RSA NETWITNESS® SUITE

System Security and User Management Guide

for Version 11.1

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

September 2019

Contents

System Security and User Management

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

Topics

Set Up System Security

This topic introduces a set of end-to-end procedures for implementing system security. Each step in the following topics explains a system-wide setting. Follow the steps in order to set up security in NetWitness Suite.

Topics

Step 1. Configure Password Complexity

This topic provides instructions to set system-wide NetWitness Suite password complexity requirements.

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 Suite software allows you to configure the password complexity requirements for internal NetWitness Suite 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 Suite.

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 Suite users. When you configure the password strength settings, they apply to internal NetWitness Suite users, including the admin user.

You can choose to enforce any combination of the following password strength requirements when a NetWitness Suite 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

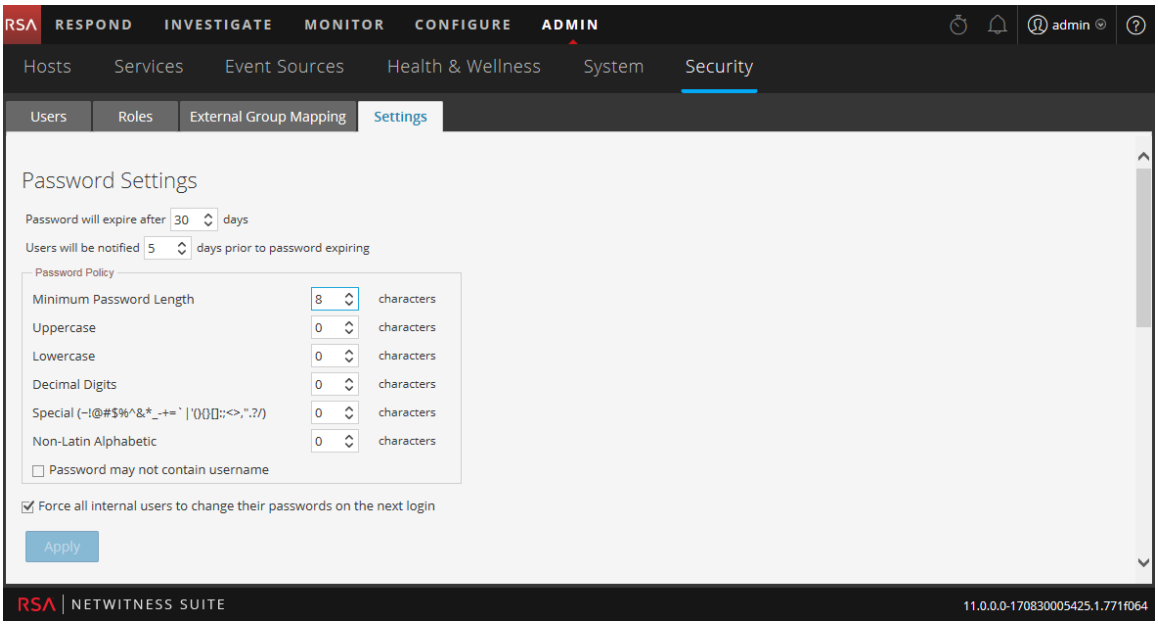
For example, you can create a strong password requirement that has a minimum of 8 characters, cannot contain the username of the user, and contains a mix of uppercase and lowercase letters, numbers, and special characters.

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.

The topic "STIG Compliant Passwords" in the *System Maintenance Guide* provides an example of a strong password policy.

Configure Password Strength

1. In NetWitness Suite, 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 Suite 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 4 characters.

Requirement	Description
Password will expire after <n> days	The default number of days before a password expires for all internal NetWitness Suite 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 Suite. The minimum value is 1 day.
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 4 characters required by default.
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 (~!@#$%^&*_-+=`|'(){}[]:;<>,".?/)	Specifies a minimum number of special characters for the password: ~!@#$%^&*_-+=`|'(){}[]:;<>,".?/

Requirement	Description
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 checked 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 Suite.

Step 2. Change the Default Admin Passwords

This topic provides instructions for changing the admin password for the NetWitness Suite service and for the Core services.

The system administrator's user account is installed with NetWitness Suite. The username is **admin** and the default password is the password that was entered in the Text-based User Interface (TUI) during the NetWitness Suite 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 Suite 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 Suite 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 Suite and on each Core service. For security, you create the Users and Roles for your organization in NetWitness Suite, and on each Core service.

Best Practices

RSA 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 Suite

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

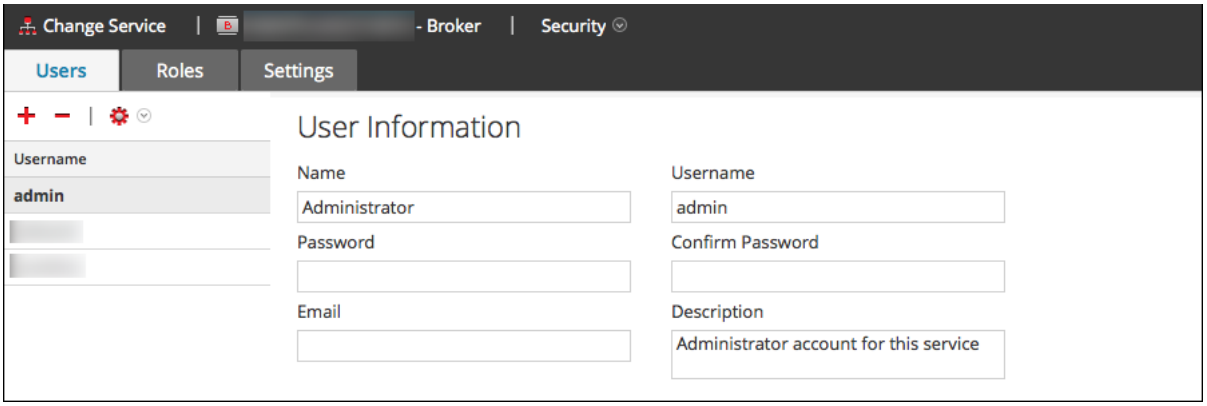
Note: After you change the admin password, you must remove and re-add a Data Source on the Reporting Engine. For more information, see the **Remove and re-add a Data Source on the Reporting Engine** section below.

Change the admin Password for Core Services

To change the admin password for a Core service:

1. In NetWitness Suite, 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:

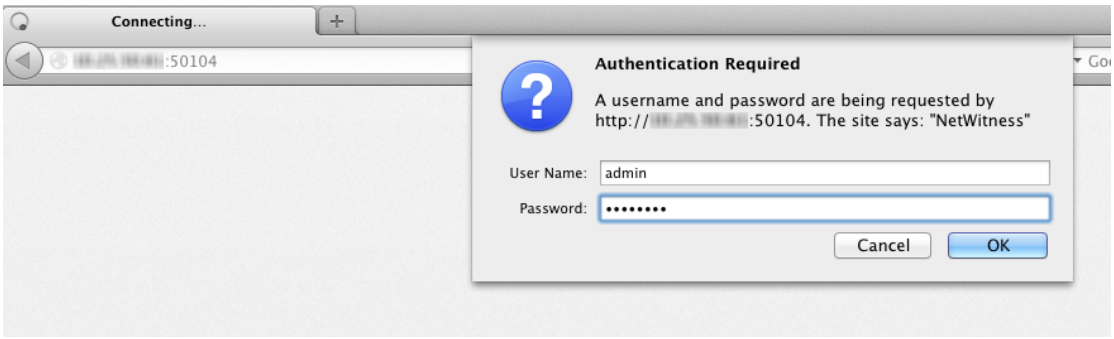
1. In NetWitness Suite, go to **ADMIN > Services**.
2. In the Services view, select Reporting Engine and **View > Config**.
3. Click the **Sources** tab.
4. Select a service to remove and click
5. Click and select **Available Services.**
6. Select the service you removed in step 4 and click **OK**.
7.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

Change the admin Password for a Service Using the REST API

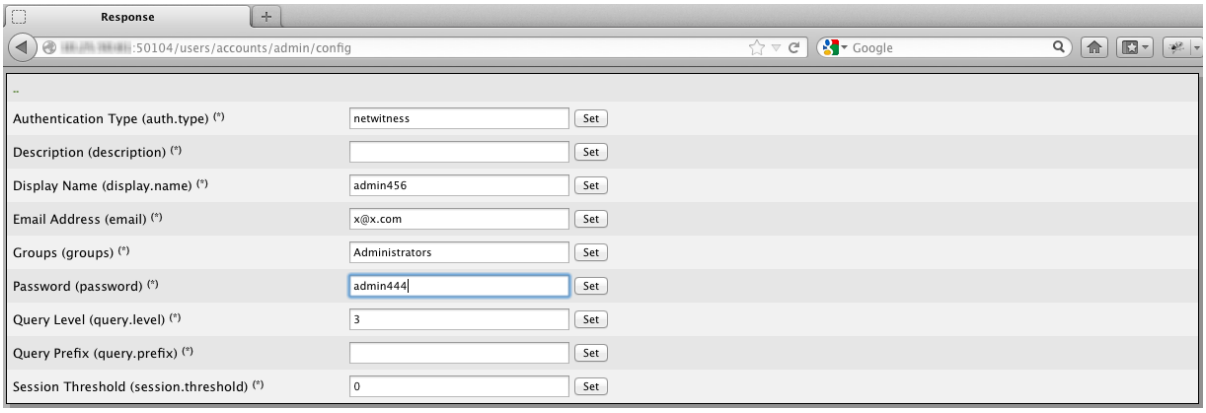
In rare circumstances, you may need to change the admin password for a Core service outside of the NetWitness Suite user interface. This is simply another way to perform the Core service password change, and is not the preferred method.

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 Suite 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**.

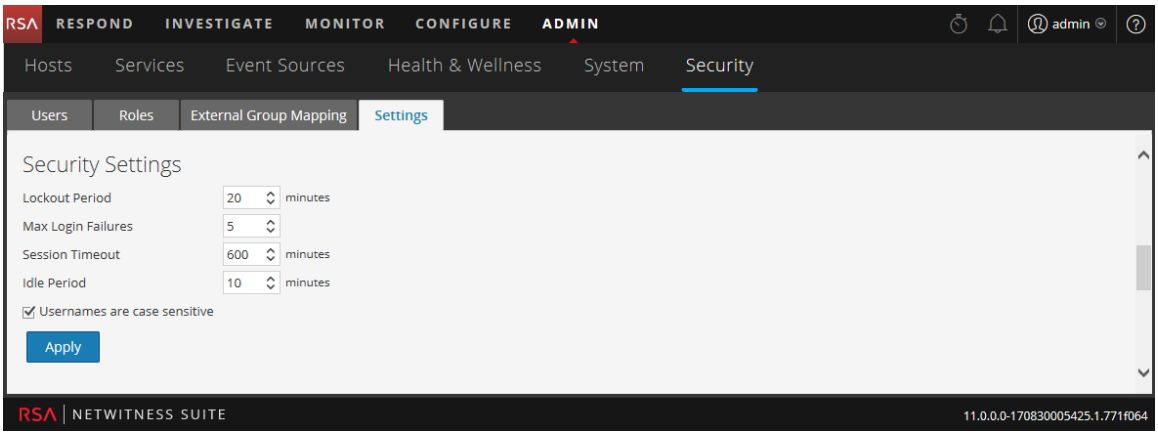
Step 3. Configure System-Level Security Settings

This topic explains how to set system-wide security parameters.

Most global security settings, such as the maximum number of failed login attempts to allow, apply to all NetWitness Suite 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 Suite users, but not external users.

Configure Security Settings

1. In NetWitness Suite, 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 Suite 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.

Field	Description
Session Timeout	The maximum duration of a user session before timing out in minutes. The default value is 600. 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 Suite 11.0 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.
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 Suite 11.0 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 Suite login screen to be case sensitive. For example, if usernames are case sensitive, you could use admin to log on to NetWitness Suite, 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 Suite.

Step 4. (Optional) Configure External Authentication

This topic introduces the external authentication methods that NetWitness Suite supports.

When a user logs in, NetWitness Suite 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 Suite user account to log on to NetWitness Suite and receive role-based permissions.

NetWitness Suite supports two methods of external authentication, Active Directory and Pluggable Authentication Modules (PAM). Topics in this section describe how to configure and test each method.

Topics

- Configure Active Directory
- Configure PAM Login Capability

Configure Active Directory

This topic explains how to configure NetWitness Suite to use Active Directory to authenticate external user logins.

When a user logs in, NetWitness Suite 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 Suite. NetWitness Suite 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.

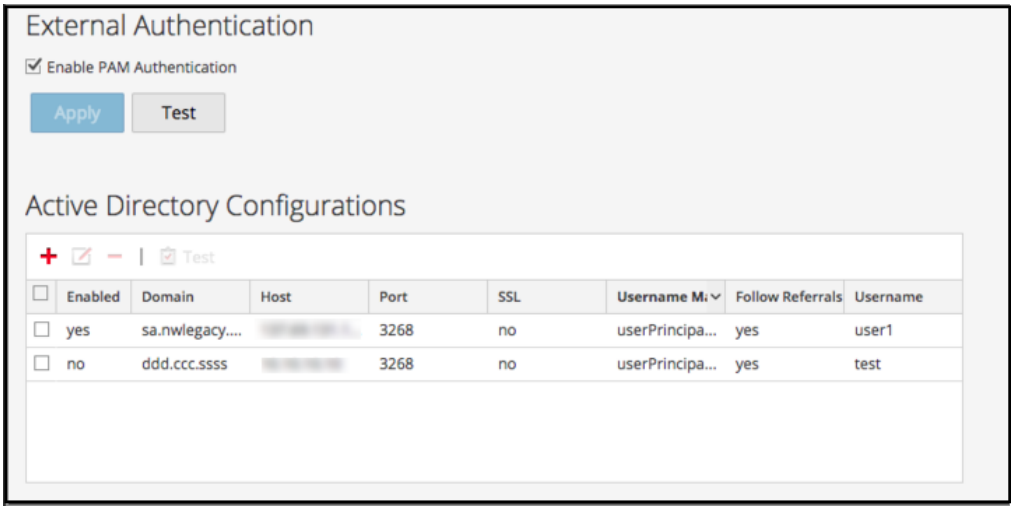
Note: The Settings tab also provides the option to enable PAM configuration, which can be used simultaneously with Active Directory configurations. For information on enabling and configuring PAM authentication, see Configure PAM Login Capability.

Procedures

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.



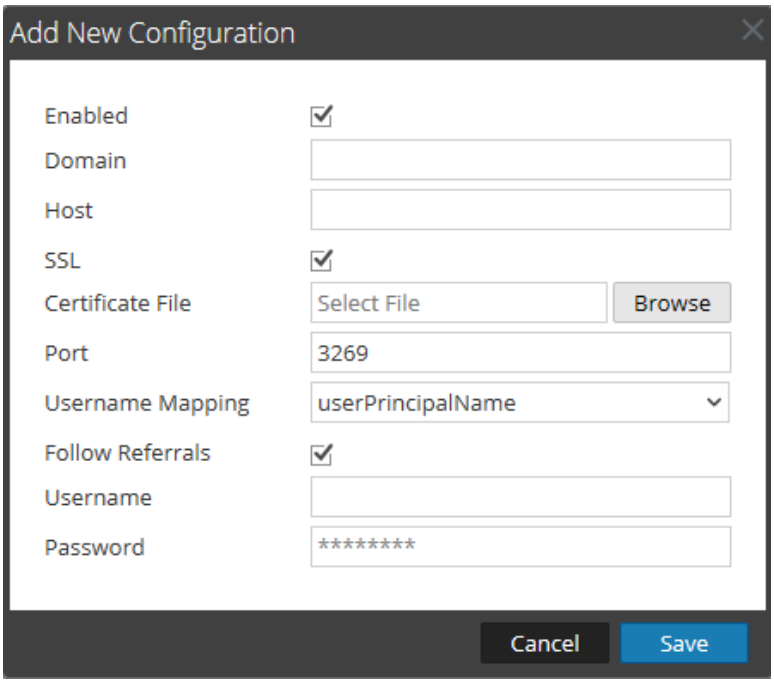
3. Add, edit, or delete domains as necessary, as described in the following sections.
   The domains added to this list are automatically populated in the External Group Mapping tab so that you can map security roles to each group.

Note: To configure security roles used for Active Directory access, see Step 5. (Optional) Map User Roles to External Groups.

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. Click the **Enabled** checkbox.
3. Enter **Domain**, **Host** and **Port** information for the Active Directory Service.
4. (Optional) To select SSL for this configuration, check 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 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.

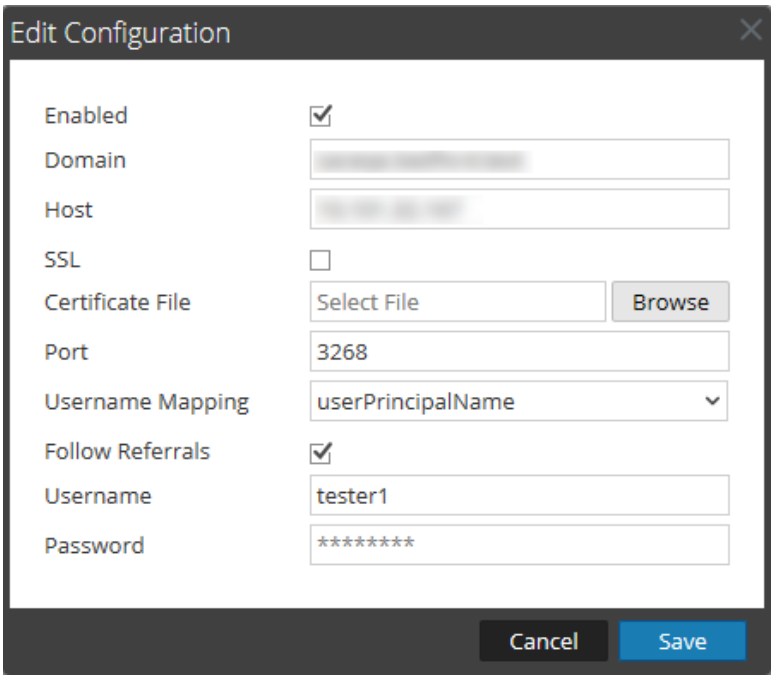
8. Click **Save**.
   The new configuration is listed in the Active Directory Configurations list.

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, check 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, click the **Follow Referrals** checkbox.
   a. If you want to disable LDAP forwarding, uncheck the box.
   b. If you want to enable LDAP forwarding, check the box.
6. In the **Username** and **Password** fields, enter the username and password for a bind user to access Active Directory. This 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 Suite 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

This topic explains how to configure NetWitness Suite to use Pluggable Authentication Modules (PAM) to authenticate external user logins.

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 Suite without having an internal NetWitness Suite account, and to receive permissions or roles determined by mapping the external group to a NetWitness Suite 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 PAM 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 Suite uses the OS-provided PAM library, and the module that the PAM library is configured to use, to authenticate users.

Note: The 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 Suite 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 Suite compares the results of the request to the NetWitness Suite External Group Mapping and if a matching group is found, the user is granted access to log on to NW 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 Suite. 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 RSA SecurID. The NSS examples include 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.

Prerequisites

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 Suite, identify the group names that you will use in the External Group mapping. When mapping roles, the role in NetWitness Suite 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, proceed to the next section, *Configure and Test the NSS 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 RSA 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. Execute 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

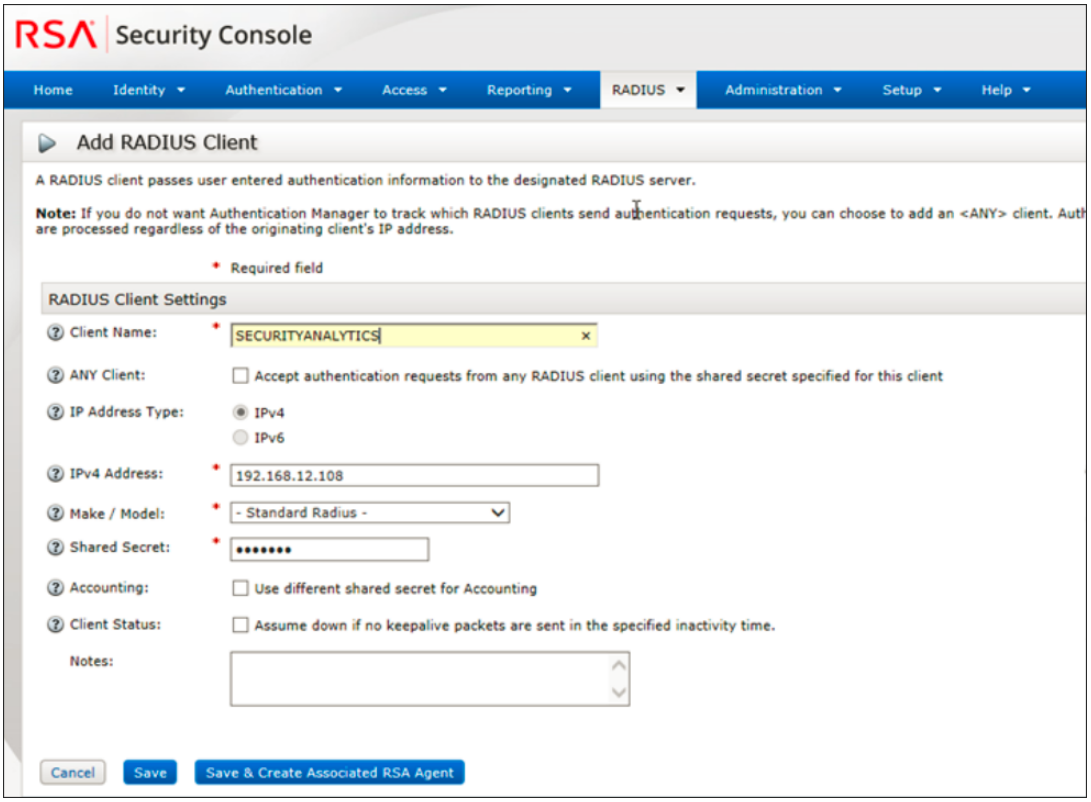
Note: The examples in these tasks use RSA Authentication Manager as the RADIUS server. You must use administrative account credentials to log on RSA Authentication Manager Security Console.

To add a RADIUS Client and Associated Agent:

1. Log on to RSA 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:

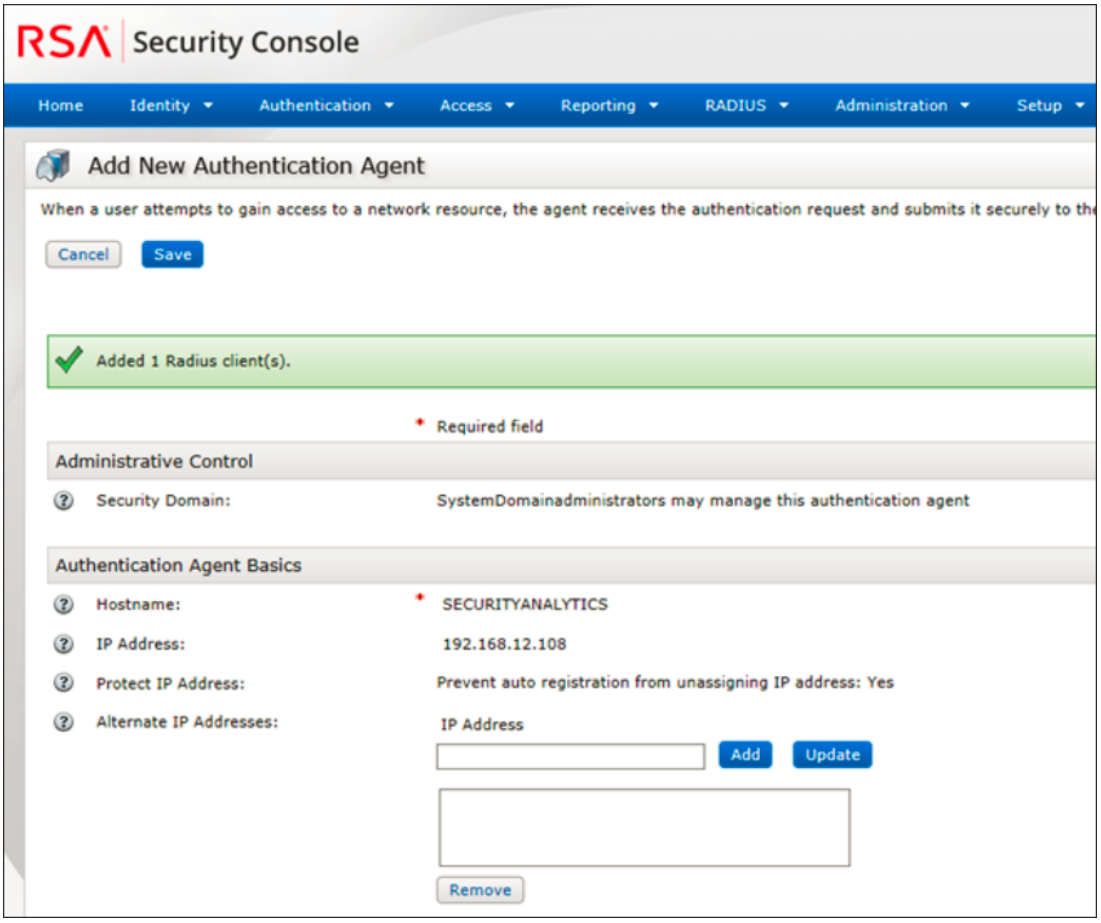
   a. In the **Client Name** field, enter the name of the client, for example, NetWitness Suite.

   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 RSA Agent.



5. Click **Save**.

If 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 Add a RADIUS Client topic in *RSA Authentication Manager 8.2 Administrator's Guide*.

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

PAM Agent for SecurID

PAM Communication Port - UDP 5500

Prerequisites

The RSA SecurID PAM module is supported only under the following conditions:

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

Process Overview

The high-level steps to configure the SecurID PAM module are:

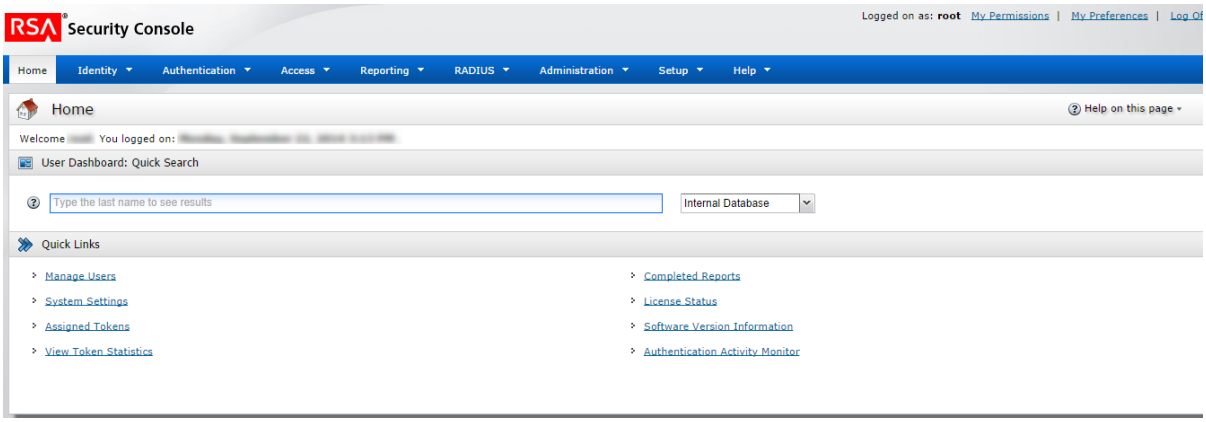
1. Configure **Authentication Manager**:
   a. Add Authentication Agent.
   b. Download configuration file.
2. Configure **NetWitness Server**:
   a. Copy configuration file from Authentication Manager and customize it.
   b. Install the PAM SecurID Module.
3. Test connectivity and authentication.

Then follow the remaining procedures in the sections that follow:

- Configure NSS.
- Enable PAM in NetWitness Server.
- Configure group mappings in NetWitness Server.

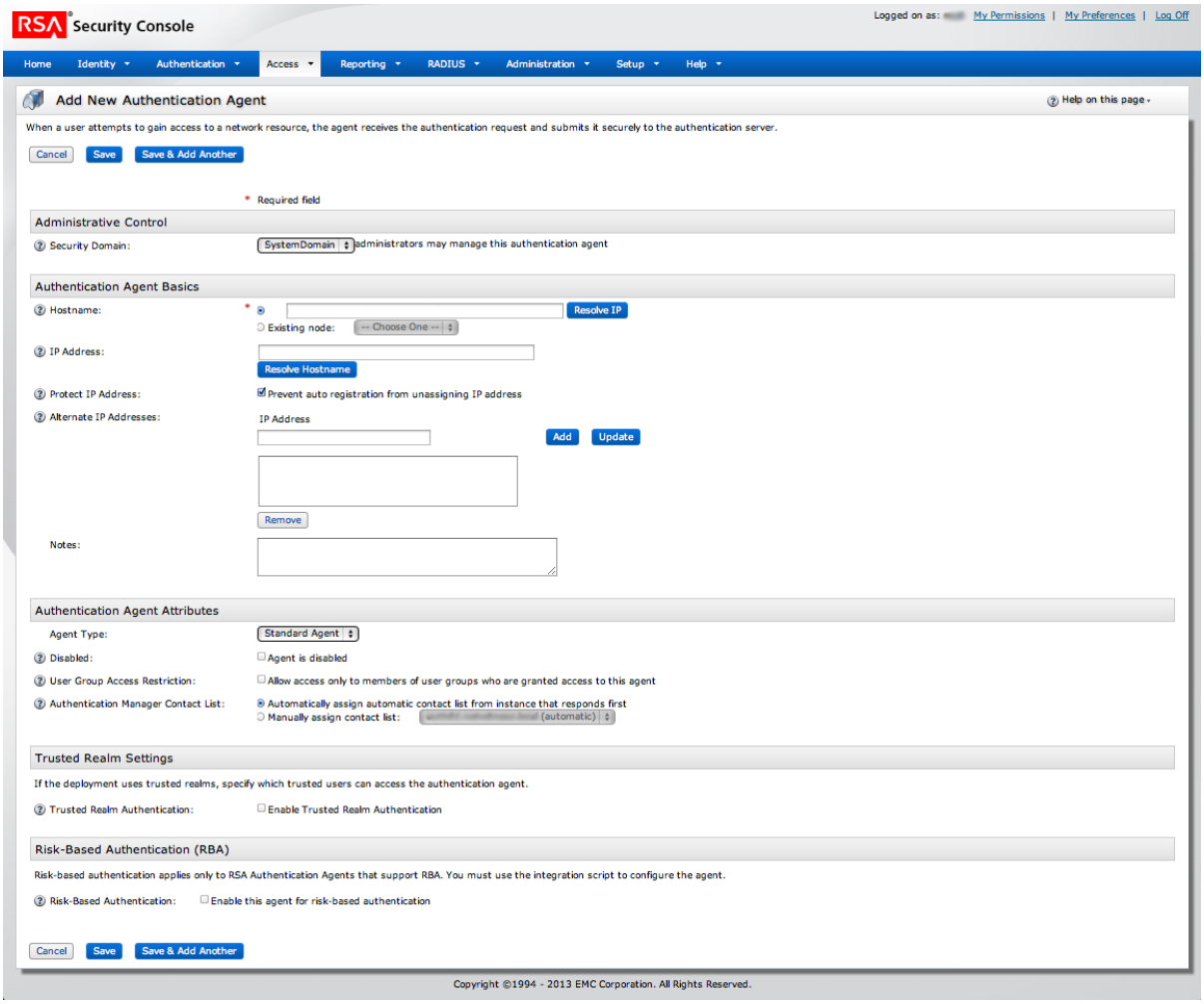
To configure Authentication Manager:

1. Log on to RSA Authentication Manager.
   The Security Console is displayed.

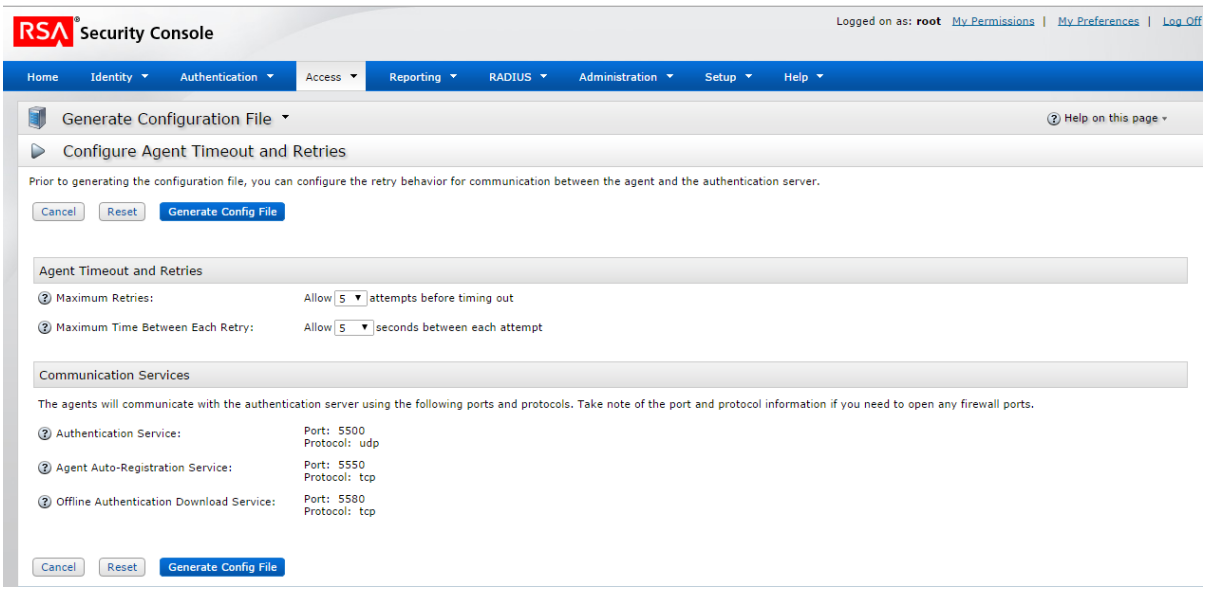


2. In the Security Console, add a new authentication agent.
   Click **Access > Authentication Agents > Add New.**

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 a directory:
   `mkdir /var/ace`
2. On the NetWitness Server, copy `sdconf.rec` from the .zip file to `/var/ace`.
3. Create a 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 Service.

Note: If the PAM SecurID setup is not complete, it may crash the Jetty server and the NetWitness Suite 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`, enter **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`. Output 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, proceed to the next section, *Configure and Test the NSS Service*.

Configure and Test the NSS Service

NSS UNIX

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: Note that this does NOT permit or allow access to the NW Server console.

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
```

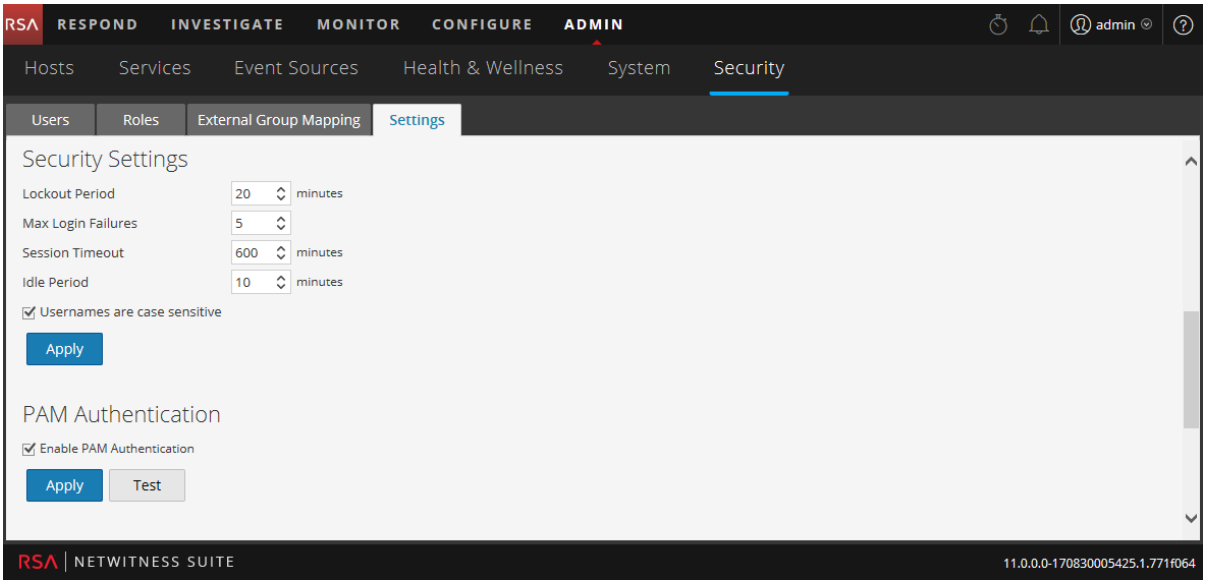
```
[root@~]# getent group mygroup
 mygroup:*:10000:myuser3
```

- 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 Suite 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 Suite has not picked up the change. A reboot of the NetWitness Suite host will cause NetWitness Suite to pick up NSS configuration changes. A restart of the Jetty server is not sufficient.

Proceed to the next section, Enable PAM in NetWitness Server.

Enable PAM in NetWitness Server

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Admin > 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**.

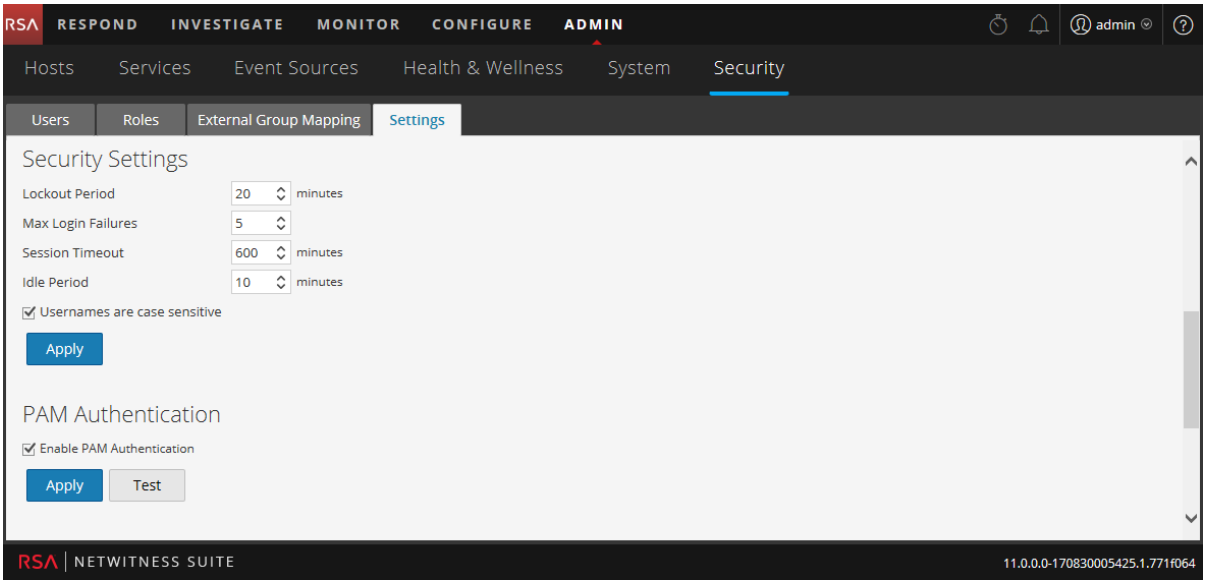


Test PAM Authentication

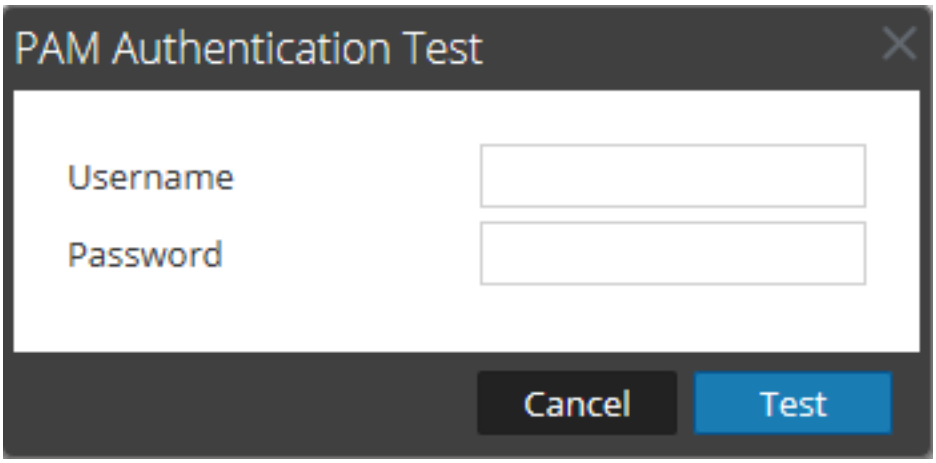
To test external authentication for PAM:

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. To configure security roles used for PAM access, see Step 5. (Optional) Map User Roles to External Groups.

How Role-Based Access Control Works

This topic explains role-based access control (RBAC) when there is a trusted connection between NetWitness Server and a Core service.

In the RSA NetWitness® Suite, 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.

Pre-Configured Roles

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

The following table lists each pre-configured 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.
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.
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.
Respond_ Administrator	Access to all Respond permissions.
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
Malware_ Analysts	Access to investigations and malware events. The only access granted to the Malware Analysts persona is the Malware Analysis module.
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 *Data Privacy Management*). 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.

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 Suite 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 Suite logon and are authenticated by the server.
- Users, already authenticated by the server, access every Core service in ADMIN > Services without entering a password.

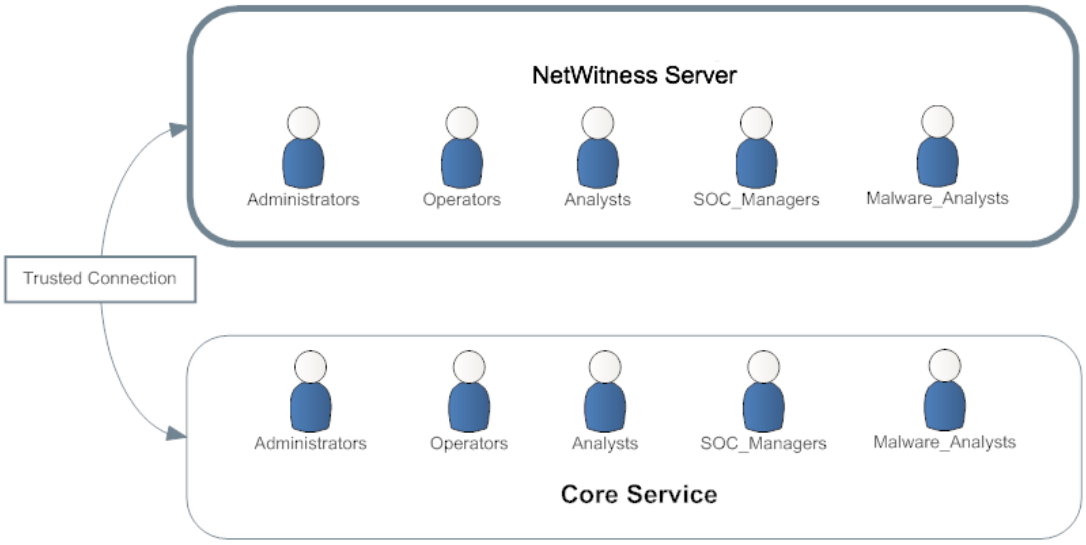
How Trusted Connections Are Established

When you install or upgrade to 11.0, trusted connections are established by default with two settings:

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

Common Role Names on the Server and Services

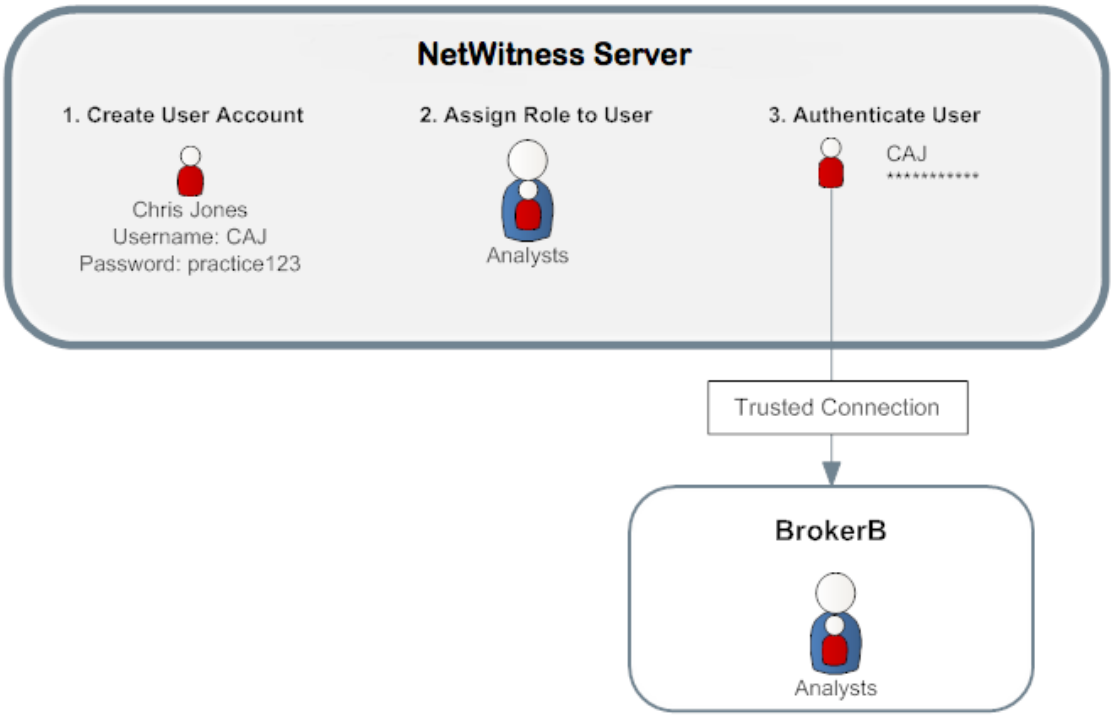
Trusted connections rely on common role names on the server and service. On a fresh installation, NetWitness Suite installs the five pre-configured roles on the server and each Core service.



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 pre-configured or custom role to Chris Jones:
   - **Pre-Configured 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.

Related Topic

- Role Permissions

Role Permissions

This topic describes access to the user interface that users assigned to the built-in NetWitness Suite roles have by default.

Within NetWitness Suite, user access to each module, dashlet, and view is restricted based on the assigned permissions described in this topic. 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 the NetWitness Suite 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 Suite user role:

- Administrators
- Operators
- Analysts
- Respond Administrator
- SOC Managers (SOC Mgrs)
- Malware Analysts (MAs)
- Data Privacy Officers (DPOs)

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 Suite 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.

Administration

The following table lists the permissions in the Administration tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
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				
Manage Auditing	Yes				Yes
Manage Email	Yes				
Manage Global Auditing	Yes				Yes
Manage Health & Wellness Policy	Yes				
Manage LLS	Yes				
Manage Logs	Yes				Yes
Manage Notifications	Yes				
Manage Plugins	Yes				

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Manage Predicates	Yes				
Manage Reconstruction	Yes				
Manage Security	Yes				Yes
Manage Services	Yes				Yes
Manage System Settings	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

Admin-server

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

Permission	Description
admin-server.configuration.manage	Permission to modify all service configuration parameters

Permission	Description
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

Alerting

The following table lists the permissions in the Alerting tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

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

Cloud-gateway-server

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

Permission	Description
cloud-gateway-server.configuration.manage	Permission to modify all service cloud gateway parameters

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

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

Permission	Description
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

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

Permission	Description
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
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. The Administrator role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
contexthub-server.*					Yes
contexthub-server.configuration.manage					
contexthub-server.connection.manage					
contexthub-server.connection.read		Yes	Yes	Yes	

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
contexthub-server.connectiontypes.read			Yes		
contexthub-server.datasource.manage		Yes	Yes	Yes	
contexthub-server.datasource.read		Yes	Yes	Yes	
contexthub-server.health.read					
contexthub-server.listentries.manage		Yes	Yes	Yes	
contexthub-server.logs.manage					
contexthub-server.metrics.read					
contexthub-server.process.manage					
contexthub-server.query.read		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	

Dashboard

The following table lists the permissions in the Dashboard tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Dashlet Access - Admin Device List Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Admin Device Monitor Dashlet					Yes
Dashlet Access - Admin News Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Alert Variance Dashlet		Yes	Yes		Yes
Dashlet Access - Alerting Recent Alerts Dashlet		Yes	Yes		Yes
Dashlet Access - Investigation Jobs Dashlet		Yes	Yes		Yes
Dashlet Access - Investigation Top Values Dashlet		Yes	Yes		Yes
Dashlet Access - Live Featured Resources Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Live New Resources Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Live Subscriptions Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Live Updated Resources Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Malware Jobs Dashlet		Yes	Yes		Yes

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Dashlet Access - Reporting Recent Report Dashlet		Yes	Yes		Yes
Dashlet Access - Reporting Charts Dashlet		Yes	Yes		Yes
Dashlet Access - Top Alerts Dashlet		Yes	Yes		Yes
Dashlet Access - Unified RSA First Watch Dashlet	Yes	Yes	Yes		Yes
Dashlet Access - Unified Shortcuts Dashlet	Yes	Yes	Yes		Yes

Endpoint-server

The following table describes the permissions in the Endpoint-server tab. The Administrators role has all of the permissions by default.

Permission	Description
endpoint-server*	All permissions (everything below)
endpoint-server.agent.manage	Permission to download and manage agent packager configuration
endpoint-server.agent.read	Permission to view the agent packager configuration
endpoint-server.ca.manage	Permission to generate and download the agent packager
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.dataretention.manage	Permission to configure the data retention policy

Permission	Description
endpoint-server.dataretention.read	Permission to view the data retention policy
endpoint-server.filter.manage	Permission to delete filters
endpoint-server.filter.read	Permission to view filters
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.machine.manage	Permission to delete hosts
endpoint-server.machine.read	Permission to view hosts
endpoint-server.metrics.read	Permission to view any metrics that the service exposes
endpoint-server.policy.manage	Permission to update and save schedule scan configuration
endpoint-server.policy.read	Permission to view existing schedule scan configuration
endpoint-server.process.manage	Permission to start and stop the service
endpoint-server.scan.manage	Permission to perform endpoint scan
endpoint-server.scan.read	Permission to view endpoint scan data
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

The following table lists the permissions in the Endpoint-server tab assigned to each role. The Administrator role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
endpoint-server*	Yes				
endpoint-server.agent.manage					
endpoint-server.agent.read					
endpoint-server.ca.manage					
endpoint-server.ca.read					
endpoint-server.configuration.manage					
endpoint-server.dataretention.manage					
endpoint-server.dataretention.read					
endpoint-server.filter.manage		Yes			
endpoint-server.filter.read		Yes			
endpoint-server.health.read					
endpoint-server.logs.manage					
endpoint-server.machine.manage		Yes			
endpoint-server.machine.read		Yes			
endpoint-server.metrics.read					
endpoint-server.policy.manage	Yes				
endpoint-server.policy.read	Yes				
endpoint-server.process.manage					
endpoint-server.scan.manage		Yes			

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
endpoint-server.scan.read		Yes			
endpoint-server.security.manage					
endpoint-server.security.read					

Esa-analytics-server

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

Permission	Description
esa-analytics-server.*	All permissions (everything below)
esa-analytics-server.analytics.manage	Permission to modify ESA analytics
esa-analytics-server.analytics.read	Permission to view ESA analytics
esa-analytics-server.configuration.manage	Permission to modify all service configuration parameters
esa-analytics-server.health.read	Permission to view any health notifications that the service exposes
esa-analytics-server.logs.manage	Permission to change log-related configuration
esa-analytics-server.metrics.read	Permission to view any metrics that the service exposes
esa-analytics-server.model.manage	Permission to modify ESA models
esa-analytics-server.model.read	Permission to view ESA models
esa-analytics-server.process.manage	Permission to start and stop the service

Permission	Description
esa-analytics-server.security.manage	Permission to modify security-related resources
esa-analytics-server.security.read	Permission to view security-related resources

Incidents

The following table lists the permissions in the Incidents tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Incident Module		Yes	Yes	Yes	Yes
Configure Incident Management Integration			Yes		Yes
Delete Alerts and incidents					Yes
Manage Alert Handling Rules			Yes		Yes
View and Manage Incidents		Yes	Yes	Yes	Yes

Integration-server

(The Integration-server permissions are available in NetWitness Suite 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

Permission	Description
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. The Administrator role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
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		
integration-server.notification.read	Yes		Yes		
integration-server.notification.send	Yes		Yes		
integration-server.process.manage					
integration-server.security.manage					
integration-server.security.read					
integration-server.template.manage	Yes		Yes		
integration-server.template.read	Yes		Yes		

Investigate

The following table lists the permissions in the Investigate tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Investigation Module		Yes	Yes	Yes	Yes

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

Investigate-server

The following table describes the permissions in the Investigate-server tab. The Administrators, Analysts, SOC Managers, Malware Analysts, and Data Privacy Officers roles have all of the permissions and are the only roles granted permissions by default.

Permission	Description
investigate-server.*	All permissions (everything below) for the Event Analysis view
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.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.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.logs.manage	Permission to change log-related configuration

Permission	Description
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.process.manage	Permission to start and stop the service
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

Live

The following table lists the permissions in the Live tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
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

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
View Live Resource Details	Yes	Yes	Yes		Yes

Malware

The following table lists the permissions in the Malware tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

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

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
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

Permission	Description
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 lists the permissions in the Reports tab assigned to each role. The Administrators role has all of the permissions by default and is not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
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
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

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
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
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

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
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.

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
respond-server.alert.read	Permission to view alerts
respond-server.alertrule.manage	Permission to create, update, or delete alert aggregation rules
respond-server.alertrule.read	Permission to view alert aggregation rules

Permission	Description
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
respond-server.incident.read	Permission to view incidents
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 Suite version 11.1 and later.) Permission to configure Respond 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 Suite version 11.1 and later.) Permission to view Respond notification settings.
respond-server.process.manage	Permission to start and stop the service

Permission	Description
respond-server.remediation.manage	Permission to create, update, or delete remediation tasks
respond-server.remediation.read	Permission to view remediation tasks
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. The Administrators and Respond Administrator roles have all of the permissions by default and are not listed.

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
respond-server.*					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	

Permission	Operators	Analysts	SOC Mgrs	MAs	DPOs
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					
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.security.manage					
respond-server.security.read					

Respond Notification Settings Permissions

(The Respond notification setting permissions are available in NetWitness Suite version 11.1 and later.)

Note: If you are updating from NetWitness Suite version 11.0 to 11.1, you will need to add additional permissions to your existing built-in NetWitness Suite user roles. For all upgrades to 11.1, 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 Respond Notification Settings (CONFIGURE > Respond 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

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 Suite local accounts
security-server.account.read	Permission to view NetWitness Suite local accounts
security-server.ca.manage	Permission to manage NetWitness Suite deployment PKI parameters (for example, sign certificates, and so on)
security-server.ca.read	Permission to view NetWitness Suite deployment PKI parameters
security-server.configuration.manage	Permission to modify all service 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

Permission	Description
security-server.permission.manage	Permission to create or remove NetWitness Suite permissions
security-server.process.manage	Permission to start and stop the service
security-server.role.manage	Permission to create, modify, or remove NetWitness Suite roles (for example, add role permissions)
security-server.role.read	Permission to view NetWitness Suite 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.user.manage	Permission to view, create, modify, or remove NetWitness Suite user profiles
security-server.user.read	Permission to view NetWitness Suite user profile details (for example, roles, login times, and so on)

Manage Users with Roles and Permissions

This topic introduces a set of end-to-end procedures for managing users in NetWitness Suite. These steps explain how to add a user in NetWitness Suite and then how to control what the user can do.

Topics

Step 1. Review the Pre-Configured NetWitness Roles

To simplify the process of creating roles and assigning permissions, there are pre-configured roles in NetWitness Suite.

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to meta and session content
Analysts	Access to meta and session content but not to configurations
Respond_ Administrator	Access to all Respond server and Incidents permissions
SOC_ Managers	Same access as Analysts plus additional permission to handle incidents
Malware_ Analysts	Access to malware events and to meta and session content
Data_Privacy_ Officers	Access to meta and session content as well as configuration options that manage obfuscation and viewing of sensitive data within the system (see Data Privacy Management).

The administrator can also add custom roles.

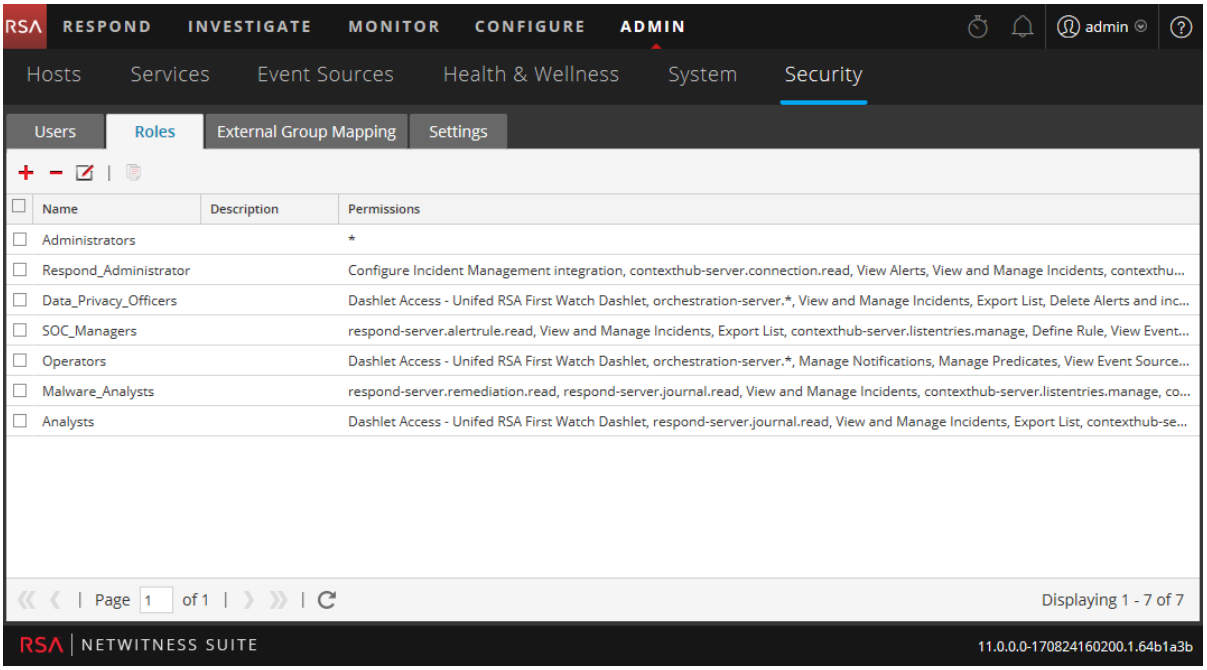
Step 2. (Optional) Add a Role and Assign Permissions

Although NetWitness Suite has pre-configured roles, you can add custom roles. For example, in addition to the pre-configured 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.

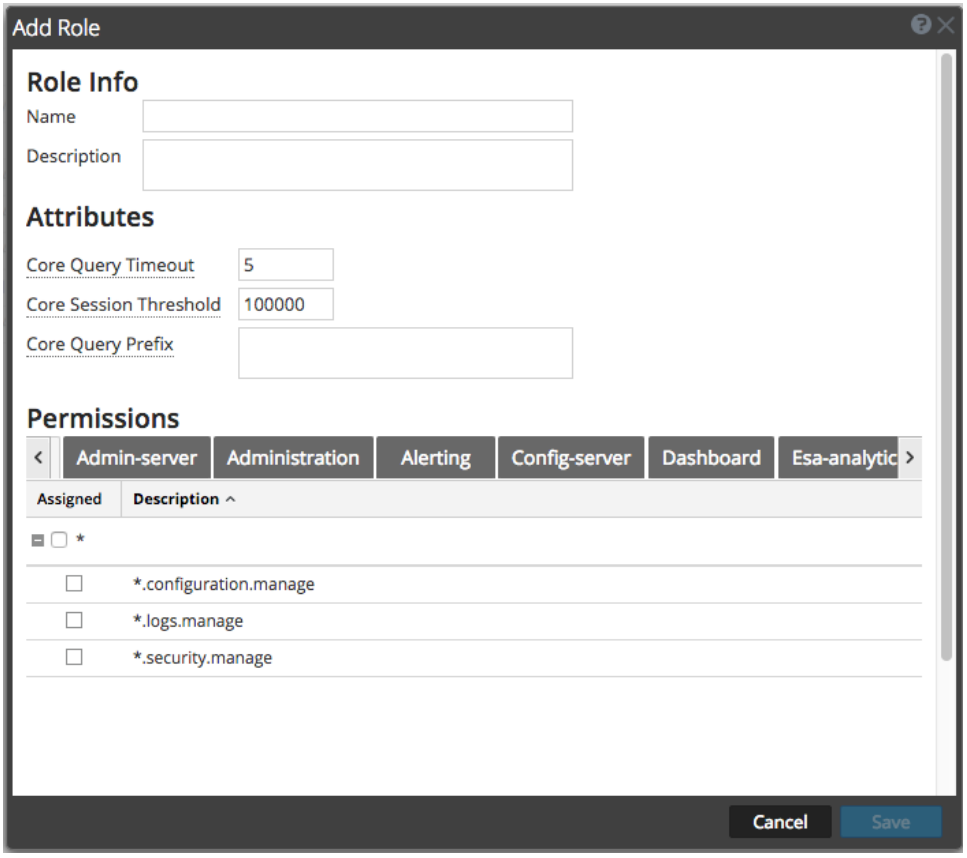
To navigate to the Roles tab:

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 Step 3. 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.

5. Repeat the previous step until you select all permissions to assign to the role.
6. Click **Save** to add the new role, which is effective immediately. You can now assign the new role to users.

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.

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

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**.

Step 3. Verify Query and Session Attributes per Role

This topic explains the query and session attributes and provides instructions for setting these attributes for user roles. This topic also describes how these role settings impact individual user settings and what happens if a user is a member of multiple roles.

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.

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. These 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 Suite 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.

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.

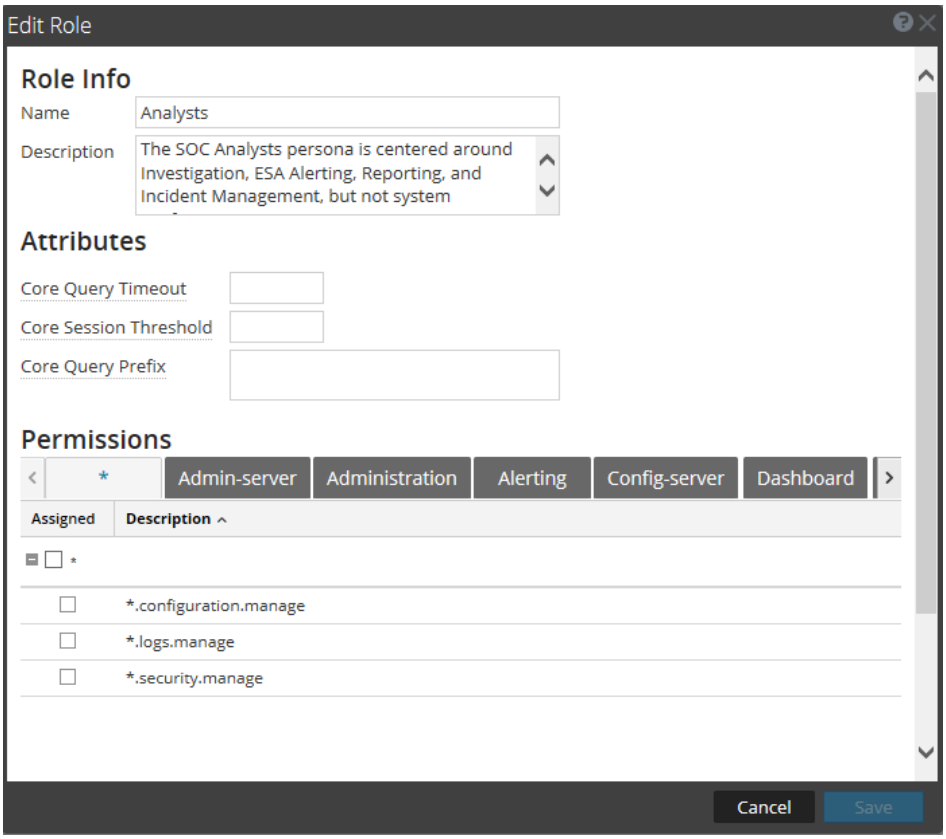
How Query-Handling Attribute Settings Apply to Individual Users

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.
4. Click **Save.**

Step 4. Set Up a User

This topic introduces procedures to set up a new user.

Topics

Add a User and Assign a Role

This topic explains how to add a new user to each type of user account, local and external. It also explains how to assign a role to a local user.

All NetWitness Suite users must have a local or external user account.

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

Local User Account	External User Account
Managed within NetWitness Suite	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, as explained in this topic	Derives permissions from each role mapped to the account's external user group, as explained in Step 5. (Optional) Map User Roles to External Groups.
NetWitness Suite manages all user information.	NetWitness Suite manages user identification only. This includes Username, Full Name and Email.

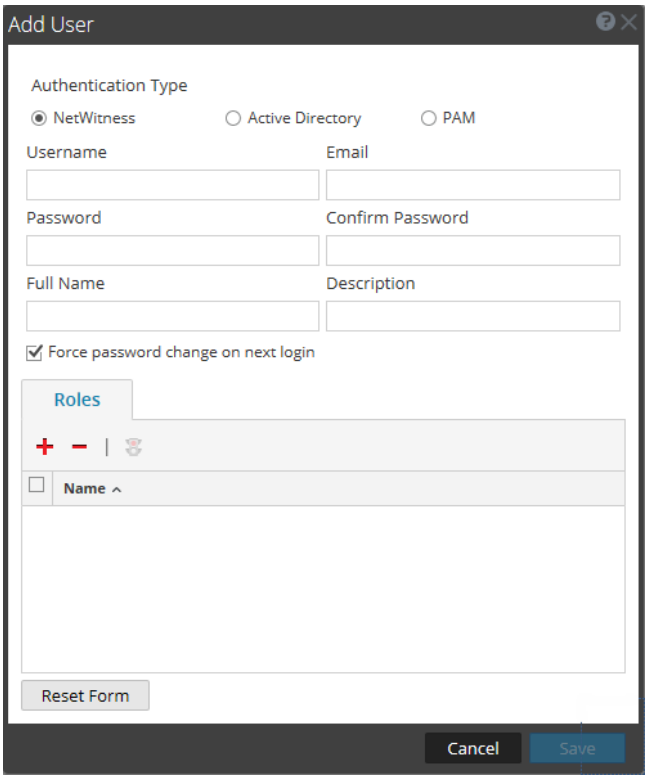
Procedures

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 User and Assign a Role

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.



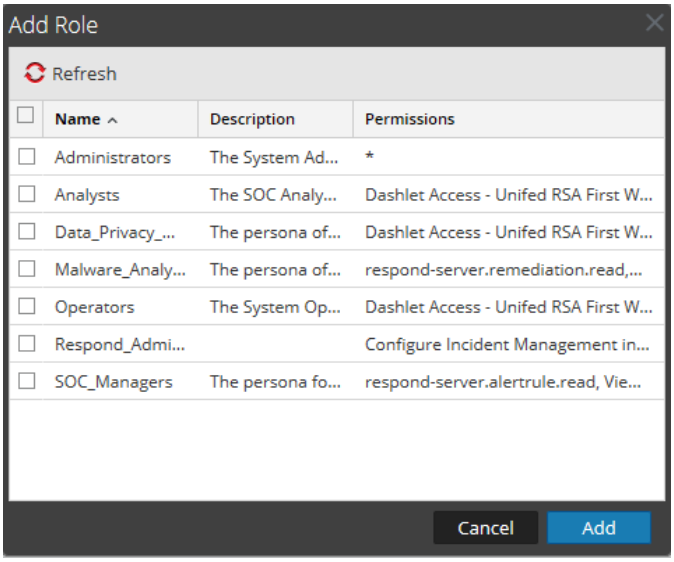
2. Type the following account information for the new user:
   - **Authentication Type**: **NetWitness** is selected by default and is the correct choice when adding a local user. This option is only displayed when there are AD or PAM configurations set up to allow for selecting that authentication type.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

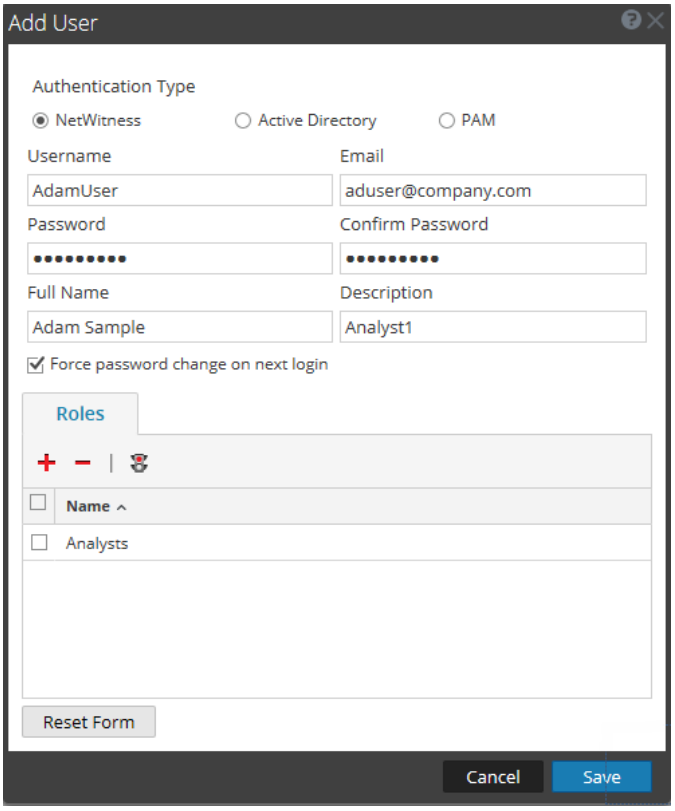
4. To assign a role to the user, click + in the **Roles** tab.

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



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

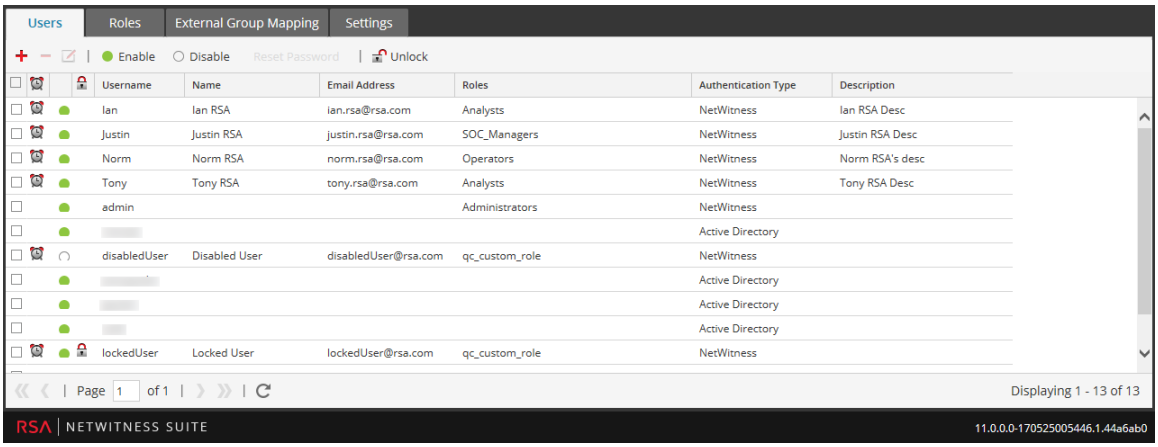
   The **Add User** dialog shows each role assigned to the user.



6. (Optional) Select a role and click to **Show all permissions** for the role.

7. 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

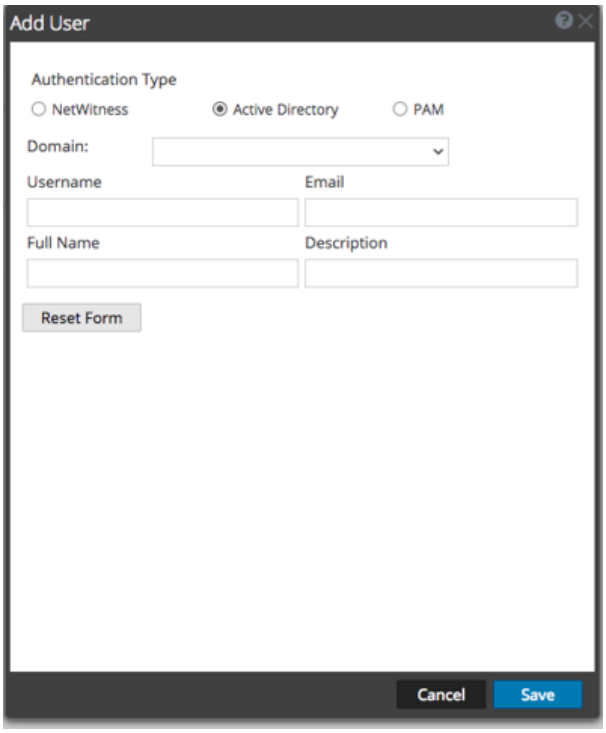
Prerequisite: External authentication must be configured. Refer to Step 4. (Optional) Configure External Authentication.

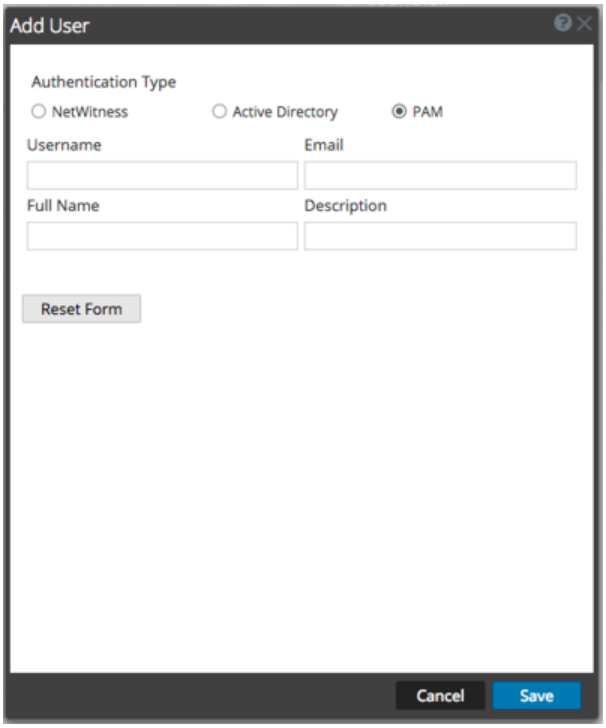
To add a user that is authenticated externally, outside of NetWitness Suite:

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 Suite
- **Email** address
- **Full Name** of the new user
- (Optional) **Description** of the user account

4. Click **Save**. The Users tab shows the new user account, which still needs a role and permissions.
5. To map a role to the new user, see Step 5. (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 .
7. Click **Save**.

Delete a User

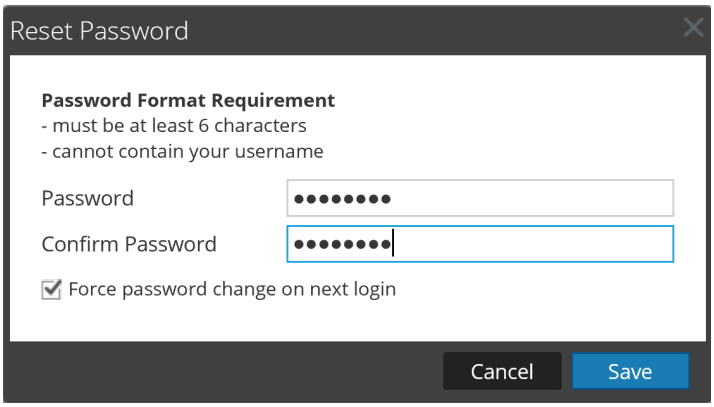
1. In the **Users** tab, select a user.
2. In the toolbar, click .

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

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 Step 1. Configure Password Complexity.

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

Enable, Unlock, and Delete User Accounts

This topic provides instructions for enabling, unlocking, and deleting user accounts.

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

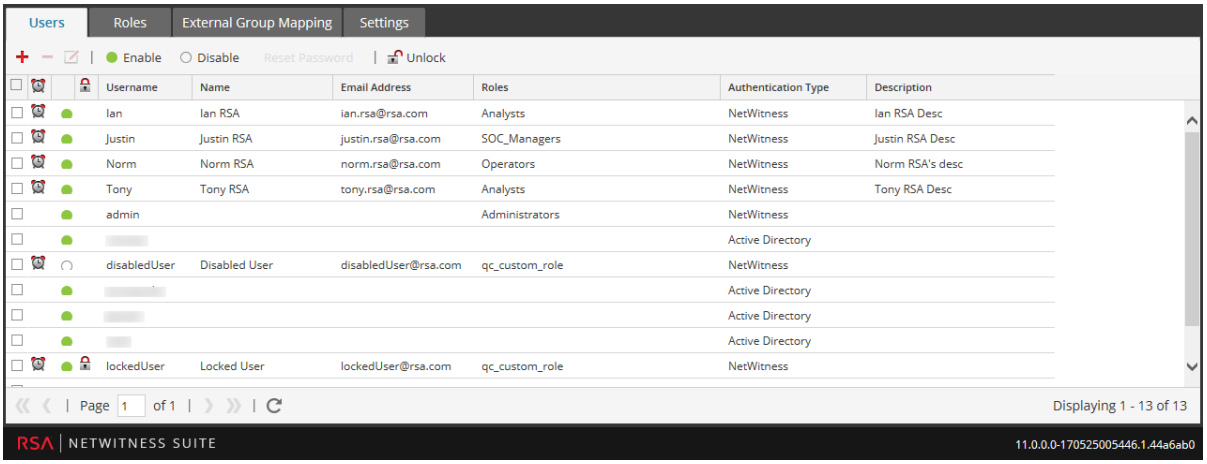
The first time an external user logs into NetWitness Suite, a new user entry is automatically created with NetWitness Suite. NetWitness Suite manages only user identification information; for example, Full Name and Email.

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

Enable Disabled NetWitness Suite User Accounts

To enable NetWitness Suite user accounts that have been disabled:

1. In NetWitness Suite, 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 dialog requests confirmation.
4. If you want to enable the accounts, click **Yes**.
   The accounts are enabled, and the user can log in to NetWitness Suite.

Disable NetWitness Suite 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 Suite user accounts:

1. In the **Users** grid, select one or more accounts.
2. Click Disable.

   A dialog requests confirmation.
3. If you want to disable the accounts, click **Yes**.

   The accounts are disabled, and the user can no longer log in to NetWitness Suite.

Unlock Locked NetWitness Suite User Accounts

A user is locked out for a period of time after a number of failed consecutive login attempts. To unlock NetWitness Suite 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 dialog requests confirmation.
3. If you want to unlock the accounts, click **Yes**.

   The accounts are unlocked, and the user can log on to NetWitness Suite.

Delete NetWitness Suite User Accounts

If not using External Authentication, a user can log on to NetWitness Suite using a local account. These local accounts are directly managed using NetWitness Suite. 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 Suite. If this is not the intention, disable the user instead of deleting the user.

To delete NetWitness Suite 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 Suite, and the users can no longer log in to NetWitness Suite.

Step 5. (Optional) Map User Roles to External Groups

This topic describes the method for mapping NetWitness Suite user roles to external groups.

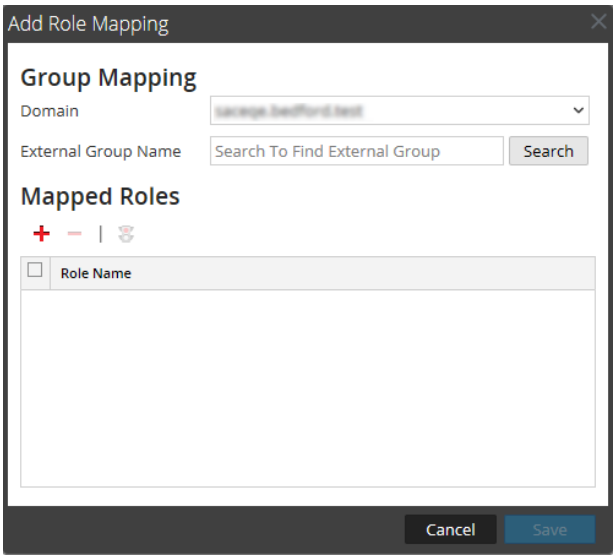
In NetWitness Suite, external groups derive permissions for various modules and views from NetWitness Suite user roles, which have permissions assigned to them. To provide access to an external group, map user roles to it. To modify an external group's access, edit the roles mapped to it. Add and delete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

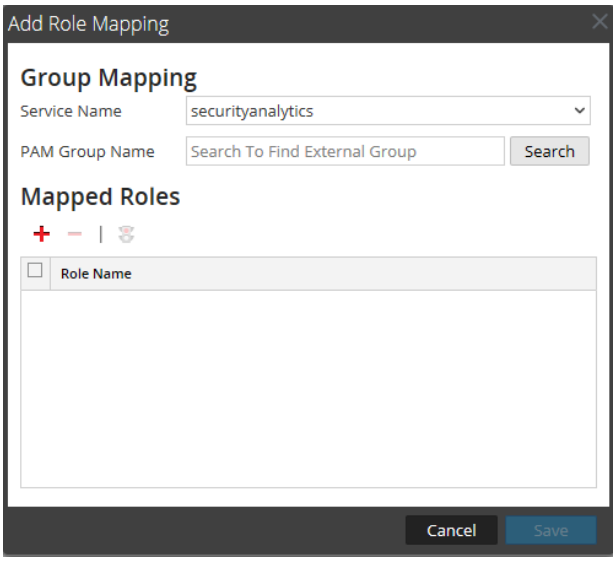
Prerequisites

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

Add Role Mapping for an External Group

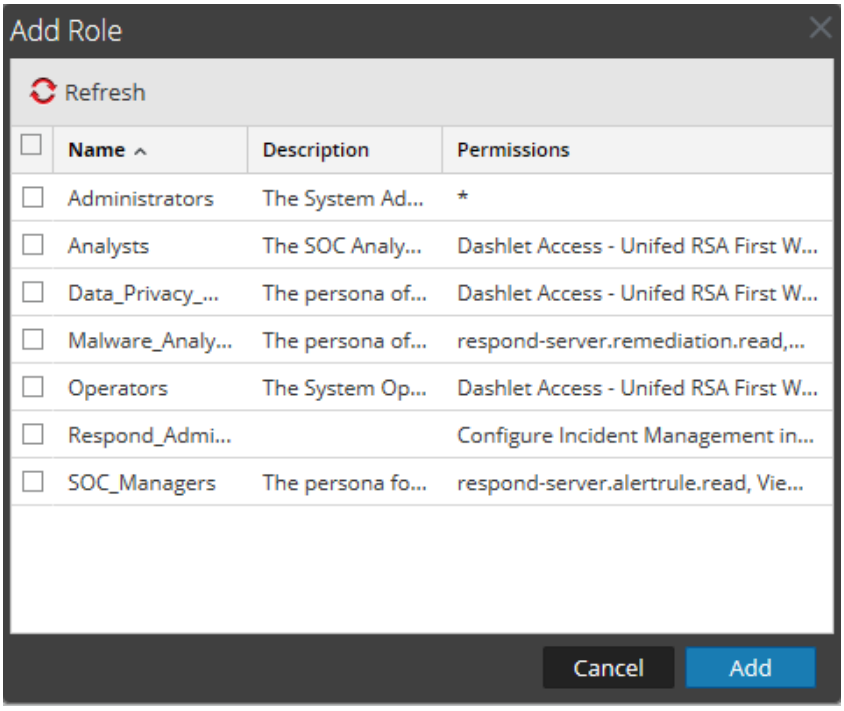
1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.
3. In the toolbar, click +.
   The **Add Role Mapping** dialog for the external authentication method you selected is displayed.





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. Click 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

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. Click 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.

Related Topic

- Search for External Groups

Search for External Groups

This topic provides instructions for searching for external groups that have NetWitness Suite user roles mapped to them.

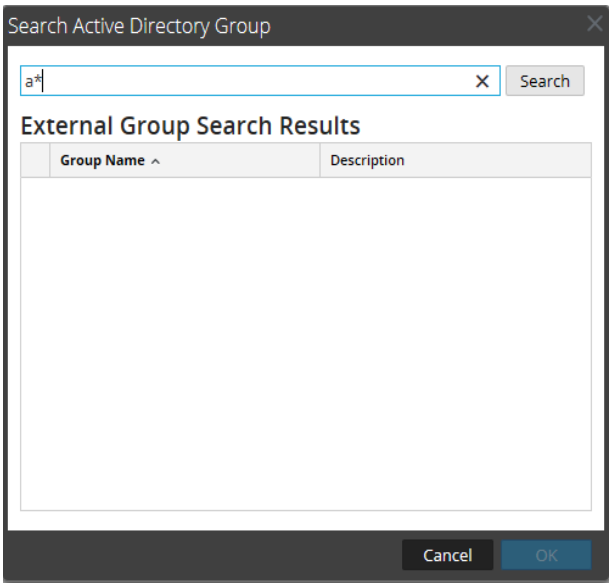
Prerequisites

A method for external user authentication must be enabled.

Procedure

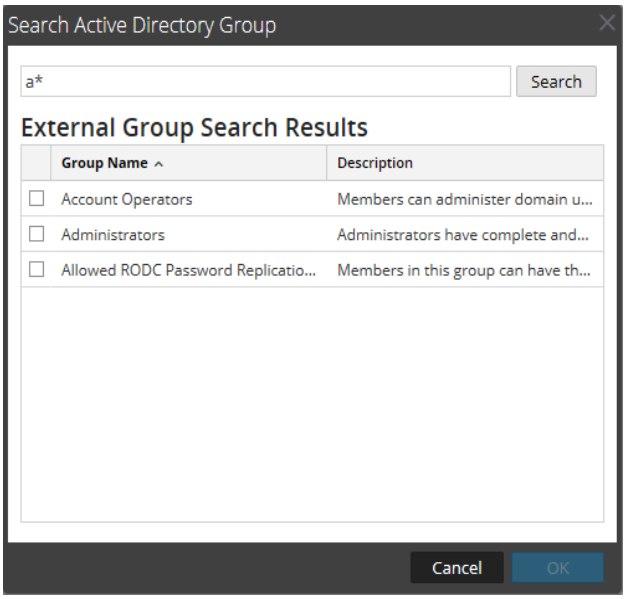
To search for an external group:

1. In NetWitness Suite, 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**.

References

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

Topics

Admin Security View

This topic describes each user interface element in the Admin > Security view and in all related dialogs and tabs. The interface components are listed in alphabetical order.

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

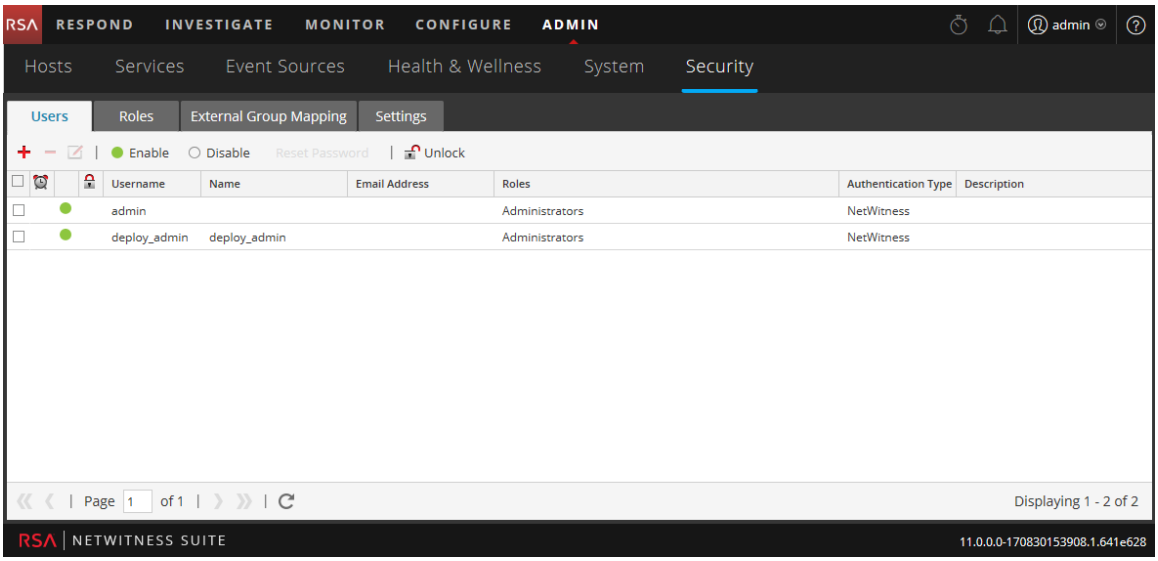
What do you want to do?

Role	I want to ...	Show me how
Admin	Manage users	Step 4. Set Up a User
Admin	Manage roles	Step 1. Review the Pre-Configured NetWitness Roles Step 2. (Optional) Add a Role and Assign Permissions
Admin	(Optional) Configure external group mappings	Step 5. (Optional) Map User Roles to External Groups
Admin	Configure settings	Step 3. Configure System-Level Security Settings

Related topics

- Users Tab
- Roles Tab
- External Group Mapping Tab
- Settings Tab

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



The Admin > Security view has four tabs:

- The **Users** tab provides a way to manage user accounts.
- The **Roles** tab provides a way to define security roles and assign roles to user accounts.
- The **External Group Mapping** tab provides a way to manage access parameters for LDAP groups.
- The **Settings** tab provides a way to configure password complexity and expiration for internal NetWitness Suite users and to configure system behavior due to failed logins and inactivity. It also provides a way to configure external authentication.

Users Tab

This topic introduces the features and functions to set up a user account in the Admin > Security view > Users tab.

Each NetWitness Suite user must have a user account. In the Users tab, you can create, edit, delete, enable/disable and unlock a user account.

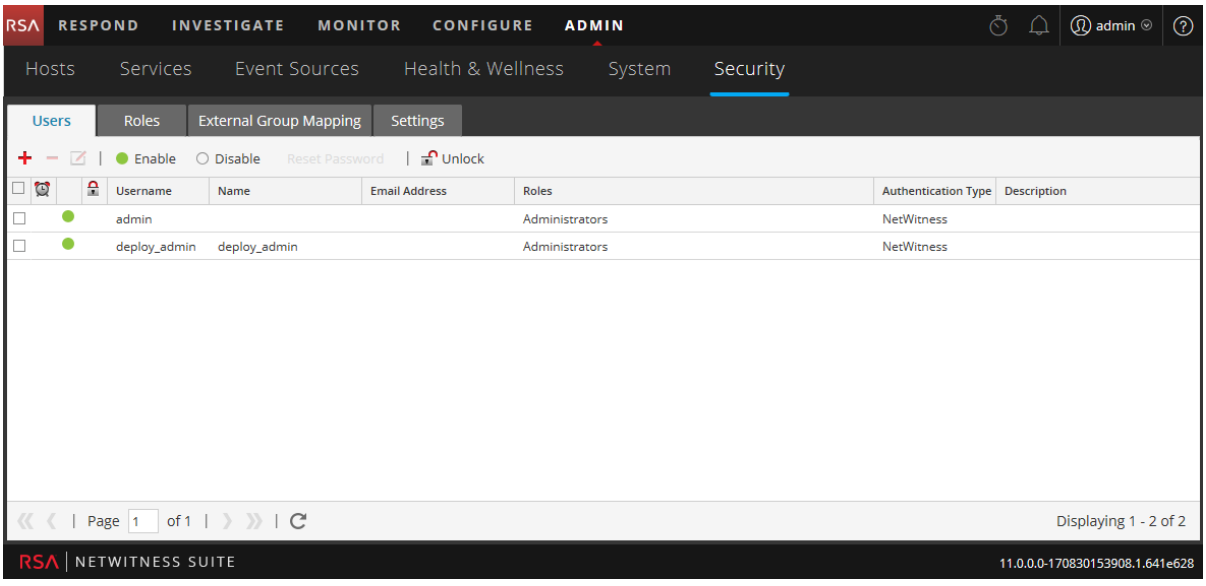
What do you want to do?

Role	I want to ...	Show me how
Admin	Set up a new user	Step 4. Set Up a User Add a User and Assign a Role
Admin	Manage user accounts	Enable, Unlock, and Delete User Accounts

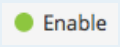
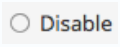
Related Topics

- Add or Edit User Dialog

To access this view, go to **ADMIN > Security**. The Security view opens to the **Users** tab by default.



The Users tab consists of the User list with a toolbar at the top. These are the toolbar features.

Feature	Description
	Opens the Add User dialog.
	Deletes the selected user.
	Opens the Edit User dialog for the selected user.
	Enables a disabled user account with all user preferences intact.
	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.

The **Users** list has these columns.

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 Suite.
Name	Name of the user to whom the account belongs.
Email Address	Email address of the user.
Roles	Role assigned to the user.
External	Authentication method, which could be external by Active Directory or PAM or internal by NetWitness Suite.
Description	Description of the user account.

Add or Edit User Dialog

This topic introduces the Add User and Edit User dialogs accessible from the Admin > Security view > Users tab.

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

What do you want to do?

Role	I want to ...	Show me how
Administrator	Add a User and Assign a Role	Step 2. (Optional) Add a Role and Assign Permissions
Administrator	Change User Information	Step 2. (Optional) Add a Role and Assign Permissions
Administrator	Reset a User Password	Step 2. (Optional) Add a Role and Assign Permissions
Administrator	Add a User for External Authentication	Step 2. (Optional) Add a Role and Assign Permissions

Related Topics

- Manage Users with Roles and Permissions
- Enable, Unlock, and Delete User Accounts

User Preferences

To display the **Add User** or **Edit User** dialog:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Do one of the following:
   - In the action bar, click  .
     The **Add User** dialog is displayed.

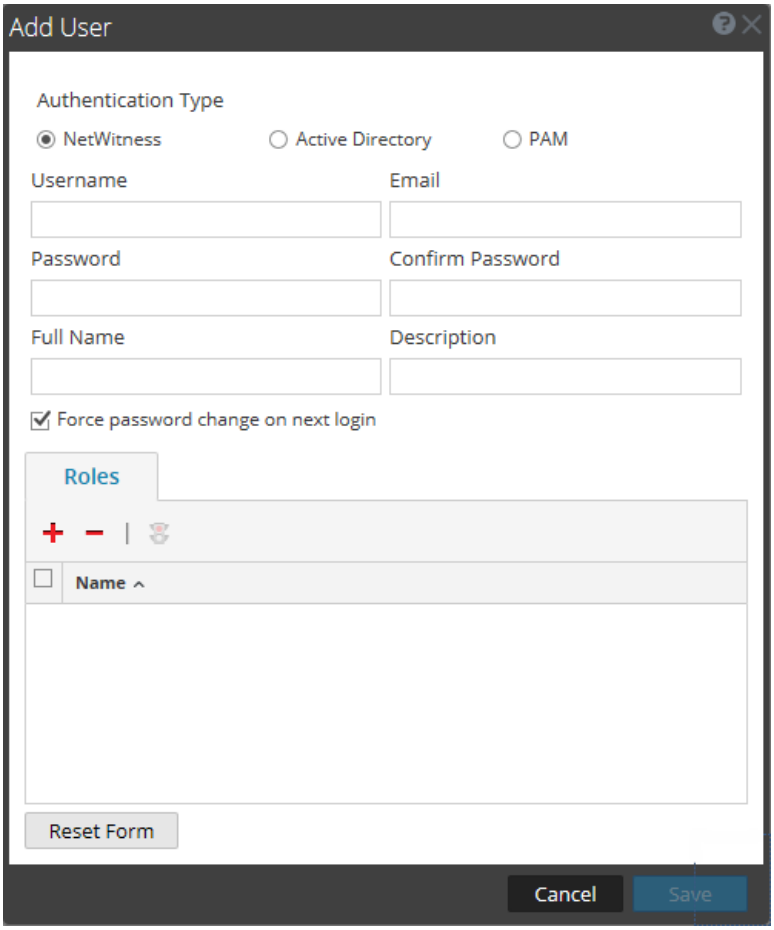
- Select a user and in the action bar, click .

  The **Edit User** dialog is displayed.

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.

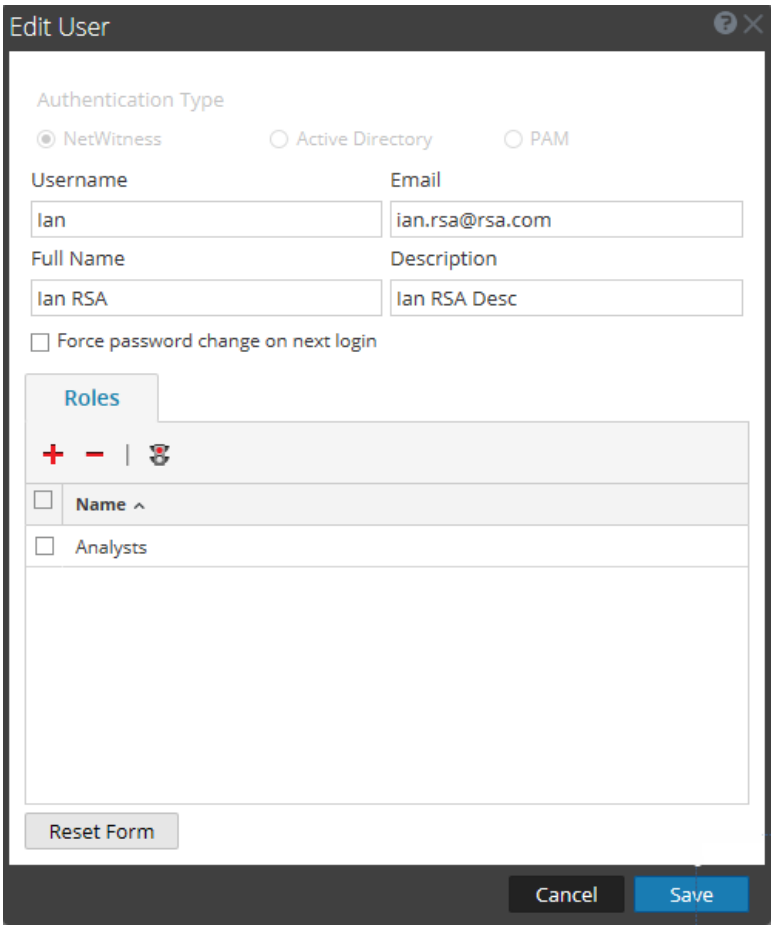
Add User Dialog

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 show:

- Authentication type
- User information
- Roles to which the user belongs

User Information

The following table provides descriptions of the user information.

Field	Description
Authentication Type	The authentication type for the user. Default selection is NetWitness, which designates an internal user. Options for external users are Active Directory and PAM. This field is disabled when editing a user.

Field	Description
Username	Username for the NetWitness Suite user account.
Full Name	Name of the user.
Password	(Add User dialog only) Password to log on to NetWitness Suite.
Confirm Password	(Add User dialog only) Password confirmation for adding the user password.
Email	Email address 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 Suite. 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.
	Removes the selected role from being assigned to the user.
	Shows permissions for the selected role.
Name	Lists each role assigned to the user.

Roles Tab

This topic introduces the functions of the Admin > Security view > Roles tab.

Roles are assigned to all NetWitness Suite 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.

What do you want to do?

Role	I want to ...	Show me how
Admin	View preconfigured roles	Step 1. Review the Pre-Configured NetWitness Roles
Admin	Create a new role	Step 2. (Optional) Add a Role and Assign Permissions

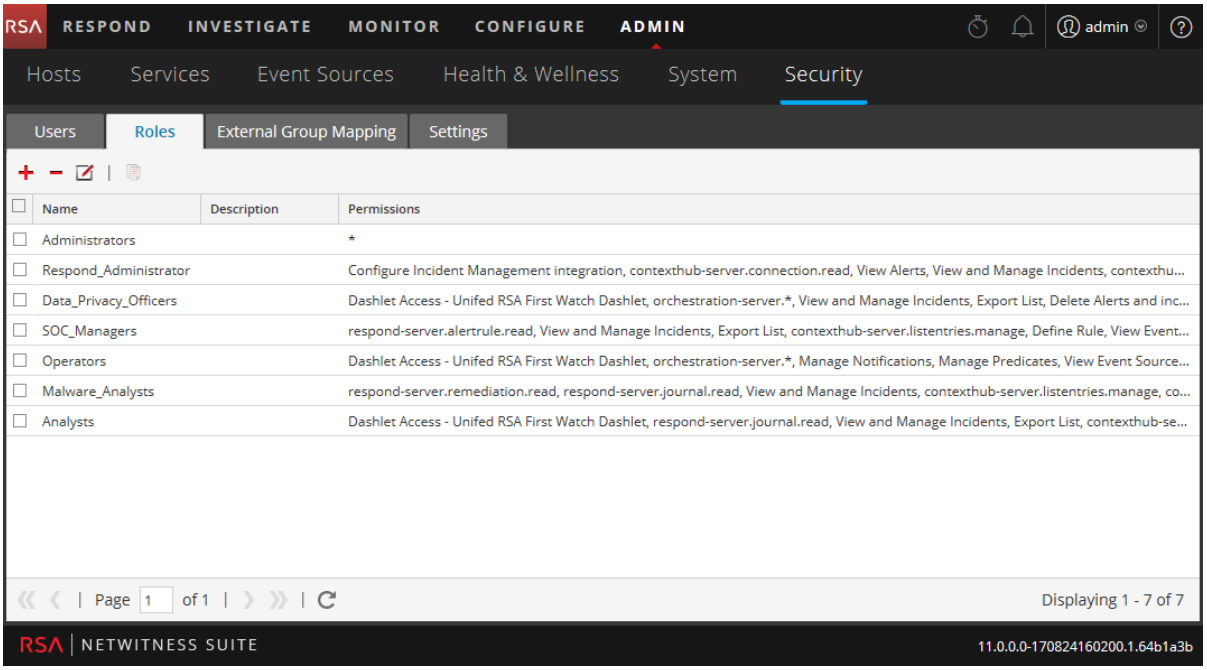
Related Topics

- Add or Edit Role Dialog

To access this view:

1. Go to **ADMIN > Security**.
   The Security view opens to the **Users** tab by default.

2. Click the **Roles** tab.



The Roles tab consists of the Roles list with a toolbar at the top.

The following table describes the toolbar features.

Feature	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.

The following table describes the roles list features.

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

This topic introduces the Add Role and Edit Role dialogs accessible from the Admin > Security view > Roles tab.

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?

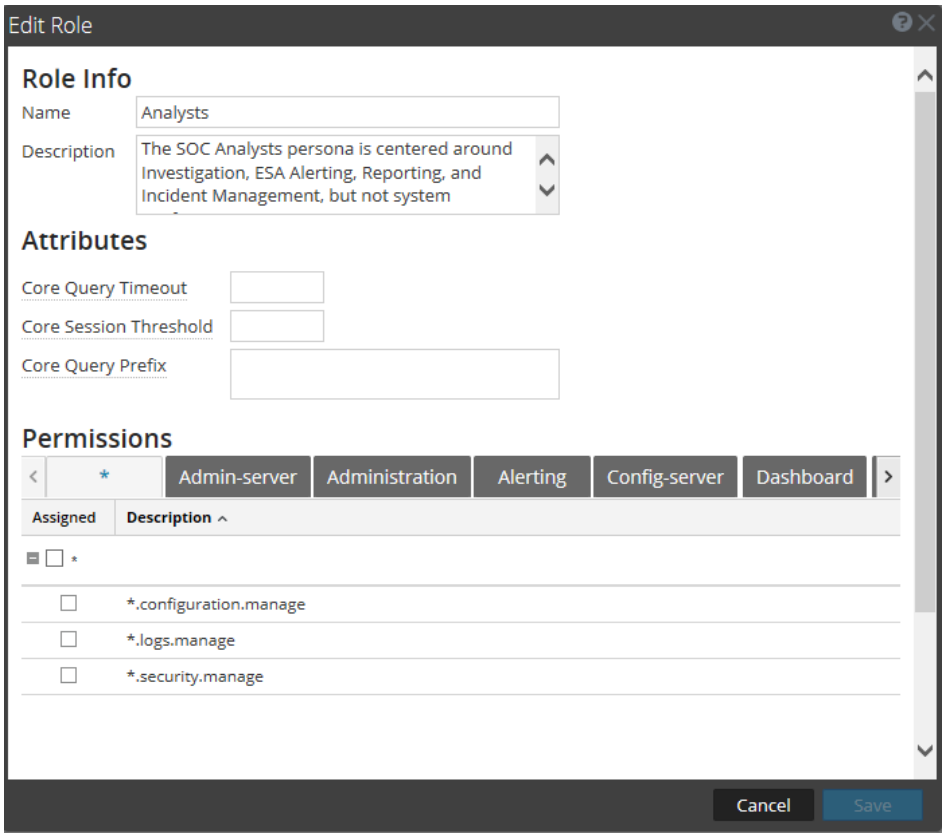
Role	I want to ...	Show me how
Admin	View preconfigured roles	Step 1. Review the Pre-Configured NetWitness Roles
Admin	Create a new role	Step 2. (Optional) Add a Role and Assign Permissions
Admin	Edit a role	Step 2. (Optional) Add a Role and Assign Permissions
Admin	Delete a role	Step 2. (Optional) Add a Role and Assign Permissions

To access this view:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view opens to the **Users** tab by default.
2. Click the **Roles** tab.
3. Do one of the following:
   - In the action bar, click  .
     The **Add Role** dialog is displayed.

- Select a role and in the action bar, click .

  The **Edit Role** dialog is displayed.



The Add Role and Edit Role dialogs include three sections: **Role Info**, **Attributes**, and **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

This is the information in the **Attributes** section. A value shown in italics indicates a default value, for example, *5*. A value shown without italics indicates a change from the default value, for example, `1200`. Step 3. Verify Query and Session Attributes per Role provides more information.

Feature	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. When migrating to NetWitness Suite 10.5 and later, if there is no value set in the roles, 5 minutes is set by default. **Note:** NetWitness Suite 10.5 and later Core services use this field.
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

This is the information in the **Permissions** section. Role Permissions describes the permissions.

Feature	Description
Module tabs	There are eight tabs, one for each module: Administration, Alerting, Incidents, Investigation, Live, Malware, Reports, and Dashboard. Each tab lists the permissions for a module.
Description column	List of all permissions for the module.
Assigned column	Checkbox that indicates if a module permission is assigned to the role.
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 Suite user roles to an external group. The External Group Mapping tab provides information about each external group to which you have mapped roles.

What do you want to do?

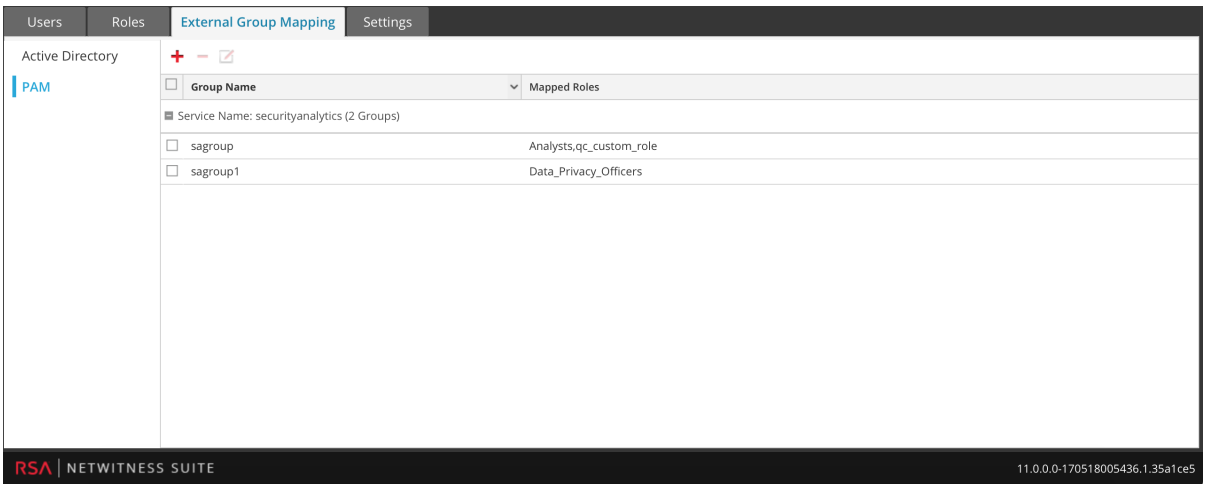
Role	I want to ...	Show me how
Admin	Map a role to an external group	Step 5. (Optional) Map User Roles to External Groups
Admin	Search for an external group	Search for External Groups

Related Topics

- Add Role Mapping Dialog
- Search External Groups Dialog

To access this view:

1. In NetWitness Suite, go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **External Group Mapping** tab.



The External Group Mapping tab consists of a toolbar and list.

The list has the following features.

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 Suite.
Mapped Roles	Displays the NetWitness Suite roles mapped to the external group.

The **toolbar** has the following features.

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

Add Role Mapping Dialog

This topic introduces the features of the Admin >Security > External Group Mapping tab > Add Role Mapping dialog.

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

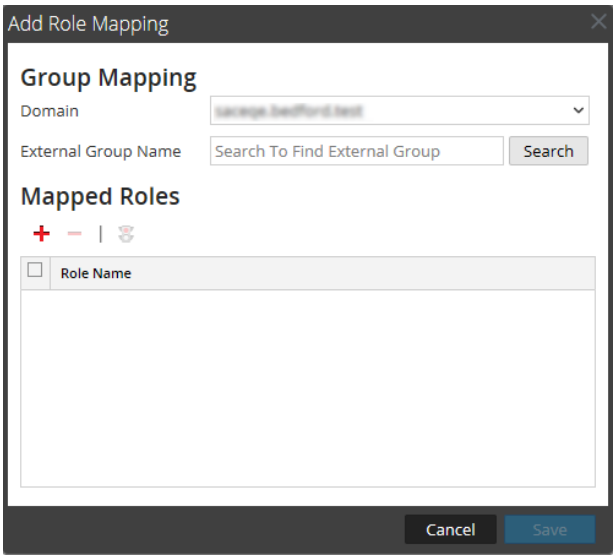
What do you want to do?

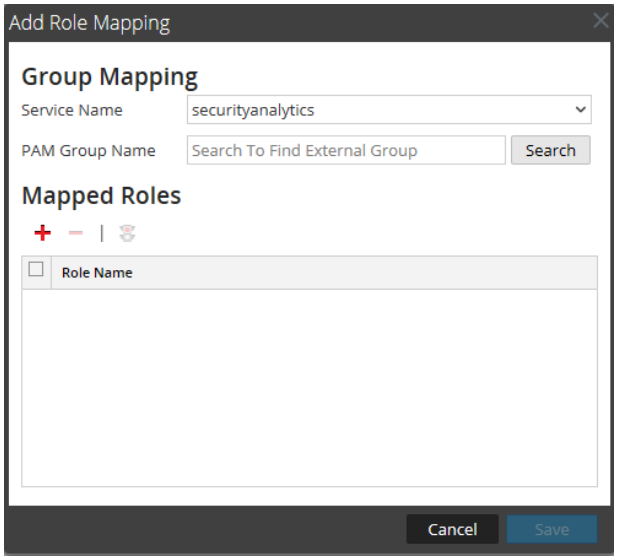
Role	I want to ...	Show me how
Admin	Map a role to an external group	Step 5. (Optional) Map User Roles to External Groups
Admin	Search for an external group	Search for External Groups

To access this dialog:

1. In NetWitness Suite, go to **ADMIN > Security**.
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.





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.

Group Mapping

The **Group Mapping** section has the following 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.

Feature	Description
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. Search is not available in the Edit Role Mapping dialog.

Mapped Roles

The **Mapped Roles** section has the following features.

Feature	Description
	Opens the Add Role dialog, in which configured NetWitness Suite user roles to add are listed.
	Removes selected roles from the Mapped Roles grid.
Name	Displays the name of the NetWitness Suite user role.
Permissions	Displays the permissions associated with the NetWitness Suite 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

This topic describes the features of the Admin > Security view > Search External Groups dialog.

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

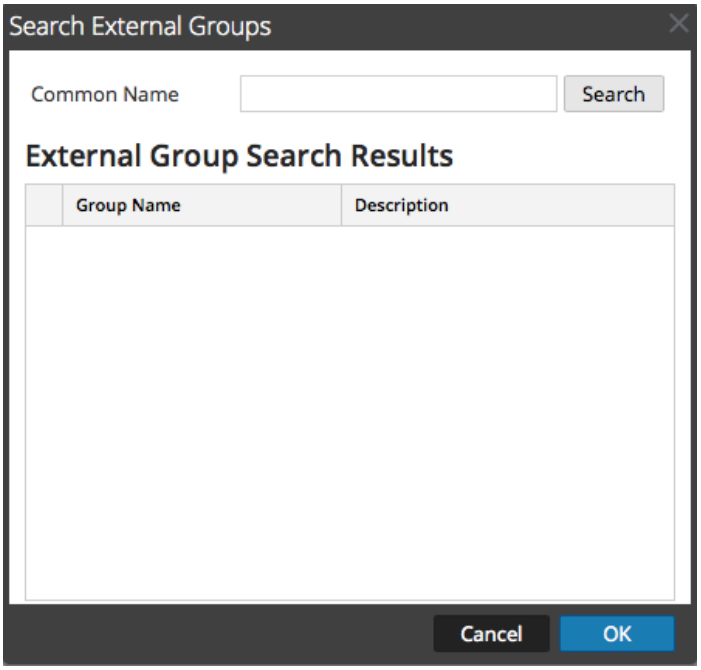
What do you want to do?

Role	I want to ...	Show me how
Admin	Map a role to an external group	Step 5. (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

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**.
   The **Search External Groups** dialog is displayed.



The following table describes the features of the Search External Groups dialog.

Feature	Description
Common Name	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

This topic explains the ADMIN > Security view > Settings tab. In the Settings tab, you configure password complexity for internal NetWitness Suite users and system-wide security parameters.

For information on configuring NetWitness Suite security, see Set Up System Security.

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.

What do you want to do?

Role	I want to ...	Show me how
Admin	Configure password complexity	Step 1. Configure Password Complexity
Admin	Configure system-level security settings	Step 3. Configure System-Level Security Settings
Admin	(Optional) Configure external authentication	Step 4. (Optional) Configure External Authentication

Related Topics

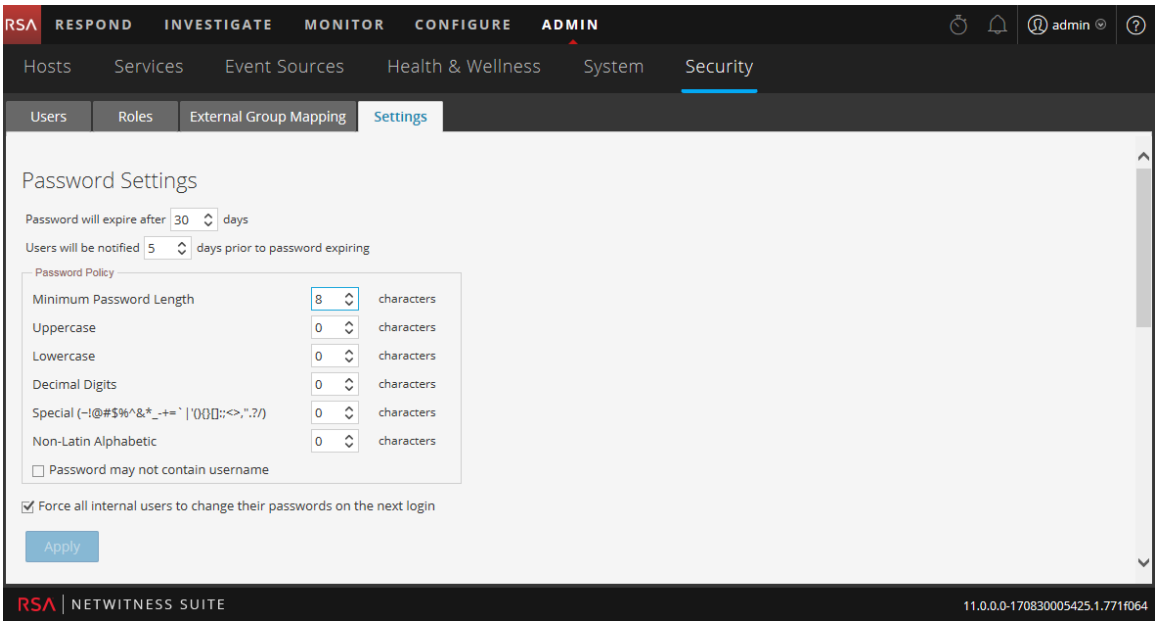
- Set Up System Security

Admin Security View Settings Tab

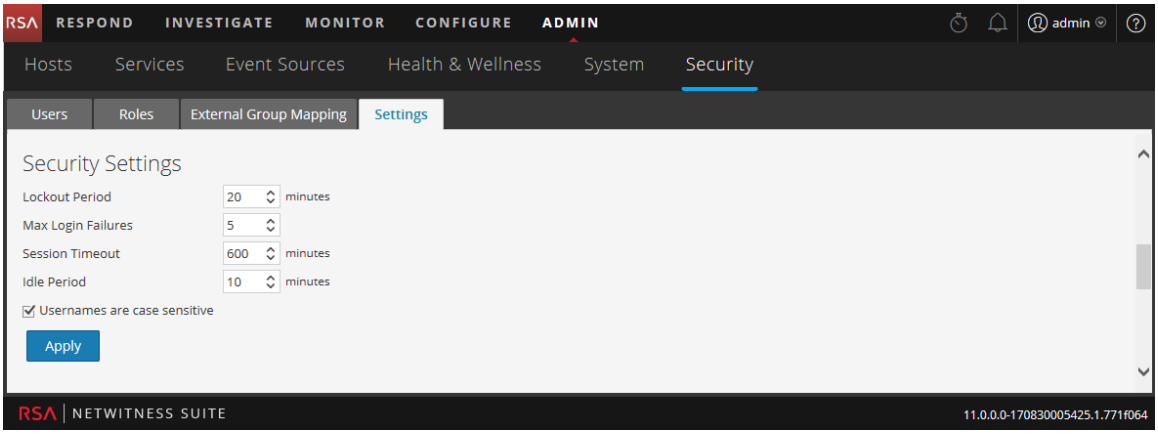
To access the Settings tab:

1. Go to **ADMIN > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.

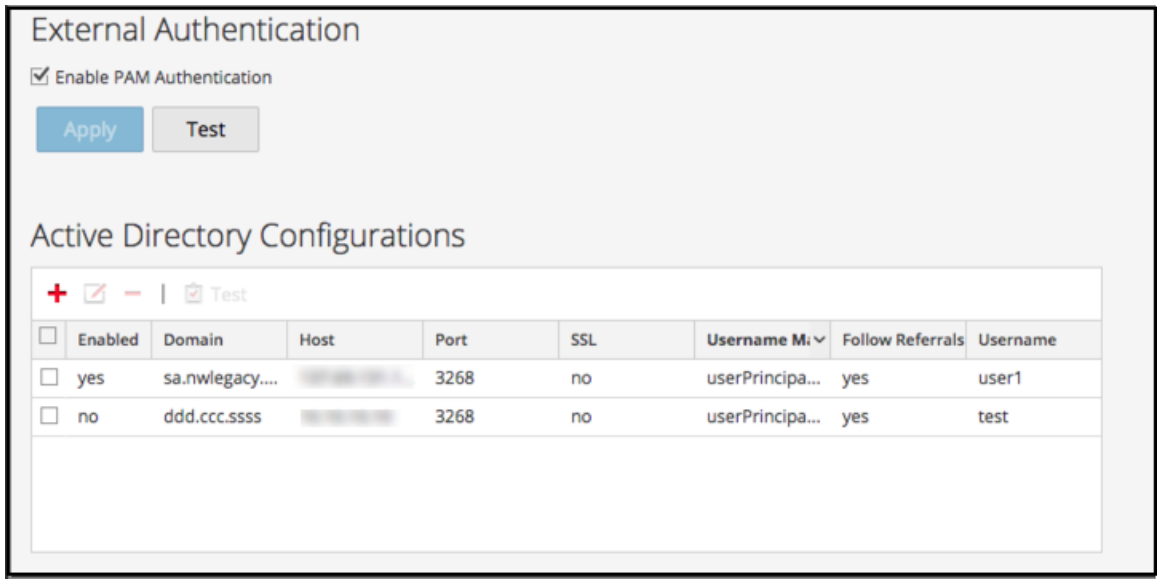
The following figure shows the Password Settings section of the Settings tab.



The following figure shows the Security Settings section of the Settings tab.



The following figure shows the PAM Authentication and Active Directory Configurations sections of the Settings tab.



Password Settings

The Password Policy section enables you to configure password complexity requirements for internal NetWitness Suite 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 Suite 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 Suite. The minimum value is 1 day.
Minimum Password Length	Specifies a minimum password length requirement for NetWitness Suite user passwords. A minimum password length prevents users from using short passwords that are easy to guess.

Option	Description
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 Suite 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 Suite 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 Suite.

Security Settings

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

Option	Description
Lockout Period	Number of minutes to lock a user out of NetWitness Suite 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 Suite login screen to be case sensitive. For example, if usernames are case sensitive, you could use admin to log on to NetWitness Suite, but you could not use Admin.

Option	Description
Apply	Makes the settings become effective immediately.

PAM Authentication

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

Option	Description
Enable PAM Authentication	Allows NetWitness Suite 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 Suite to use Active Directory to authenticate external user logins.

Option	Description
Enabled	Enables Active Directory authentication for NetWitness Suite 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 Suite 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.

Option	Description
Follow Referrals	Indicates whether NetWitness Suite will follow LDAP referrals made by Active Directory.
Username	Username of the user 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 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.