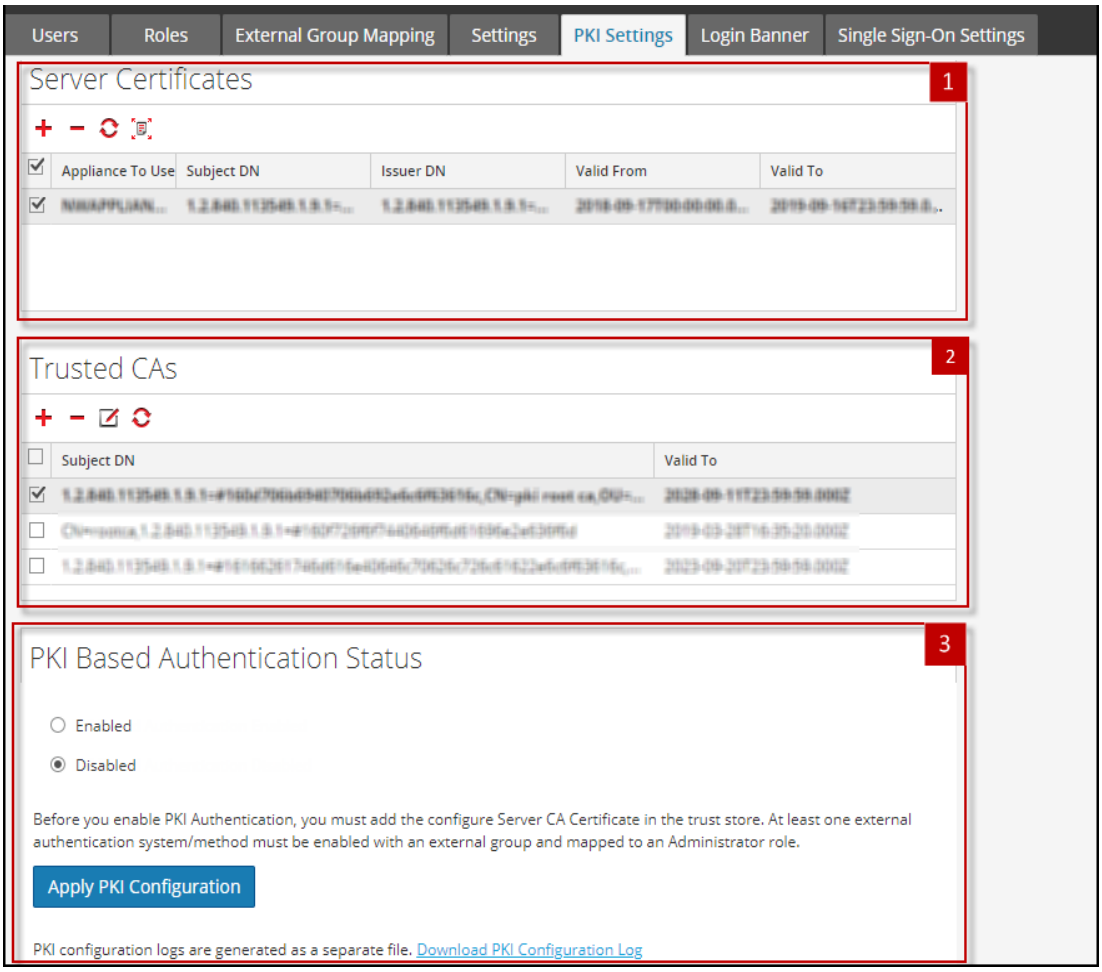


What do you want to do?

Role	I want to ...	Show me how
Admin	Configure External Authentication	Configure Active Directory
Admin	Map user Roles to External Groups	(Optional) Map User Roles to External Groups
Admin	Import Server Certificate	Import Server Certificate and Trusted CA Certificate
Admin	Enable PKI Authentication	Enable PKI Authentication

Quick Look

To access this view, go to  **(Admin) > Security** and click the **PKI Settings** tab.



The **PKI Settings** tab includes the following sections.

1 **Server Certificates**
2 **Trusted CAs**
3 **PKI Based Authentication Status**

Server Certificates

The **Server Certificates** section enables you to import a server certificate with its private key to NetWitness Server. The following table lists the **Server Certificates** features and their description.

Feature	Description
Appliance to Use	The device to use the certificate
Subject DN	The entity to which the certificate is issued.
Issuer DN	The entity which issued the certificate.
Valid From	The start date for the certificate validity.
Valid To	The end date till when a certificate is valid.

Trusted CAs

The **Trusted CAs** section enables you to import a Certificate Authority (CA) certificate to NetWitness. The following table lists the **Trusted CAs** features and their description.

Feature	Description
Subject DN	The entity to which the certificate is issued.
CA	Indicates whether the certificate is Certificate Authority (CA).
Valid To	The end date till when a certificate is valid.

PKI Based Authentication Status

The **PKI Based Authentication Status** section enables you to enable PKI authentication in NetWitness. The following table list the **PKI Based Authentication Status** features and their description.

Feature	Description
Enabled	Select the option to enable PKI.
Disabled	Select the option to disable PKI.
Apply PKI Configuration	Enables PKI authentication for NetWitness users.

Login Banner Tab

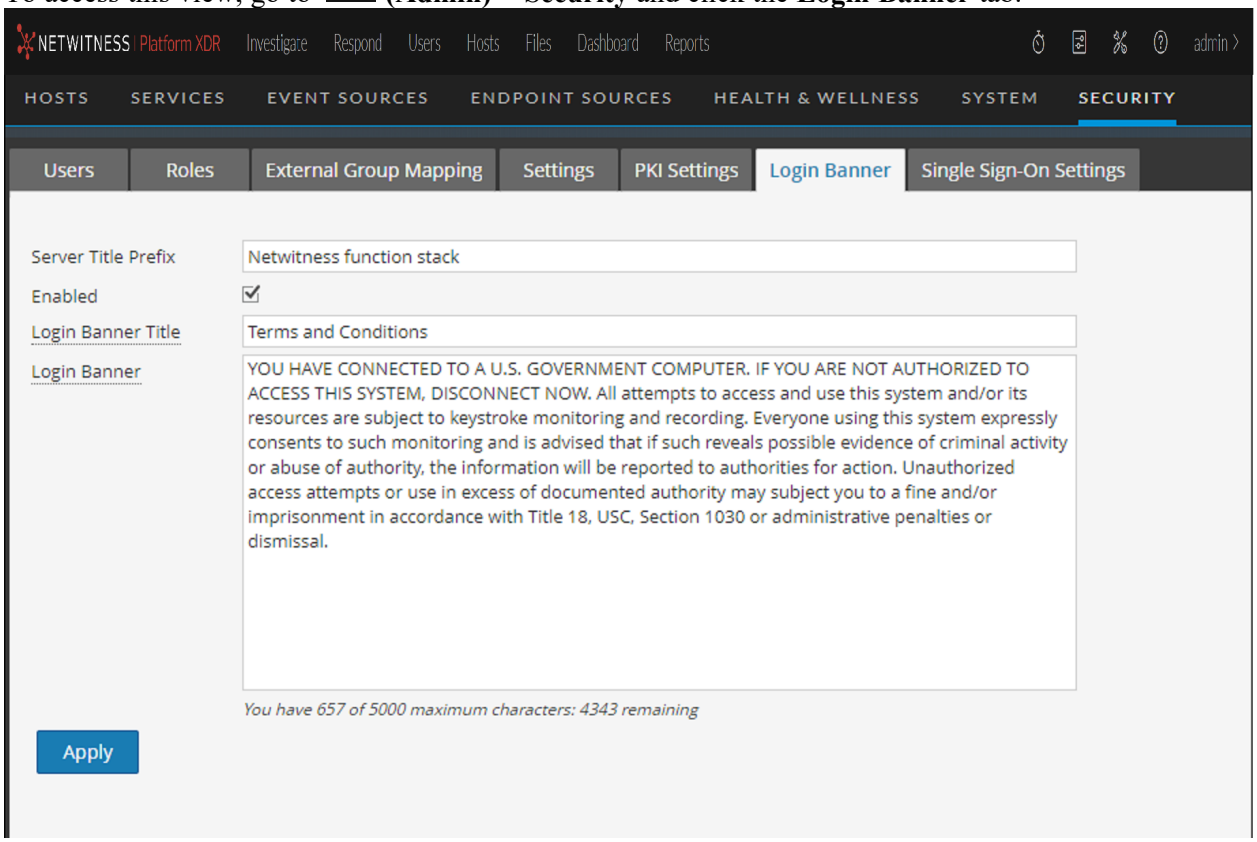
The Login Banner tab provides a way to add a banner to the NetWitness login screen, which will prevent a user from logging on until they agree to the conditions. Add the server title prefix to differentiate the NetWitness Server of the current tab, when you have multiple deployed in your system. You can customize the default title and text of the login banner. The banner is disabled by default.

What do you want to do?

Role	I want to ...	Show me how
Admin	Create or enable a login banner	(Optional) Create a Customized Login Banner

Quick Look

To access this view, go to **(Admin) > Security** and click the **Login Banner** tab.



The following table lists the features of the Login Banner tab.

Feature	Description
Server Title Prefix	Displays the prefix of the NetWitness Server on the title bar.
Enabled	Checkbox that indicates whether or not the login banner is enabled. This box is cleared by default.
Login Banner Title	Shows the title of the dialog box that contains the login conditions.
Login Banner	Shows the conditions the user must acknowledge.

Single Sign-On Settings Tab

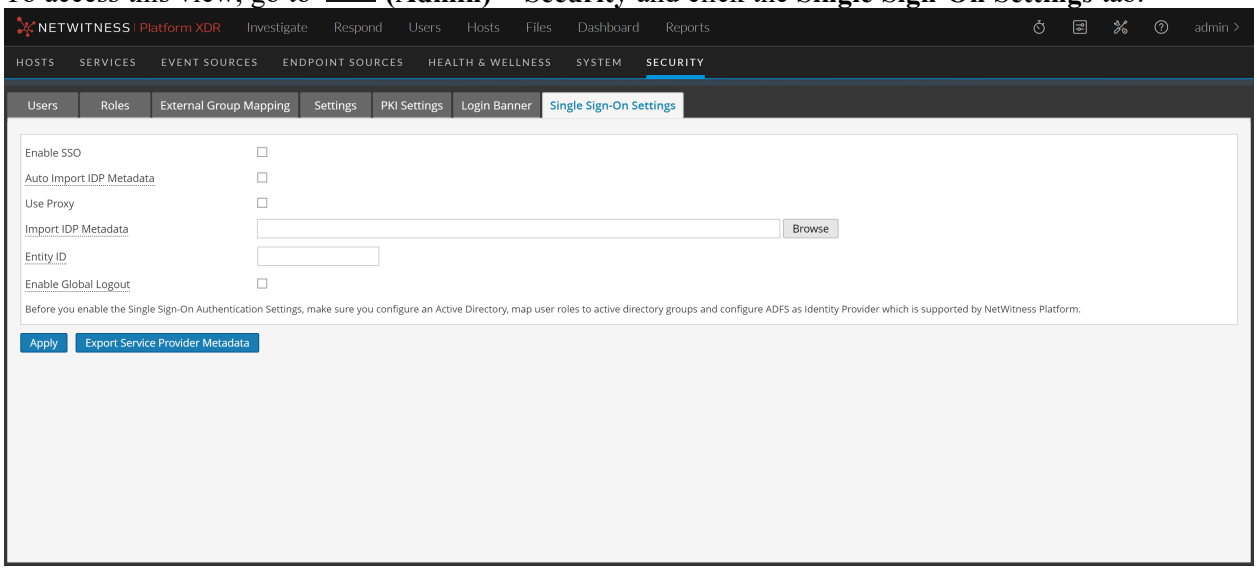
The SSO Settings tab provides a way to enable SSO.

What do you want to do?

Role	I want to ...	Show me how
Admin	Enable SSO Settings	Configure Single Sign-On
Admin	Configure Active Directory	Configure Active Directory
Admin	Configure ADFS as IDP for NetWitness	For instructions on how to configure ADFS as IDP for NetWitness, see the *Configure SAML 2.0 provider settings for portals* topic in Microsoft documentation.
Admin	Map User Roles to External Groups	Manage Users with Roles and Permissions

Quick Look

To access this view, go to **(Admin) > Security** and click the **Single Sign-On Settings** tab.



The following table lists the features of the Single Sign-On tab.

Feature	Description
Enable SSO	Checkbox that indicates whether or not the single sign-on is enabled. This box is cleared by default.

Feature	Description
Auto Import IDP Metadata	If selected the latest IDP metadata is downloaded at regular intervals.
Metadata URL	Enter the metadata URL generated when the connection was established with the ADFS.
Use Proxy	If enabled, the requests to IDP will be routed through the proxy configured in  (Admin) > System > HTTP Proxy settings.
Import IDP Metadata	Enter the metadata URL generated when the connection was established with the ADFS. **Note:** Make sure you update the link every time the IDP metadata is updated.
Entity ID	A unique identifier for NetWitness unique amongst all the applications managed by the same IDP.
Enable Global Logout	Checkbox that enables Global Logout setting for users. When Global Logout is enabled, the user is logged out of NetWitness and also from other applications authenticated by ADFS.
Apply	The admin-server is restarted after which you will get notified in the notification tray when the metadata is ready to be downloaded.
Export Service Provider Metadata	Exports an XML file which is uploaded to IDP to establish the connection between NetWitness (SP) and IDP (ADFS) for authentication.