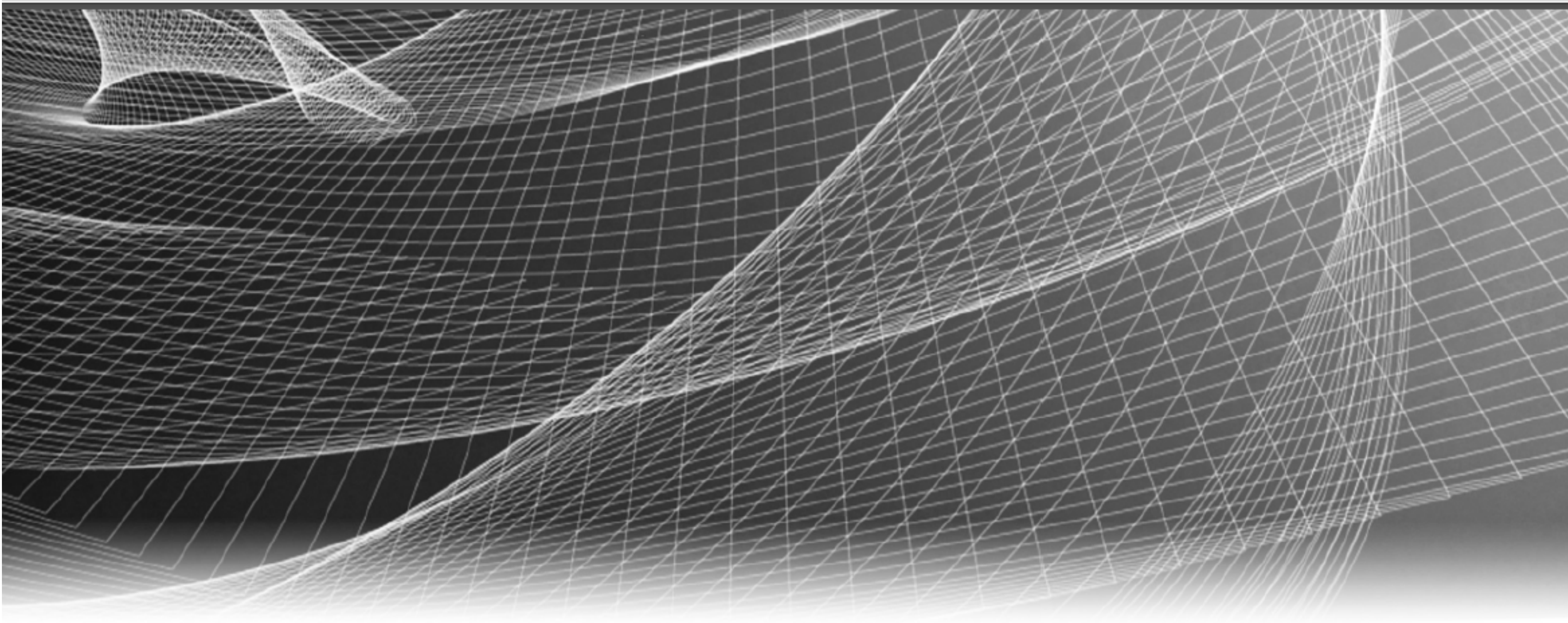


RSA Security Analytics

System Security and User Management

for Version 10.6.5

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

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

January 2018

Contents

System Security and User Management Overview 7

How Role-Based Access Control W orks 8

Pre-Configured Roles 8

Trusted Connections Between Server and Service 9

How Trusted Connections Are Established 10

Common Role Names on the Server and Services 10

End-to-End Workflow for User Setup and Service Access 11

Role Permissions 13

Set Up System Security 25

Step 1. Configure Password Complexity 26

Password Strength 26

Configure Password Strength 27

Step 2. Change the Default admin Passwords 29

Best Practices 29

Change the admin Password for the Security Analytics Service 29

Change the admin Password for Security Analytics Core Services 29

Remove and re-add a Data Source on the Reporting Engine 30

Change the admin Password for a Service Using the REST API 31

Step 3. Configure System-Level Security Settings 32

Configure Security Settings 32

Step 4. (Optional) Configure External Authentication 34

Configure Active Directory 35

Configure Active Directory Authentication 35

Add a New Active Directory Configuration 36

Edit an Active Directory Configuration 37

Test an Active Directory Configuration 39

Test an Active Directory User Lookup 39

Delete an Active Directory Configuration 39

Configure PAM Login Capability 40

Pluggable Authentication Modules 40

Name Service Switch 40

PAM and NSS Combination 41

Process Overview 41

PAM K erberos 42

PAM LDAP 44

PAM RADIUS 46

Add a RADIUS Client and Associated Agent 48

PAM Agent for SecurID 50

Configure and Test the NSS Service 54

NSS UNIX 55

NSS Samba 55

NSS LDAP 58

Test NSS Functionality 62

Test External Authentication 65

Step 5. (Optional) Use Custom Server Certificate 66

Supported Certificate Formats 66

Procedures 67

Step 6. (Optional) Configure PKI Authentication 71

Step 7. (Optional) Create a Customized Login Banner 72

Create and Enable a Customized Login Banner 72

Manage Users with Roles and Permissions 75

Step 1. Review the Pre-Configured Security Analytics Roles 76

Step 2. (Optional) Add a Role and Assign Permissions 77

Add a Role and Assign Permissions 78

Duplicate a Role 79

Change Permissions Assigned to a Role 79

Delete a Role 79

Step 3. Verify Query and Session Attributes per Role 80
Query and Session Attributes 80
How Query-Handling Attribute Settings Apply to Individual Users 81
Procedure 81
Step 4. Set Up a User 84
Add a User and Assign a Role 85
Add a User and Assign a Role 85
Add a User for External Authentication 89
Change User Information or Roles 90
Delete a User 90
Verify Query and Session Attributes per User 92
Enable, Unlock, and Delete User Accounts 95
Step 5. (Optional) Map User Roles to External Groups 98
Prerequisites 98
Add Role Mapping for an External Group 99
Edit Role Mapping for a Group 100
Search for External Groups 102
Set Up Public Key Infrastructure (PKI) Authentication 105
Overview 106
Security Analytics PKI Authentication Workflow 106
Configure PKI Authentication 108
Step 1. Configure Active Directory 109
Step 2. Map User Roles to External Groups 110
Step 3. Import Server Certificate and Trusted CA Certificate 111
Step 4. Configure User Principal Settings 112
Step 5. Import Certificate Revocation List 115
Specify CRL file on HTTP server 115
Import Local CRL file using Security Analytics UI 116
Specify CRL as LDAP Resource using Security Analytics UI 116
Specify OCSP Responder using Security Analytics UI 117
Configure CRL Settings 118

Step 6. Enable PKI 120
Enable PKI Authentication 120
System Security and User Management: Additional Procedures 123
Delete Certificate Revocation List 124
Delete CRL 124
Delete Server Certificate and Trusted CA Certificate 125
Procedures 125
Disable PKI 127
Disable PKI 127
System Security and User Management: References 129
Administration Security View 130
Add or Edit Role Dialog 132
Add or Edit User Dialog 136
Add Role Mapping Dialog 141
External Group Mapping Tab 143
Login Banner Tab 145
Roles Tab 147
Search External Groups Dialog 149
Settings Tab 151
PKI Settings Tab 156
Server Certificates 157
Trusted CAs 158
CRLs 158
CRL Settings 159
User Principal Settings 160
Enable PKI 161
Users Tab 162
Certificate Attributes 164
System Security and User Management: Troubleshooting 165
Possible Issues 165

System Security and User Management Overview

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

- How Role-Based Access Control Works
- Set Up System Security
- Manage Users with Roles and Permissions
- Set Up Public Key Infrastructure (PKI) Authentication
- System Security and User Management: Additional Procedures
- System Security and User Management: References
- System Security and User Management: Troubleshooting

How Role-Based Access Control Works

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

In Security Analytics, 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 Security Analytics. 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 Incident Management.
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 Incident Management, but not system configuration.
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 Incident Management.
Malware_Analysts	Access to investigations and malware events. The only access granted to the Malware Analysts persona is the Malware Analysis module.

Role	Permission
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 Security Analytics Server to manage and authenticate users. This reduces administration on each service because authenticated users do not have to be defined locally in each Security Analytics 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 Security Analytics 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 Security Analytics 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 Security Analytics Log On and are authenticated by the server.
- Users, already authenticated by the server, access every core service in **Administration** > **Services** without entering a password.

How Trusted Connections Are Established

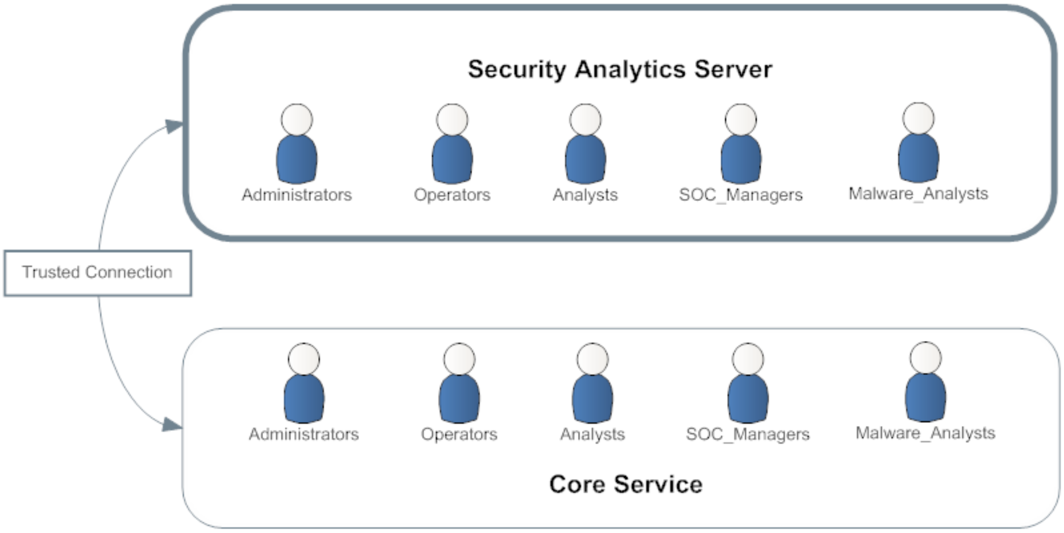
When you install or upgrade to 10.6, trusted connections are established by default with two settings:

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

To establish a trusted connection, each Security Analytics Core service must be upgraded to 10.4 or later. Trusted connections are not backwards compatible with Security Analytics Core 10.3.x or earlier.

Common Role Names on the Server and Services

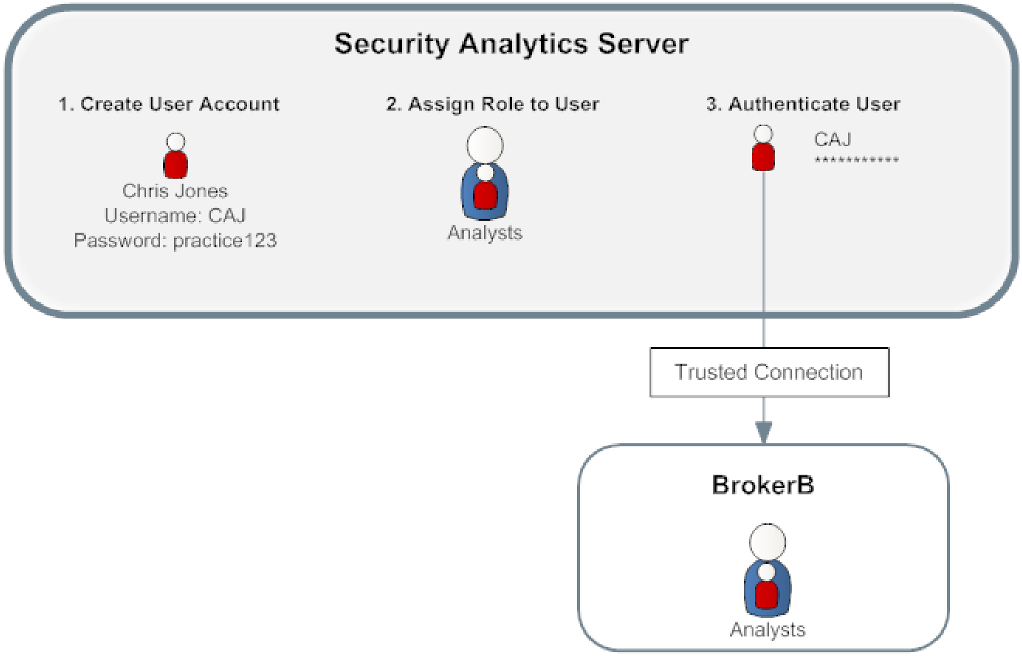
Trusted connections rely on common role names on the server and service. On a fresh installation, Security Analytics installs the five pre-configured roles on the server and each core service. If you upgrade to 10.6 from 10.3x or earlier, Security Analytics does not install the new SOC_Managers and Malware_Anlaysts roles. You must add these roles to 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 Security Analytics Server and the service BrokerB.



1. On Security Analytics 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 Security Analytics 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 Security Analytics roles have by default.

Within Security Analytics, user access to each module, dashlet, and view is restricted based on the assigned permissions described in this topic. The tables have a row for each permission with columns to indicate if it is a default permission for each user role:

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

Administration

The following table lists the permissions in the Administration tab:

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Administration Module	Yes	Yes	Yes	Yes	Yes	Yes
Access Health & Wellness	Yes	Yes	Yes	Yes	Yes	Yes
Apply System Updates	Yes	Yes				
Can Opt In to Live Intelligence Sharing	Yes	Yes				
Manage Global Auditing	Yes	Yes				Yes

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Manage Health & Wellness Policy	Yes	Yes				
Manage SA Advanced Settings	Yes	Yes				
Manage SA Auditing	Yes	Yes				Yes
Manage SA Email	Yes	Yes				
Manage SA LLS	Yes	Yes				
Manage SA Logs	Yes	Yes				Yes
Manage SA Notifications	Yes	Yes				
Manage SA Plugins	Yes	Yes				
Manage SA Predicates	Yes	Yes				
Manage SA Reconstruction	Yes	Yes				
Manage SA Security	Yes	Yes				Yes
Manage Services	Yes	Yes				Yes
Manage System Settings	Yes	Yes				

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Modify ESA Settings	Yes	Yes				
Modify Event Sources	Yes	Yes				
Modify Hosts	Yes	Yes				
Modify Services	Yes	Yes				Yes
View Event Sources	Yes	Yes		Yes		
View Health & Wellness Policy	Yes	Yes	Yes	Yes		
View Health & Wellness Stats Browser	Yes	Yes	Yes	Yes		Yes
View Hosts	Yes	Yes				Yes
View Services	Yes	Yes				Yes

Alerting

The following table lists the permissions in the Alerting tab:

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

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
View Rules	Yes	Yes		Yes		Yes

Incidents

The following table lists the permissions in the Incidents tab:

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

Investigation

The following table lists the permissions in the Investigation tab:

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Access Investigation Module	Yes		Yes	Yes	Yes	Yes
Context Lookup	Yes		Yes	Yes	Yes	

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

Live

The following table lists the permissions in the Live tab:

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Live						
Access Live Module	Yes	Yes	Yes	Yes		Yes
Manage Live System Settings	Yes	Yes				
Resources						
Deploy Live Resources	Yes	Yes				Yes
Manage Live Feeds	Yes	Yes				Yes

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Manage Live Resources	Yes	Yes				Yes
Search Live Resources	Yes	Yes	Yes	Yes		Yes
View Live Resource Details	Yes	Yes	Yes	Yes		Yes

Malware

The following table lists the permissions in the Malware tab:

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

Reports

The following table lists the permissions in the Reports tab:

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Alert						
Define RE Alert	Yes		Yes	Yes		Yes

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

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

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Define Schedule	Yes		Yes	Yes		Yes
Delete Schedule	Yes		Yes	Yes		Yes
View Schedules	Yes		Yes	Yes		Yes
Warehouse Analytics						
Define Jobs	Yes		Yes	Yes		Yes
Delete Jobs	Yes		Yes	Yes		Yes
Manage Jobs	Yes		Yes	Yes		Yes
View Jobs	Yes		Yes	Yes		Yes

Dashboard

The following table lists the permissions in the Dashboard tab:

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Dashlet Access - Admin Device List Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Admin Device Monitor Dashlet	Yes	Yes				Yes
Dashlet Access - Admin News Dashlet	Yes	Yes	Yes	Yes		Yes

Permission	Administrators	Operators	Analysts	SOC Mgrs	MAs	DPOs
Dashlet Access - Alert Variance Dashlet	Yes		Yes	Yes		Yes
Dashlet Access - Alerting Recent Alerts Dashlet	Yes		Yes	Yes		Yes
Dashlet Access - Investigation Jobs Dashlet	Yes		Yes	Yes		Yes
Dashlet Access - Investigation Top Values Dashlet	Yes		Yes	Yes		Yes
Dashlet Access - Live Featured Resources Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Live New Resources Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Live Subscriptions Dashlet	Yes	Yes	Yes	Yes		Yes
Dashlet Access - Live Updated Resources Dashlet	Yes	Yes	Yes	Yes		Yes

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

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 Security Analytics.

Topics

- Step 1. Configure Password Complexity
- Step 2. Change the Default admin Passwords
- Step 3. Configure System-Level Security Settings
- Step 4. (Optional) Configure External Authentication
- Step 6. (Optional) Configure PKI Authentication
- Step 7. (Optional) Create a Customized Login Banner

Step 1. Configure Password Complexity

This topic provides instructions to set system-wide Security Analytics 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, Security Analytics software allows you to configure the password complexity requirements for internal Security Analytics 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.

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

You can choose to enforce any combination of the following password strength requirements when a Security Analytics 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.

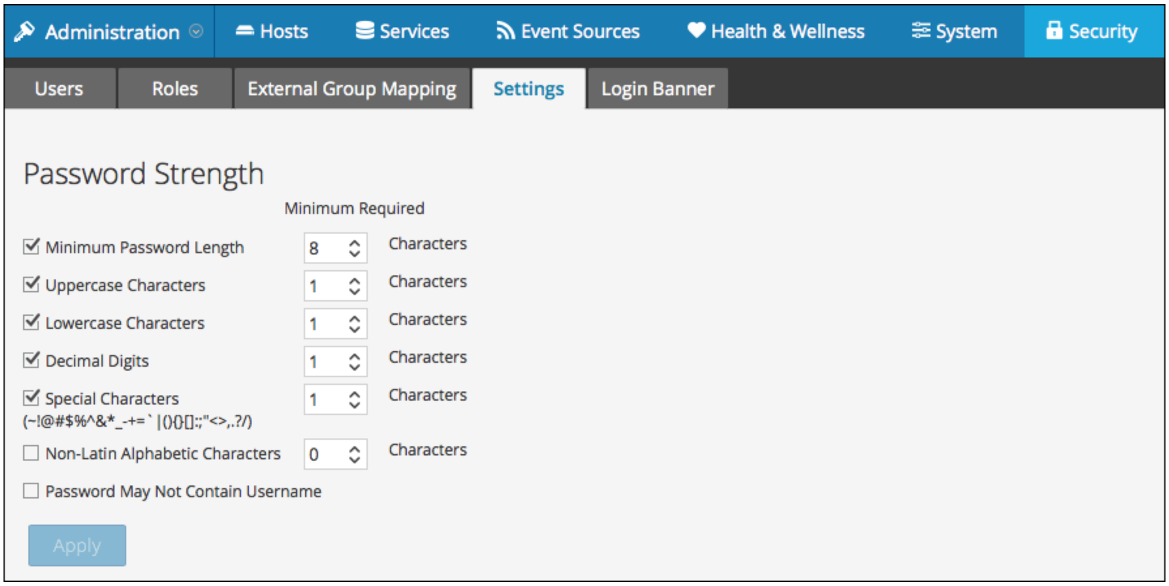
STIG Compliant Passwords in the *System Maintenance Guide* provides an example of a strong password policy.

Configure Password Strength

1. In the **Security Analytics** menu, select **Administration** > **Security**.

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

2. Click the **Settings** tab.



Password Strength

	Minimum Required	
☑ Minimum Password Length	8	Characters
☑ Uppercase Characters	1	Characters
☑ Lowercase Characters	1	Characters
☑ Decimal Digits	1	Characters
☑ Special Characters (~!@#$%^&*_-+=` |(){}[]:;"<>,.?/)	1	Characters
☐ Non-Latin Alphabetic Characters	0	Characters
☐ Password May Not Contain Username		

3. In the **Password Strength** section, select the password complexity requirements to enforce when Security Analytics users set their passwords and specify the minimum characters required, if applicable. Clear the checkbox for the requirements that you do not want to enforce.

Requirement	Description
Minimum Password Length	Specifies a minimum password length. A minimum password length prevents users from using short passwords that are easy to guess.
Uppercase Characters	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

<table>
<tr><th>Requirement</th><th>Description</th></tr>
<tr><td>Lowercase Characters</td><td>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</td></tr>
<tr><td>Base 10 Digits</td><td>Specifies a minimum number of decimal characters (0 through 9) for the password.</td></tr>
<tr><td>Special Characters (~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/)</td><td>Specifies a minimum number of special characters for the password:<br>~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/</td></tr>
<tr><td>Non-Latin Alphabetic Characters</td><td>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)</td></tr>
<tr><td>Password May Not Contain Username</td><td>Specifies that a password cannot contain the case-insensitive username of the user.</td></tr>
</table>

4. Click **Apply**.
5. In the confirmation dialog, select an answer to the following question: Do you want to force all internal users to change their passwords on the next login?
   - **Yes**: Forces all internal users to change their passwords the next time they log on to Security Analytics. This overrides any individual user account settings.
   - **No**: Forces only those internal users with the **Force password change at next login** option enabled in their individual user account settings to change their password the next time they log on to Security Analytics.

The password strength settings take effect when Security Analytics users create or change their passwords.

Step 2. Change the Default admin Passwords

This topic provides instructions for changing the admin password for the Security Analytics service and for the Security Analytics Core services.

The system administrator's user account is installed with Security Analytics. The username is **admin** and the default password is **netwitness**. 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 Security Analytics 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 Security Analytics 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 Security Analytics and on each Security Analytics Core service. For security, you create the Users and Roles for your organization in Security Analytics, and on each Security Analytics 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 Security Analytics Service

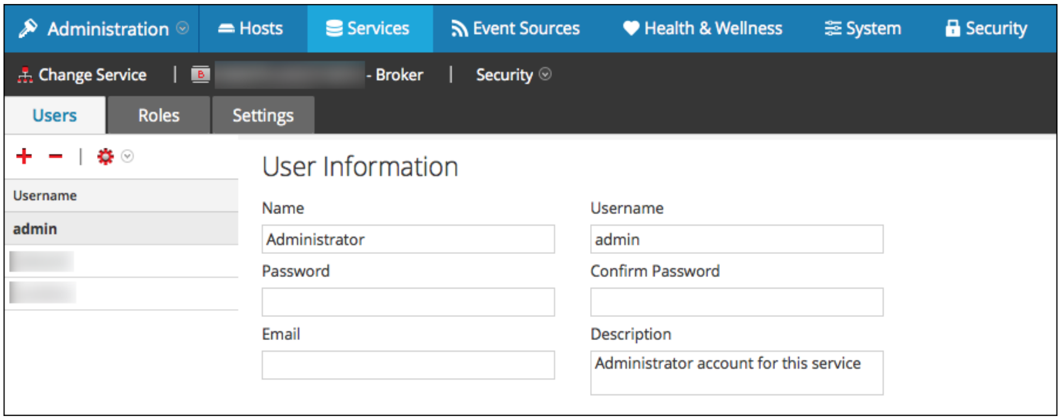
Change the **admin** password for the Security Analytics service in the Profile view. See **Change Password** in the *Security Analytics Getting Started Guide*. The password of the **admin** user does not propagate to Core services.

> **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 Security Analytics Core Services

To change the admin password for a Core service:

1. In the **Security Analytics** menu, select **Administration > Services.**
2. Select a service, and then select ⚙ > **View** > **Security**.
3. On the **Users** tab, select the **admin** user.



Username
admin
[redacted]
[redacted]

User Information

Name: Administrator

Username: admin

Password:

Confirm Password:

Email:

Description: Administrator account for this service

4. In the **Password** field, type a new admin password for the selected service.

   Note: The **Password** field cannot be empty.

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 the **Security Analytics** menu, select **Administration > 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 Security Analytics user interface. This is simply another way to perform the Security Analytics Core password change, and is not the preferred method.

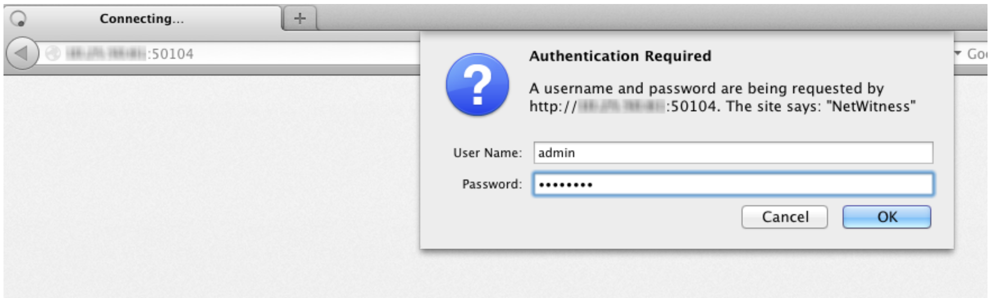
To change the admin password for the service using the REST User Interface:

1. Open a web browser, and go to the following URL:

   `<hostname>:<port>`

   where the **hostname** is the name of a Security Analytics Core service and **port** is the port used for REST communication. Here is an example for a Security Analytics Decoder: `http://10.20.30.40:50104`

   The authentication dialog is displayed.



Authentication Required

A username and password are being requested by http://[redacted]:50104. The site says: "NetWitness"

User Name: admin

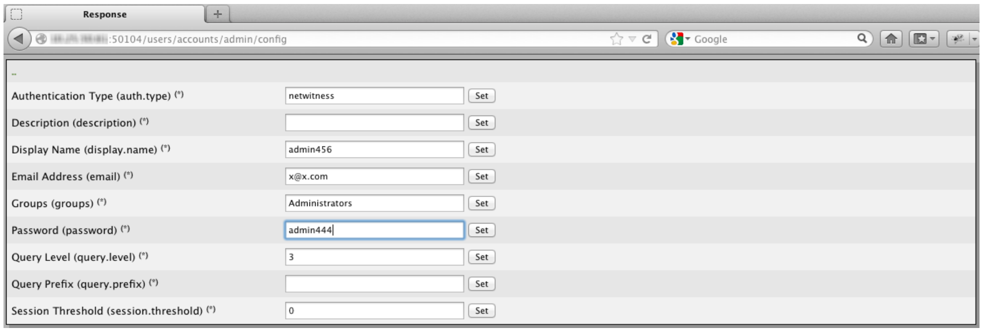
Password: ••••••••

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.



[redacted]:50104/users/accounts/admin/config

..

Authentication Type (auth.type) (*)	netwitness	Set
Description (description) (*)		Set
Display Name (display.name) (*)	admin456	Set
Email Address (email) (*)	x@x.com	Set
Groups (groups) (*)	Administrators	Set
Password (password) (*)	admin444	Set
Query Level (query.level) (*)	3	Set
Query Prefix (query.prefix) (*)		Set
Session Threshold (session.threshold) (*)	0	Set

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 Security Analytics users and sessions. Settings related to password expiration, such as password expiration period and the default number of days before user passwords expire, apply to internal Security Analytics users, but not external users.

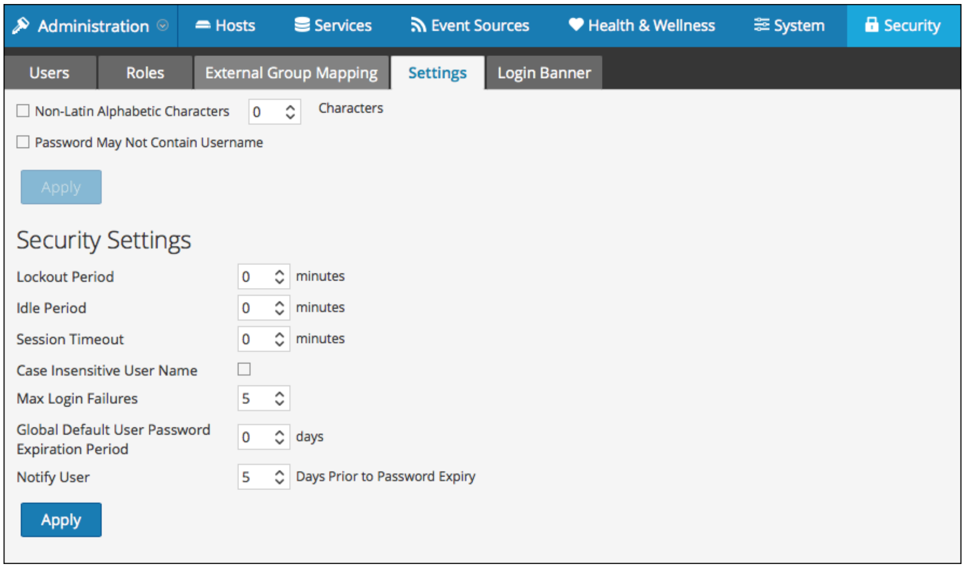
In addition to specifying the global default user expiration period, you can specify if and when internal Security Analytics users receive notification that their passwords are about to expire. The password expiration notification consists of a one-time email and password expiration messages when they log on to Security Analytics.

Configure Security Settings

1. In the **Security Analytics** menu, select **Administration > Security**.

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

2. Click the **Settings** tab.



☐ Non-Latin Alphabetic Characters 0 Characters

☐ Password May Not Contain Username

Security Settings

Lockout Period	0	minutes
Idle Period	0	minutes
Session Timeout	0	minutes
Case Insensitive User Name	☐	
Max Login Failures	5	
Global Default User Password Expiration Period	0	days
Notify User	5	Days Prior to Password Expiry

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 Security Analytics after the configured number of failed logins is exceeded. The default value is 20 minutes.

Field	Description
Idle Period	Number of minutes of inactivity before a session times out. The default value is 60. If the value is 0, the session will not timeout.
Session Timeout	The maximum duration of a user session before timing out 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.
Case Insensitive User Name	Select this option if you want the RSA Security Analytics Username field on the login screen to be case insensitive. For example, you could use Admin or admin to log on to Security Analytics.
Max Login Failures	The maximum number of unsuccessful login attempts before a user is locked out. The default value is 5
Global Default User Password Expiration Period	The default number of days before a password expires for all internal Security Analytics users. A value of zero (0) disables password expiration. For upgrades and new installations, the default value is zero (0).
Notify User <n> Days Prior to Password Expiry	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 Security Analytics. A value of zero (0) disables automatic password expiration notification. If you set the Global Default User Password Expiration Period to zero (0), users do not receive automatic password expiration notifications.

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 Security Analytics.

Step 4. (Optional) Configure External Authentication

This topic introduces the external authentication methods that Security Analytics supports.

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

Security Analytics 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
- Test External Authentication

Configure Active Directory

This topic explains how to configure Security Analytics to use Active Directory to authenticate external user logins.

When a user logs in, Security Analytics 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 **Administration** > **Security** > **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 Security Analytics. Security Analytics 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.

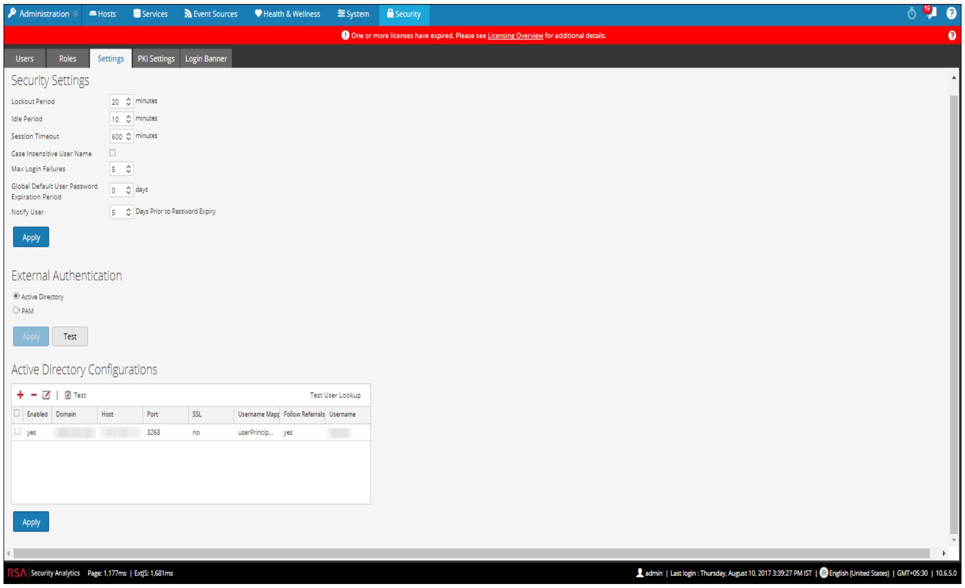
Procedures

Configure Active Directory Authentication

1. In the **Security Analytics** menu, select **Administration** > **Security**.

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

2. Click the **Settings** tab.



One or more licenses have expired. Please see Licensing Overview for additional details.

Security Settings

Lockout Period	20	minutes
Idle Period	10	minutes
Session Timeout	600	minutes
Case Insensitive User Name	□	
Max Login Failures	5	
Global Default User Password Expiration Period	0	days
Notify User	5	Days Prior to Password Expiry

External Authentication

● Active Directory
○ PAM

Active Directory Configurations

□	Enabled	Domain	Host	Port	SSL	Username Mapp	Follow Referrals	Username
□	yes	[redacted]	[redacted]	3268	no	userPrincip...	yes	[redacted]

RSA Security Analytics Page: 1,177ms | ExtJS: 1,681ms

admin | Last login : Thursday, August 10, 2017 3:39:27 PM IST | English (United States) | GMT+05:30 | 10.6.5.0

3. In the **External Authentication** section, select **Active Directory**.

   The Active Directory Configurations list is displayed in the panel so that you can add or edit a configuration.

4. When all configurations are added click **Apply**.

   The domains added to this list and enabled are automatically populated in the External Group Mapping tab so that you can map security roles to each group.

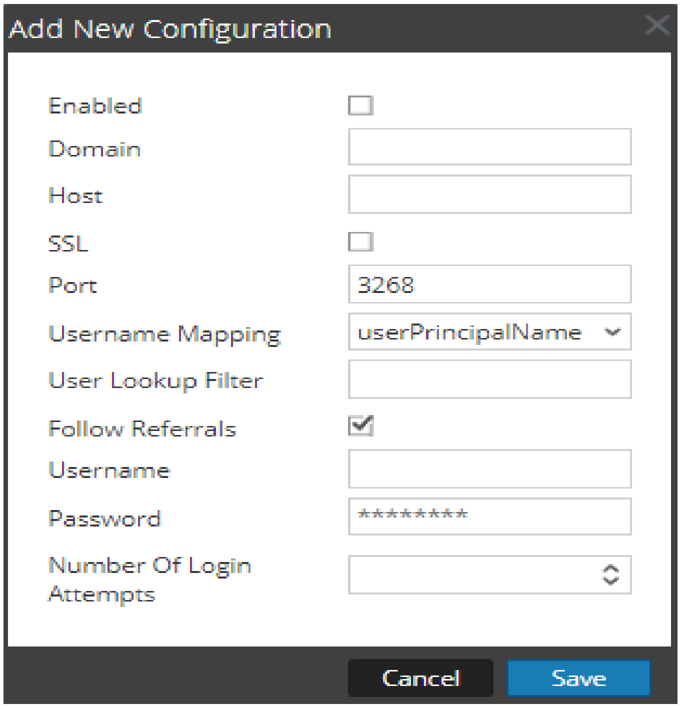
Note: To configure security roles used for Active Directory access, see Step 5. (Optional) Map User Roles to External Groups.

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.



Enabled	□
Domain	
Host	
SSL	□
Port	3268
Username Mapping	userPrincipalName
User Lookup Filter	
Follow Referrals	☑
Username	
Password	*********
Number Of Login Attempts	

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 **Use SSL** checkbox.

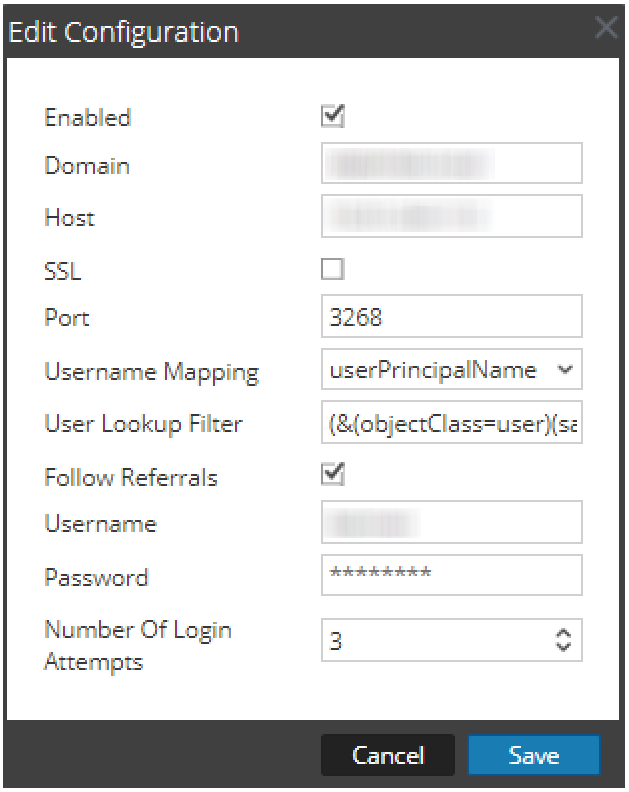
5. In the **Username Mapping** field, select the Active Directory search field to use for username mapping. You can select userPrincipalName (UPN) or sAMAccountName.

6. In the **User Lookup Filter** field, (if PKI is enabled) to find a user in the Active Directory using AD Attributes other than 'sAMAccountName' or 'userPrincipalName' you must configure the custom LDAP filter.
   For example, (&(objectClass=user)(objectClass=top)(samAccountName={username})). The {username} in the filter is replaced with the value extracted from the user certificate.
7. For sites that have multiple authentication servers, click **Follow Referrals** to enable or disable LDAP referral following for AD group lookups.
8. To provide credentials to bind to the Active Directory Service while searching Active Directory group, enter the credentials in the **Username** and **Password** fields.
9. In the **Number of Login Attempts** field, select the number of login attempts performed by Security Analytics when the AD service is unavailable.
10. 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**, click ✎.
   The Edit Configuration dialog is displayed.



Edit Configuration

Enabled ☑

Domain [redacted]

Host [redacted]

SSL □

Port 3268

Username Mapping userPrincipalName

User Lookup Filter (&(objectClass=user)(sa

Follow Referrals ☑

Username [redacted]

Password ********

Number Of Login Attempts 3

2. (Optional) Enter the **Domain**, **Host** and **Port** information for the Active Directory Service.
3. (Optional) To select SSL for this configuration, check the **Use SSL** checkbox.
4. (Optional) In the **Username Mapping** field, select the the Active Directory search field to use for username mapping.
5. (Optional) In the **User Lookup Filter** field, (if PKI is enabled) to find a user in the Active Directory using AD Attributes other than 'sAMAccountName' or 'userPrincipalName' you must configure the custom LDAP filter.
6. 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.
7. To provide credentials to bind to the Active Directory Service while searching Active Directory group, enter the credentials in the **Username** and **Password** fields.
8. In the **Number of Login Attempts** field, select the number of login attempts performed by Security Analytics when the AD service is unavailable.
9. 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.

Test an Active Directory User Lookup

To verify that the active directory user lookup method is configured correctly:

1. Under **Active Directory Configurations**, click **Test User Lookup**.

   The **Test User Lookup** dialog is displayed.
2. Enter the user name that you want to test for authentication using the current Active Directory.
3. Click **Test**.

   If the test succeeds, you can access the active directory service else you must 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 indicates that the selected configuration is deleted from the list.

Configure PAM Login Capability

This topic explains how to configure Security Analytics 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 Security Analytics without having an internal Security Analytics account, and to receive permissions or roles determined by mapping the external group to a Security Analytics 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 are Active Directory, RADIUS, or LDAP. For implementation, each authentication provider uses its own module, which is in the form of an operating system (OS) package such as pam_ldap. Security Analytics 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 operating system (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. Security Analytics 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. Security Analytics compares the results of the request to the Security Analytics External Group Mapping and if a matching group is found, the user is granted access to log on to SA 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 Security Analytics. 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, LDAP, and RADIUS. The NSS examples include Samba, LDAP, and UNIX. The PAM and NSS module combination used is determined by site needs.

> **Note:** For pre-10.4 services that use untrusted connections, all PAM users must also be configured in all Security Analytics Core services, and PAM needs to be configured on every EL6 Core host. While this document does not address configuring PAM Authentication and Users for Core services, such as Decoder and Concentrator, the steps for configuring the PAM module are the same, except that the Security Analytics Core services use a different PAM configuration file, `/etc/pam.d/netwitness`.

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 Security Analytics Server.
4. Create group mappings in Security Analytics Server.

Prerequisites

This feature is only available for EL6 based Security Analytics Version 10.4 or later.

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.

If you purchased a new host with Security Analytics 10.4 or later installed, the required rpm packages for Kerberos, LDAP, RADIUS, and Samba are installed by default.

Before beginning setup of PAM in Security Analytics, identify the group names that you will use in the External Group mapping. When mapping roles, the role in Security Analytics 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 LDAP
- PAM RADIUS
- SecurID

PAM Kerberos

Kerberos Communication Ports – TCP 88

Note: If Security Analytics Server and Security Analytics Malware Analysis share the same server, once you setup the PAM Kerberos, the Malware Analysis Samba (SMB) configuration will be disabled.

To configure PAM authentication using Kerberos:

1. If you upgraded to Security Analytics 10.6, execute the following command, otherwise skip this step:
   `yum --enablerepo=nwupdates 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.

```
[libdefaults]
 default_realm = <DOMAIN.COM>
 dns_lookup_realm = true
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

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

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

 [appdefaults]
 pam = {
   debug = true   ticket_lifetime = 36000
  renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
  }
```

3. Test the Kerberos configuration with the command:
   `kinit <user>@<DOMAIN.COM>`
   No output after entering the password indicates success.

4. Edit the Security Analytics 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 LDAP

LDAP Communication Ports - TCP 389 or TCP 636

TCP 389 can be used for both unencrypted and in most cases encrypted traffic and is usually sufficient. Most modern LDAP implementations support the `start_tls` command once connected to port 389, which upgrades the connection from an unencrypted to an encrypted state. In this instance, LDAP URIs still begin with `ldap://` even when using `start_tls`.

TCP 636 is used only in instances where the LDAP server does not support the `start_tls` command. In this case, LDAP URIs begin with `ldaps://` and the `start_tls` command is not used.

To configure PAM authentication using LDAP:

1. If you upgraded to Security Analytics 10.6, execute the following command, otherwise skip this step:
   ```
   yum --enablerepo=nwupdates install openldap-clients
   ```

2. Edit the LDAP configuration files, `/etc/pam_ldap.conf` and `/etc/openldap/ldap.conf` as shown in the following examples

> **Note:** The two LDAP configuration files serve different purposes. The **pam_ldap.conf** file is used by the PAM Module only. The **`openldap/ldap.conf`** file is used by the **`openldap`** client tools, such as **`ldapsearch`**, which is used for troubleshooting the basic LDAP communications. **Replace variables, which are delimited by <angle brackets>, with your values and omitting the angle brackets. Capitalization is required where shown.**

Sample `/etc/pam_ldap.conf` file entries

```
base <dc=domain,dc=com>
 uri ldap://<server.domain.com>
 binddn <binduser@domain.com>
 bindpw <secret>
```

```
nss_map_objectclass posixAccount user
nss_map_objectclass shadowAccount user
nss_map_attribute uid sAMAccountName
nss_map_attribute homeDirectory unixHomeDirectory
nss_map_attribute shadowLastChange pwdLastSet
nss_map_objectclass posixGroup group
nss_map_attribute uniqueMember member
pam_login_attribute sAMAccountName
pam_filter objectclass=User
```

Sample `/etc/openldap/ldap.conf` file entries

```
URI ldap://<server.domain.com>
BASE <DC=domain,DC=com>
TLS_CACERTDIR /etc/openldap/certs
```

3. (Optional) To enable secure transport for LDAP communication with peer certificate verification (more secure), add the lines shown below to `/etc/pam_ldap.conf` and `/etc/openldap/ldap.conf`:

   Lines to add to `/etc/pam_ldap.conf`:

   ```
   ssl start_tls
   tls_cacertfile /etc/openldap/certs/myca.pem
   ```

   Lines to add to `/etc/openldap/ldap.conf`:

   ```
   ssl start_tls
   tls_cacert /etc/openldap/certs/myca.pem
   ```

   `myca.pem` is a file that contains a base64-encoded PEM-format x.509 certificate for the root CA (not the issuing CA) of the certificate chain that issued the domain controller's secure LDAP certificate. Contact your Active Directory administrator to obtain this root CA certificate. The certificate file must be in PEM format.

   > **Note:** Windows domain controllers do not by default enable secure LDAP transport. They require the installation of a server certificate for Server Authentication. Obtaining and installing this certificate onto the DC is outside the scope of this document. Some guidance on this is available at https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx.

4. (Optional) To enable secure transport for LDAP communication without peer certificate add the lines shown below to `/etc/pam_ldap.conf` and `/etc/openldap/ldap.conf`:

   Lines to add to `/etc/pam_ldap.conf`

   ```
   ssl start_tls
   ```

```
tls_reqcert never
```

Lines to add to `/etc/openldap/ldap.conf`

```
ssl start_tls
tls_checkpeer no
```

5. To test the LDAP configuration, enter the following command:
   `ldapsearch -x -D <user>@<domain.com> -W`

6. To perform an advanced test or to troubleshoot your bind user, connect as your Bind User (example Mike Cool) and search for the user, see what the user's distinguished name (DN) is and use that value as the `binddn` in `pam_ldap.conf`, for example:
   a. **`ldapsearch -b "dc=domain,dc=com" -D mcool@domain.com -h server.domain.com -W "(cn=Cool*)" |grep Cool`**
      The grep will hide the password prompt (-W)
   b. Type the password and press ENTER.

7. Edit the Security Analytics 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_ldap.so`

This completes the configuration for PAM LDAP. 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 Security Analytics Server to your RADIUS Server's Client list and configure a shared secret. For instructions, see Add a RADIUS Client and Associated Agent.

To configure PAM authentication using RADIUS:

1. If you upgraded to Security Analytics 10.6, execute the following command, otherwise skip this step:
   `yum --enablerepo=nwupdates 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 Security Analytics 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
```

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 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. If you upgraded to Security Analytics 10.6, execute the following command to check if the PAM RADIUS package is installed:

   rpm -qa | grep pam_radius_auth

   Example:
   ```
   [root@ ~]# rpm -qa | grep pam_radius_auth
              pam_radius_auth-1.3.17-1.x86_64
              [root@ ~]#
   ```

   If the `pam_radius_auth package` is not available then use the following command to install the required PAM RADIUS package:

   yum --enablerepo=nwupdates 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` & `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 Security Analytics 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`)

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.

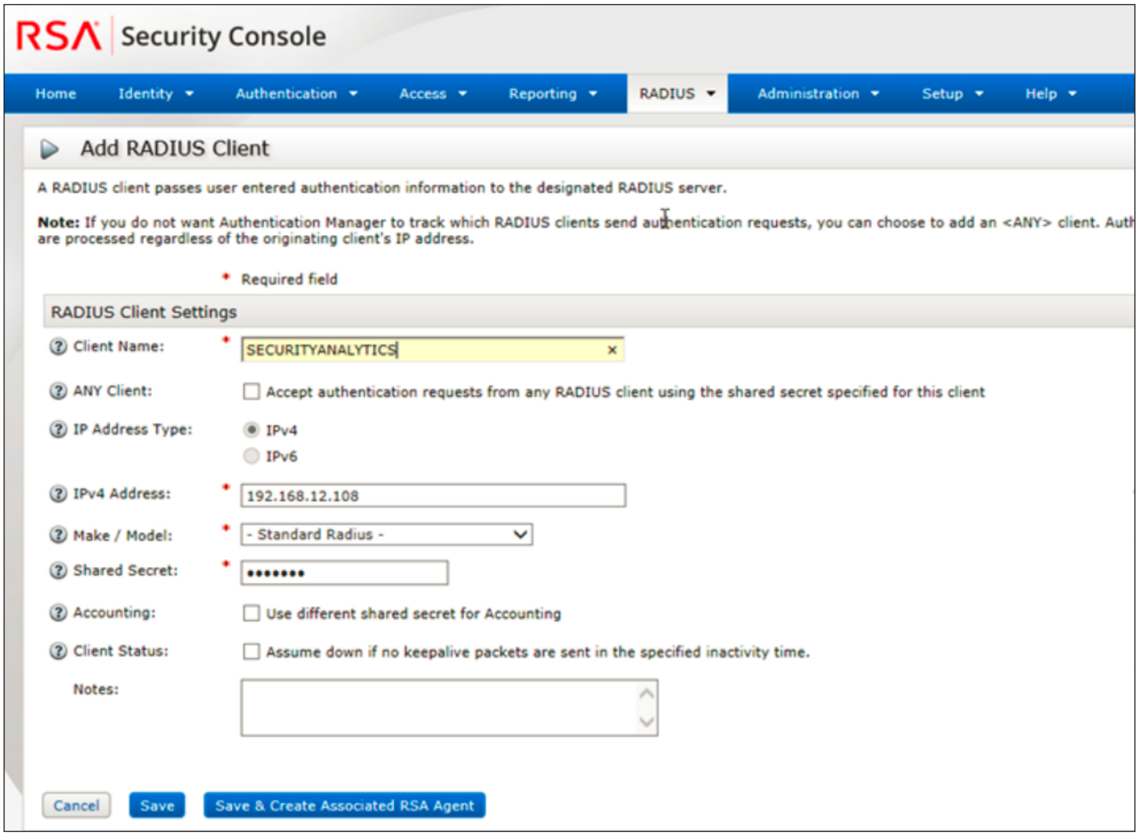
To add a RADIUS Client and Associated Agent:

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.



Add RADIUS Client

A RADIUS client passes user entered authentication information to the designated RADIUS server.

Note: If you do not want Authentication Manager to track which RADIUS clients send authentication requests, you can choose to add an <ANY> client. Auth
are processed regardless of the originating client's IP address.

* Required field

RADIUS Client Settings

Client Name: * SECURITYANALYTICS

ANY Client: □ Accept authentication requests from any RADIUS client using the shared secret specified for this client

IP Address Type: ● IPv4 ○ IPv6

IPv4 Address: * 192.168.12.108

Make / Model: * - Standard Radius -

Shared Secret: * •••••••

Accounting: □ Use different shared secret for Accounting

Client Status: □ Assume down if no keepalive packets are sent in the specified inactivity time.

Notes:

3. In RADIUS Client Settings, provide the following information:

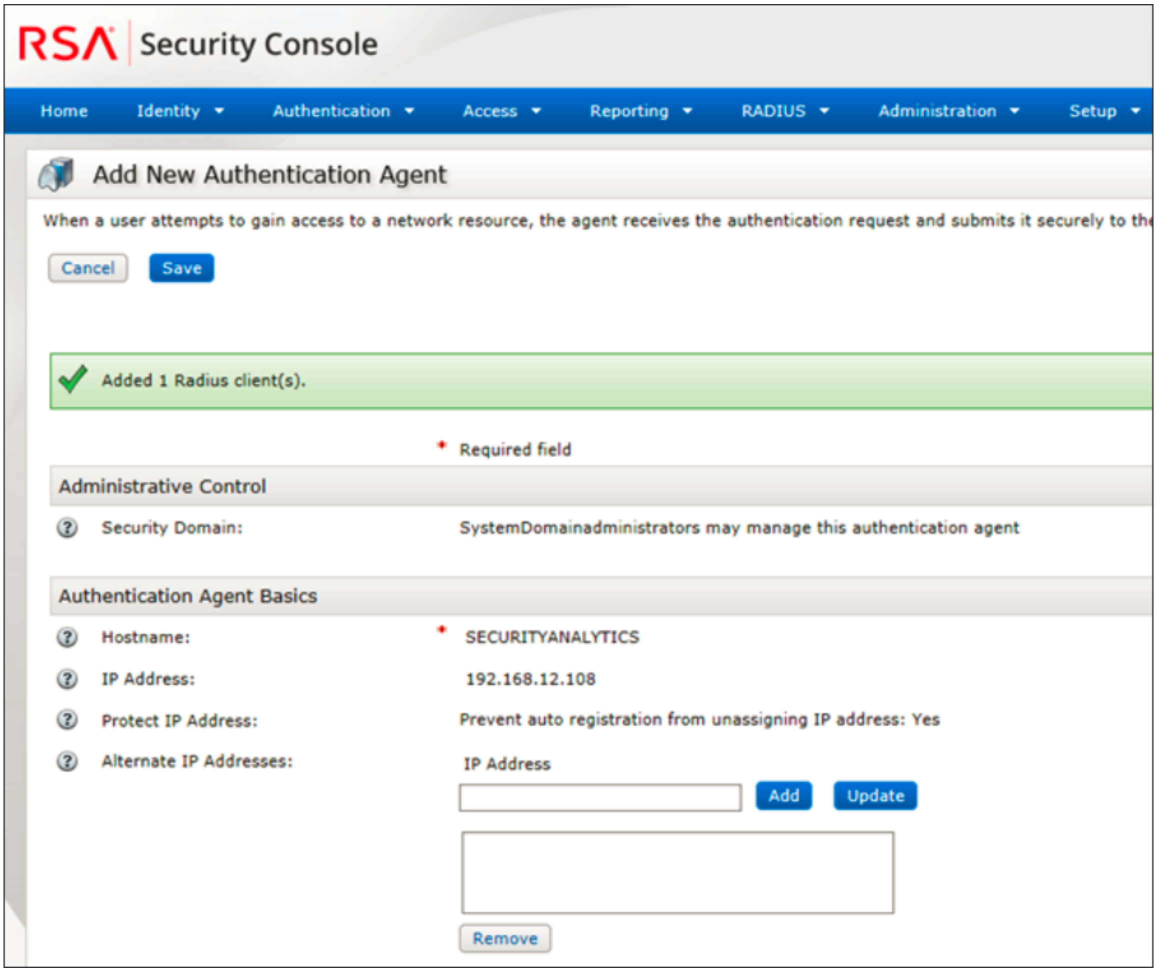
   a. In the **Client Name** field, enter the name of the client, for example, SECURITY ANALYTICS.

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**.



Add New Authentication Agent

When a user attempts to gain access to a network resource, the agent receives the authentication request and submits it securely to the

Added 1 Radius client(s).

* Required field

Administrative Control

Security Domain: SystemDomainadministrators may manage this authentication agent

Authentication Agent Basics

Hostname: * SECURITYANALYTICS

IP Address: 192.168.12.108

Protect IP Address: Prevent auto registration from unassigning IP address: Yes

Alternate IP Addresses: IP Address

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. All Security Analytics core services in the deployment must be running at a minimum version 10.4.0. Security Analytics 10.3.x or earlier is not supported.
2. Trusted connections must be enabled and functioning between Security Analytics and Security Analytics 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 **Security Analytics server**:
   a. Copy configuration file from Authentication Manager and customize it.
   b. Install the PAM SecurID Module.
3. Test connectivity and authentication.

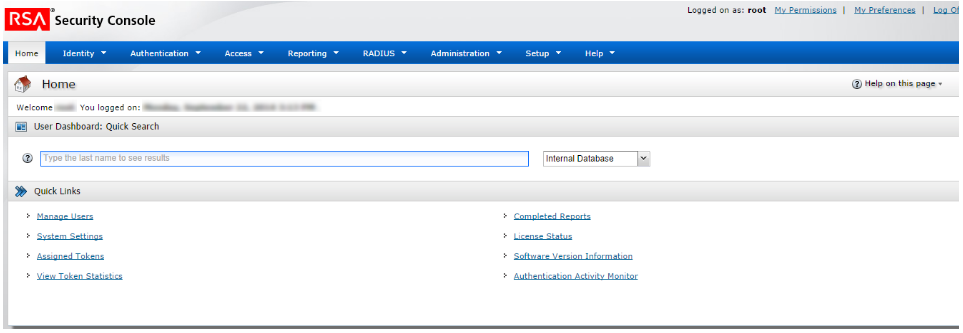
Then follow the remaining procedures in the sections that follow:

- Configure NSS.
- Enable PAM in Security Analytics.
- Configure group mappings in Security Analytics server.

To configure Authentication Manager:

1. Log on to RSA Authentication Manager.

   The Security Console is displayed.



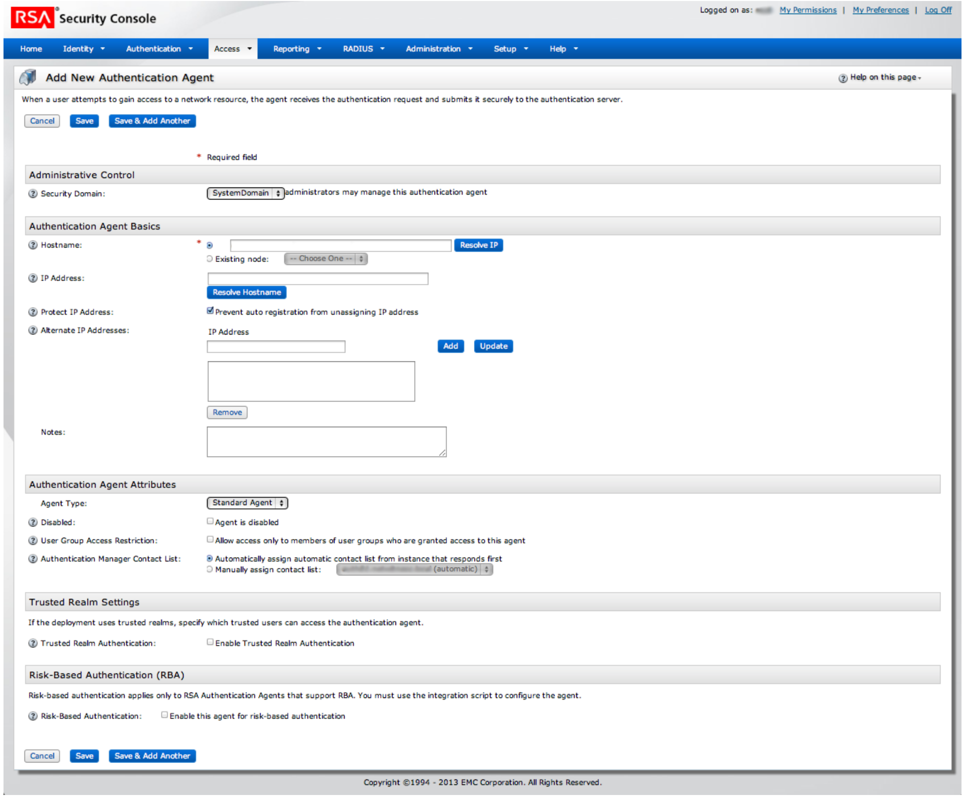
Logged on as: root

Welcome [redacted] You logged on: [redacted]

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

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

   The Add New Authentication Agent page is displayed.



Add New Authentication Agent

When a user attempts to gain access to a network resource, the agent receives the authentication request and submits it securely to the authentication server.

* Required field

Administrative Control

Security Domain: SystemDomain administrators may manage this authentication agent

Authentication Agent Basics

Hostname: * ●
○ Existing node: -- Choose One --

IP Address:

Protect IP Address: ☑ Prevent auto registration from unassigning IP address

Alternate IP Addresses: IP Address

Notes:

Authentication Agent Attributes

Agent Type: Standard Agent

Disabled: □ Agent is disabled

User Group Access Restriction: □ Allow access only to members of user groups who are granted access to this agent

Authentication Manager Contact List: ● Automatically assign automatic contact list from instance that responds first
○ Manually assign contact list: [redacted] (automatic)

Trusted Realm Settings

If the deployment uses trusted realms, specify which trusted users can access the authentication agent.

Trusted Realm Authentication: □ Enable Trusted Realm Authentication

Risk-Based Authentication (RBA)

Risk-based authentication applies only to RSA Authentication Agents that support RBA. You must use the integration script to configure the agent.

Risk-Based Authentication: □ Enable this agent for risk-based authentication

Copyright ©1994 - 2013 EMC Corporation. All Rights Reserved.

3. In the **Hostname** field, type the hostname of the Security Analytics server.

4. Click **Resolve IP**.

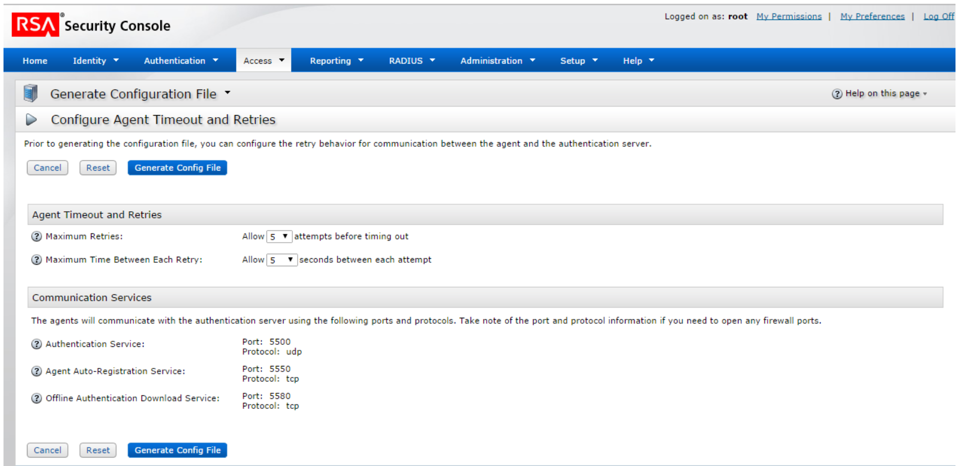
   The IP address of the Security Analytics server is automatically displayed in the **IP Address** field.

5. Keep the default settings and click **Save**.

6. Generate a configuration file.

   Click **Access > Authentication Agents > Generate Configuration File**.

The Generate Configuration File page is displayed.


RSA Security Console
Logged on as: root My Permissions | My Preferences | Log Off
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Help on this page
Cancel Reset Generate Config File

Generate Configuration File

Configure Agent Timeout and Retries

Prior to generating the configuration file, you can configure the retry behavior for communication between the agent and the authentication server.

Agent Timeout and Retries

Maximum Retries: Allow 5 attempts before timing out

Maximum Time Between Each Retry: Allow 5 seconds between each attempt

Communication Services

The agents will communicate with the authentication server using the following ports and protocols. Take note of the port and protocol information if you need to open any firewall ports.

Authentication Service: Port: 5500 Protocol: udp

Agent Auto-Registration Service: Port: 5550 Protocol: tcp

Offline Authentication Download Service: Port: 5580 Protocol: tcp

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:

Note: In version 10.4 or later, OVAs and installation ISOs pre-install the SecurID package. If this applies to your environment, skip step 5 in the below procedure.

1. On the Security Analytics server, make a directory:

   mkdir /var/ace

2. On the Security Analytics 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 Security Analytics 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 Security Analytics server PAM configuration file, **/etc/pam.d/securityanalytics** by adding this line:

   auth required pam_securid.so

   If the file does not exist, create it and add this 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:** 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 whole path must have -rw------- root root permission.

> **Note:** If the PAM SecurID setup is not complete, it may crash the Jetty server and Security Analytics UI will not be displayed. You must wait till 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/63bit/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,

   Click **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
   ```

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

Choose an NSS Service

There are three NSS service options: Samba, LDAP, and UNIX. There are advantages and disadvantages to all three.

NSS Samba Pros	NSS Samba Cons
Purpose built for Active Directory	Cannot be used with non-AD back-ends
Minimal to no configuration must be performed in Active Directory	Potentially more difficult to configure and troubleshoot
No special user accounts needed	Requires the SA Server machine be joined to the Active Directory Domain
	Uses many ports to communicate with Active Directory; more difficult to implement across firewalls and proxies

NSS LDAP Pros	NSS LDAP Cons
Basic configuration is simpler	May require additional configuration and roles inside of Active Directory
Can communicate with any LDAP implementation	Requires configuration of an LDAP bind account
Uses a single TCP port for communication - easier to work with firewalls and proxies	More difficult to enable secure transport unless configured to not validate server certificates
Does not require joining SA host to AD domain	

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 SA Server console.

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

NSS Samba

Note: If Security Analytics Server and Security Analytics Malware Analysis share the same service, once you setup NSS Samba, the Malware Analysis Samba (SMB) configuration will be disabled.

AD Winbind Communication Ports

The following ports are the minimum ports internal testing indicates should be open to permit NSS Samba functionality. These are provided only as a reference.

TCP 88 - Kerberos
TCP 139 - Netbios
TCP 389 - LDAP
UDP 53 - DNS
UDP 88 - Kerberos
UDP 389 - LDAP

Additional ports may be needed, depending on site-specific requirements of implementation. See the following article for information on all ports Active Directory communication may require: http://technet.microsoft.com/en-us/library/dd772723%28ws.10%29.aspx

To configure NSS Samba:

1. Edit the Samba configuration file, `/etc/samba/smb.conf`, as follows. Replace variables, which are delimited by <angle brackets>, with your values and omitting the angle brackets. Capitalization is required where shown.

   ```
   [global]
    workgroup = domain
    netbios name = <SA_APPLIANCE_HOSTNAME>
    password server = <ADSERVER.DOMAIN.COM>
    realm = <DOMAIN.COM>

    local master = no
    security = ads
    syslog only = yes
    log file = /var/log/samba/log.%m
    max log size = 5120
    idmap config * : range = 16777216-33554431
    template shell = /bin/bash
    winbind use default domain = true
    winbind offline logon = false
    winbind enum groups = yes
   ```

2. To enable and start the Windows binding service, `winbind`, enter the following commands:

   ```
   chkconfig winbind on
   service winbind start
   ```

3. Edit the NSS configuration file, `/etc/nsswitch.conf`. Update only the below 2 entries and leave the rest all default:

   ```
   passwd:      files winbind
   group:       files winbind
   ```

4. To join the Domain, enter the following command:

   ```
   net ads join -U <DomainAdminUser>
   ```

5. To store the Domain Controller SID, enter the following command:

   ```
   net rpc getsid -S <SERVER.DOMAIN.COM>
   ```

6. Test NSS functionality as described in the *Test NSS Functionality* section.

7. When you have confirmed that NSS is working properly from the command line, to reboot the host for the NSS changes to take effect, enter the following command.

   ```
   reboot
   ```

To troubleshoot NSS Samba:

To confirm whether NSS Winbind is able to communicate successfully with Active Directory:

1. Enter the following commands:

   `wbinfo -u` to return a list of AD users

   `wbinfo -g` to return a list of AD groups

2. If neither command succeeds, run `winbind` in console debug mode by entering the following commands:

   ```
   service winbind stop
   winbindd -S -F -d <optional debugleve 0-10>
   ```

3. From a separate ssh session, repeat step 1 and watch the `winbindd` output for any indication of the problem.

   Increase `winbindd` debugging verbosity as needed.

4. Make any necessary adjustments to `/etc/samba/smb.conf`.

5. In the `winbindd` debug window from step 2, stop `winbindd` by typing `CTRL-C`.

   Repeat steps 1 and 2 and continue troubleshooting until the `wbinfo` commands succeed.

6. Once the `wbinfo` commands succeed, use the `getent` commands from the Testing NSS Functionality section of this guide to test NSS.

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

7. When `getent` succeeds, stop the command line `winbindd` by typing `CTRL-C` and enter the following command to start the service daemon:

   ```
   service winbind start
   ```

If `wbinfo -g` succeeds from the command line but search for external group mapping does not display any Active Directory groups:

1. Add the following line to to `/etc/samba/smb.conf`:

   ```
   allow trusted domains = no
   ```

2. Type **`service winbind restart`**.

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

NSS LDAP

Note: These instructions require all Active Directory PAM user and NSS group objects to have their `uidNumber` and `gidNumber` attributes set to UNIX-style UID and GID numbers in order to be used by NSS LDAP. Older Active Directory schemas may not have these attributes by default. Newer AD schemas may have these attributes but they may not be defined in each object. Correctly configuring these attributes is beyond the scope of this document. Contact your Active Directory administrator to have these attributes defined for your PAM users and NSS groups.

An LDAP bind user must be created in Active Directory in order for NSS to be used. This user should be configured to not have its password expire. Because these credentials must be specified to the NSS LDAP service in plaintext, the permissions of `/etc/nslcd.conf` should be left at their default of 600 so the file cannot be read by system users other than root.

LDAP Communication Ports - TCP 389 or TCP 636

TCP 389 can be used for both unencrypted and in most cases encrypted traffic and is usually sufficient. Most modern LDAP implementations support the `start_tls` command once connected to port 389, which upgrades the connection from an unencrypted to an encrypted state. In this instance, LDAP URIs still begin with `ldap://` even when using `start_tls`.

TCP 636 is only used in instances where the LDAP server does not support the `start_tls` command. In this instance, LDAP URIs begin with `ldaps://` and the `start_tls` command is not used.

To configure the NSS module for LDAP with Active Directory:

1. Obtain the `nss-pam-ldapd` package from the SMCUPDATE repository or from the Security Analytics Server Updates Repository if the server is synchronized with SMCUPDATE. This requires a configured Live Account in Security Analytics.

2. To install the package, do one of the following:

   a. To install directly from SMCUPDATE, enter the following command:
   `yum --enablerepo=sa install nss-pam-ldapd`

   b. To install from the Security Analytics Updates Repository, enter the following command:
   `yum --enablerepo=nwupdates install nss-pam-ldapd`

3. Edit `/etc/nslcd.conf` to include the lines below, ensuring that all existing lines in the file are first commented out using a hash mark # at the beginning of the line:

```
 #see note in NSS LDAP Communication Ports section for guidance on
using ldap:// or ldaps://
 uri ldap://<ldapServerHost>/
 base dc=<yourDomain>,dc=<com>
 binddn <ldapBindUser@yourdomain.com>
 bindpw <bindPassword>
 bind_timelimit 30
 timelimit 30
 idle_timelimit 3600
 pagesize 1000
 referrals off
 filter passwd (&(objectClass=user)(!(objectClass=computer))
(uidNumber=*)(unixHomeDirectory=*))
 map    passwd uid              sAMAccountName
 map    passwd homeDirectory    unixHomeDirectory
 map    passwd gecos            displayName
 filter shadow (&(objectClass=user)(!(objectClass=computer))
(uidNumber=*)(unixHomeDirectory=*))
 map    shadow uid              sAMAccountName
 map    shadow shadowLastChange pwdLastSet
 filter group  (objectClass=group)
 map    group  uniqueMember     member
 uid nslcd
 gid ldap
```

4. (Optional) To enable secure transport for LDAP communication with peer certificate verification (more secure), add these lines to `/etc/nslcd.conf`:
   `ssl start_tls`

```
tls_cacert /etc/openldap/certs/myca.pem
```

`myca.pem` is a file that contains a base64-encoded PEM-format x.509 certificate for the root CA (not the issuing CA) of the certificate chain that issued the domain controller's secure LDAP certificate. Contact your Active Directory administrator to obtain this root CA certificate. The certificate file must be in PEM format.

> **Note:** Windows Domain Controllers do not by default enable secure LDAP transport. They require the installation of a server certificate for Server Authentication. Obtaining and installing this certificate onto the DC is outside the scope of this document. Some guidance on this is available from this URL:
> https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

5. (Optional) To enable secure transport for LDAP communication without peer certificate add these lines to `/etc/nslcd.conf`:
   ```
   ssl start_tls
   tls_reqcert never
   ```
6. Edit the NSS configuration file `/etc/nsswitch.conf`. Update only the below two entries and leave the rest at their default values:
   ```
   passwd:files ldap
   group:files ldap
   ```
7. To enable and start the NSLCD service, enter these commands:
   ```
   chkconfig nslcd on
   service nslcd start
   ```
8. Test NSS functionality using guidance in the *Test NSS Functionality* section. If NSS tests fail, troubleshoot NSS LDAP as described in *Troubleshoot NSS LDAP*.
9. When you have confirmed that NSS is working properly from the command line, reboot the host for the NSS changes to take effect.
   ```
   reboot
   ```

To troubleshoot NSS LDAP:

1. To troubleshoot NSS LDAP, first stop the nslcd service by entering the following command:
   ```
   service nslcd stop
   ```
2. To output troubleshooting and status information from the service to the console, run the nslcd service in debug mode from the command line.
   ```
   nslcd -d
   ```

3. (Optional) To increase debug verbosity, add an additional d multiple times to the end of nslcd -d, for example, enter the following command:
   ```
   nslcd -ddd
   ```
4. From a separate ssh session, use the `getent` commands from the Testing NSS Functionality section of this guide to test NSS. Watch the debug output from nslcd for any indications of where the failure is occurring. Increase nslcd debugging verbosity as needed.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
5. Make any necessary adjustments to `/etc/nslcd.conf` based on the output of step 2 or 3.
6. In the nslcd debug window from step 2 or 3, stop `nslcd` with `CTRL-C`. Repeat step 2 or 3 and continue troubleshooting until the `getent` command succeeds.
7. When `getent` succeeds, stop the command line `nslcd` and start the service daemon:
   ```
   service nslcd start
   ```

Common problems may include:

- LDAP secure transport SSL certificate not installed on LDAP/AD server.
- CA certificate verification failed – comment out the `tls_cacert` line in `/etc/nslcd.conf` and instead try `tls_reqcert never`. If it succeeds, you know that certificate verification that is failing.
  - Root CA certificate is not in PEM format.
  - Using issuing CA certificate rather than root CA certificate.
  - LDAP server's SSL certificate name does not match its hostname.
- Incorrect base DN.
- LDAP bind user or password is not specified correctly.
- Incorrectly specifying `ldaps://` instead of `ldap://` in `uri` line of `/etc/nslcd.conf`. `ldaps://` should only be used when using LDAPS but not using the `start_tls` command.
- Active Directory users and groups do not have `uidNumber` or `gidNumber` attributes set.
- Network firewall is blocking communications.
- LDAP server hostname specified cannot be resolved.
  - Incorrect DNS settings in `/etc/resolv.conf`.
  - Bad hostname specified in `uri` line of `/etc/nslcd.conf`.

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

Test NSS Functionality

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

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

Output should be similar to:

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

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

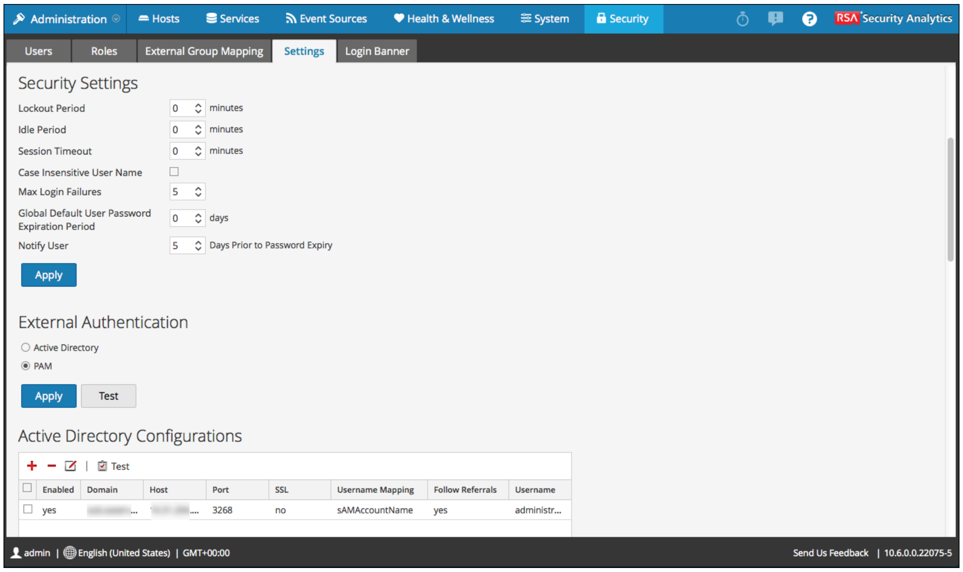
- If neither command produces output, NSS is not working properly for external authorization. Refer to the troubleshooting guidance for your NSS module provided in this document.
- If `getent` commands succeed and authentication success is confirmed in `/var/log/secure` but Security Analytics still fails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

Proceed to the next section, Enable PAM in Security Analytics server.

Enable PAM in Security Analytics Server

1. Log on to Security Analytics and in the Security Analytics menu, select **Administration** > **Security**.
   The Administration Security view is displayed with the Users tab open.
2. Click the **Settings** tab.

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



Security Settings

Lockout Period	0 minutes
Idle Period	0 minutes
Session Timeout	0 minutes
Case Insensitive User Name	□
Max Login Failures	5
Global Default User Password Expiration Period	0 days
Notify User	5 Days Prior to Password Expiry

External Authentication

○ Active Directory
● PAM

Active Directory Configurations

□	Enabled	Domain	Host	Port	SSL	Username Mapping	Follow Referrals	Username
□	yes	[redacted]	[redacted]	3268	no	sAMAccountName	yes	administr...

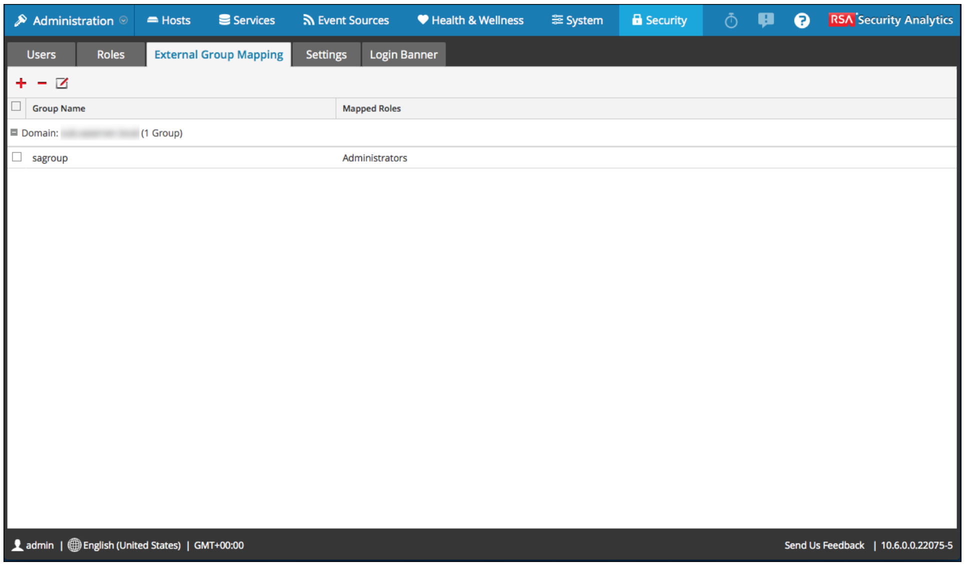
admin | English (United States) | GMT+00:00

PAM is enabled, and Active Directory is automatically disabled. The Active Directory configuration settings are stored and hidden. Perform a test authentication with the PAM configuration, For instructions, see Test External Authentication.

Proceed to the final section, Create Group Mappings in Security Analytics server.

Create Group Mappings in Security Analytics Server

1. In the Security view, click the **External Group Mapping** tab.



□	Group Name	Mapped Roles
⊟	Domain: [redacted] (1 Group)	
□	sagroup	Administrators

admin | English (United States) | GMT+00:00

2. Click + to Add a Role Mapping.

   The Add Role Mapping page is displayed.

3. Map the external group names to the appropriate Security Analytics roles as described in Step 5. (Optional) Map User Roles to External Groups.

   The external group name and the Security Analytics role name must match.

   For example, Analysts and Analysts but not Analysts and Analyst.

Test External Authentication

This topic explains how to test the currently enabled External Authentication method in Security Analytics.

When a user logs in, Security Analytics first attempts to authenticate locally. If no local user is found, and External Authentication configuration using Active Directory or PAM is enabled, an attempt is made to authenticate externally. You can test the currently enabled external authentication method in the **Administration** > **Security** > **Settings** tab.

Procedure

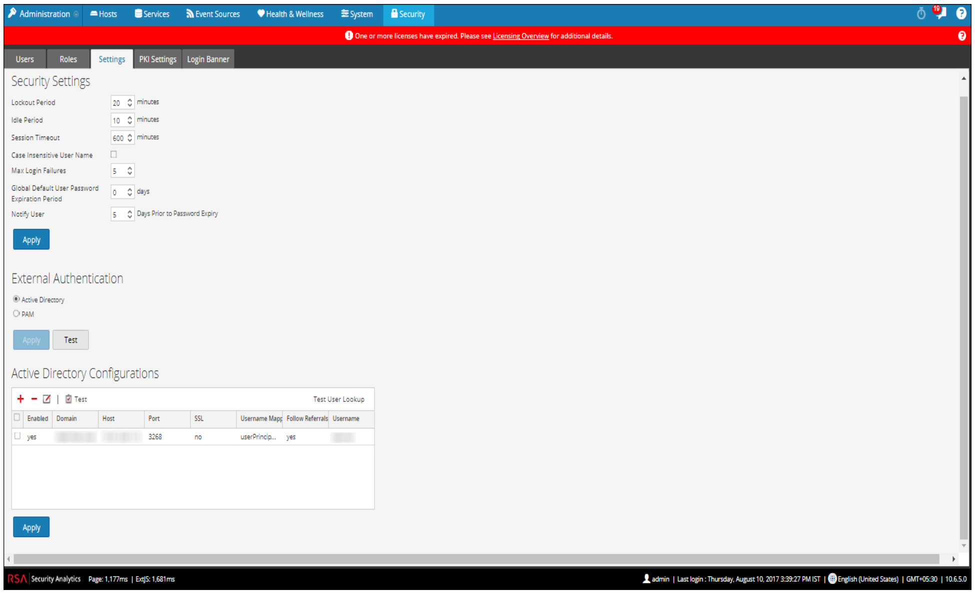
To test external authentication:

1. In the **Security Analytics** menu, select **Administration > Security**.

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

2. Click the **Settings** tab.

3. Under **External Authentication**, select **Active Directory** or **PAM**.



One or more licenses have expired. Please see Licensing Overview for additional details.

Security Settings

Lockout Period	20	minutes
Idle Period	10	minutes
Session Timeout	600	minutes
Case Insensitive User Name	□	
Max Login Failures	5	
Global Default User Password Expiration Period	0	days
Notify User	5	Days Prior to Password Expiry

External Authentication

● Active Directory
○ PAM

Active Directory Configurations

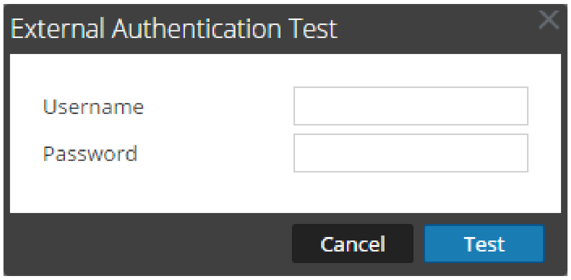
□	Enabled	Domain	Host	Port	SSL	Username Mapp	Follow Referrals	Username
□	yes	[redacted]	[redacted]	3268	no	userPrincip...	yes	[redacted]

Page: 1,177ms | ExtJS: 1,681ms

admin | Last login: Thursday, August 10, 2017 3:39:27 PM IST | English (United States) | GMT+05:30 | 10.6.5.0

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

   The **External Authentication Test** dialog is displayed.



External Authentication Test

Username

Password

5. Enter the user name and password that you want to test for authentication using the current Active Directory or PAM configuration.

   > **Note:** If you are using RSA Authentication Manager as your external authentication component, you must enter the Passcode in the **Password** field.

6. Click **Test**.

   The external authentication method is tested to ensure connectivity.

7. If the test does not succeed, review and edit the configuration (see Configure Active Directory or Configure PAM Login Capability.

Step 5. (Optional) Use Custom Server Certificate

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

Supported Certificate Formats

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

- For server certificate with its private key:
  - pkcs12 or .p12
  - jks
  - pfx
- For trusted CA certificate:
  - pkcs12 or .p12
  - jks
  - pfx
  - pem
  - crt
  - der
  - cer

Note: The .pfx, .p12, .jks are containers that can contain one or more private keys and its chains or certificates. PEM is a BASE64 encoded certificate that can contain multiple certificates.

Note: The alias name for a Security Analytics server certificate cannot contain the following Brace Characters: [ ] { } ( ) < > or the characters & (ampersand) ! (exclamation point) or | (pipe).

Procedures

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

The CSR can be submitted to the Certificate Authority (CA) Server to get the Server Certificate based on the CSR created. Once the certificate is created, these steps will help you to package the Private Key and the Signed Certificate that can be uploaded to Security Analytics Server to be used as a Server Certificate. If a Server Certificate has already been created (along with its private key), you can skip these steps and upload the certificate to the Security Analytics Server.

Perform the following steps to create a CSR for Jetty Certificate:

1. Change the directory to /root:

   ```
   cd /root
   ```

2. Create a new directory:

   ```
   mkdir sa_pki_server_cert
   ```

3. Change the directory to the newly created directory:

   ```
   cd sa_pki_server_cert
   ```

4. Create a Private Key of 2048 Bits:

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

5. Create a CSR:

   ```
   openssl req -new -nodes -out server_cert_request.csr -newkey rsa:4096
   -keyout sa_server_pki_private_key.key -config <ssl_conf_file>
   ```

   And, the ssl_conf_file (for example, openssl.cnf), contains:

   ```
   subjectAltName = @alt_names
   ```

   In the `alt_names` section, provide the domain names that you want to use with SSL.

   For example,

   `DNS.1 = <domain1>`

   `DNS.2 = <domain2>` and so on.

6. Check that the CSR and Private Key match.

   ```
   openssl req -noout -modulus -in server_cert_request.csr | openssl md5
   openssl rsa -noout -modulus -in sa_server_pki_private_key.key |
   ```

```
openssl md5
```

An example output is:

```
[root@ABCD open_ssl_test]# openssl rsa -noout -modulus -in server_
private.key | openssl md5
(stdin)= 88df3d1ea5b2f411712b96d2ed4a72f5
[root@ABCD open_ssl_test]# openssl req -noout -modulus -in server_
cert_request.csr | openssl md5
(stdin)= 88df3d1ea5b2f411712b96d2ed4a72f5
```

> **Note:** Ensure you make a note of both the stdin's.

7. Submit the CSR to a CA and get a signed certificate.

8. Copy the Certificate in PEM format to the newly created directory:
   ```
   /root/sa_pki_server_cert/signed_certificate.pem
   ```

9. Check that the certificate that you receive from CA has the correct public key and it matches the above two outputs. If they do not match, you might have omitted the previous steps.
   ```
   openssl x509 -noout -modulus -in certificate.crt | openssl md5
   ```

   > **Note:** You can use the **xca** tool to complete these steps.

   For example:

   ```
   [root@ABCD open_ssl_test]# mv test.crt certificate.crt
   [root@ABCD open_ssl_test]# openssl x509 -noout -modulus -in
   certificate.crt | openssl md5
   (stdin)= 3e2f4bbd1f32ae097902afcc1893089e
   [root@ABCD open_ssl_test]# openssl rsa -noout -modulus -in sa_
   server_pki_private_key.key | openssl md5
   (stdin)= 3e2f4bbd1f32ae097902afcc1893089e
   [root@ABCD open_ssl_test]# openssl req -noout -modulus -in
   server_cert_request.csr | openssl md5
   (stdin)= 3e2f4bbd1f32ae097902afcc1893089e
   ```

10. Copy the Private Key and Certificate to a Key Store.
    ```
    openssl pkcs12 -export -descert -name <myservercert> -in signed_
    certificate.pem -inkey sa_server_pki_private_key.key -out
    keystore.p12
    ```

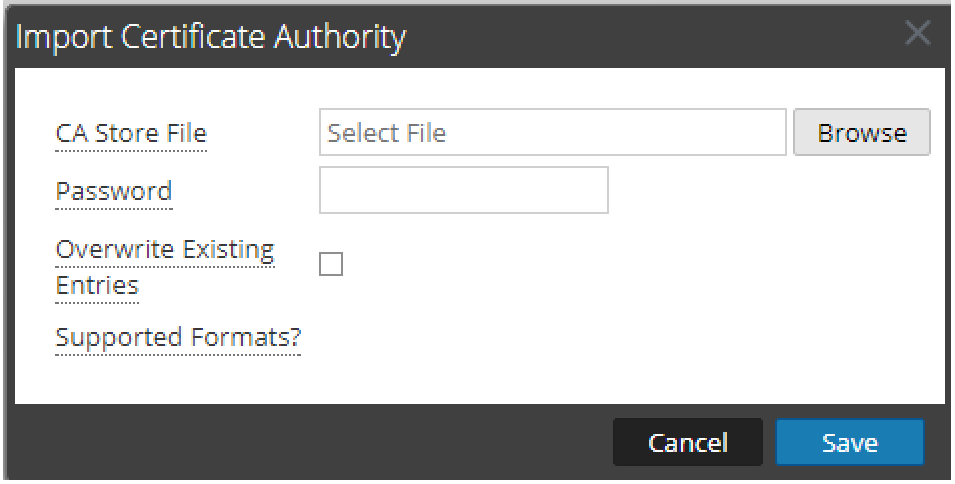
11. Provide a password, for example **sa**, to the Key Store.

Import Trusted CAs

1. In the **Security Analytics** menu, select **Administration** > **Security.**
   The Security view is displayed with the **Users** tab open.

2. Click the **PKI Settings** tab.

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



4. In the **CA Store File** field, click **Browse** and select the certificate or certificate store.

5. In the **Password** field, enter the password of the certificate or certificate store.

   Note: The password is applicable only for .pkcs12 or .p12, .pfx, and .jks certificate store formats.

6. If you already have an existing CA file with the same name as the one that you are importing, and you want to overwrite it and take the new CA file, select the **Overwrite Existing Entries** checkbox.

7. Click **Save**.
   The CA certificate is successfully added to the Security Analytics Trusted CAs store.

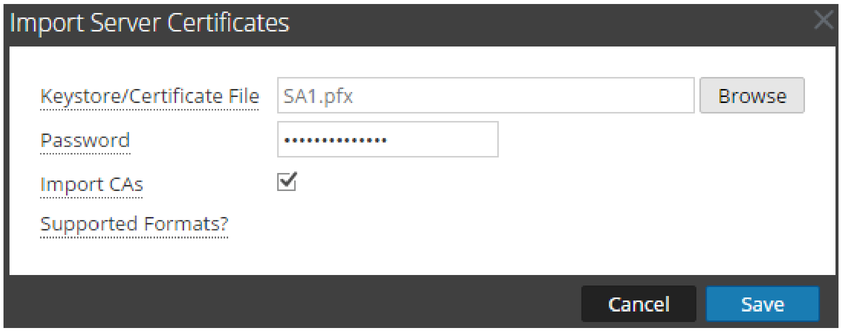
Import SA Server Certificate with its Private Key

1. In the **Security Analytics** menu, select **Administration** > **Security.**
   The Security view is displayed with the **Users** tab open.

2. Click the **Settings** tab.

3. In the **Server Certificates** section, click ✚.

   The Import Server Certificates dialog is displayed.



Import Server Certificates

Keystore/Certificate File: SA1.pfx

Password: ••••••••••••••

Import CAs ☑

Supported Formats?

4. In the **Keystore/Certificate File** field, click **Browse** and select the certificate store.

5. In the **Password** field, enter the password of the certificate store.

6. (Optional) If the user certificate and Security Analytics server certificate are issued by the same CA, select the **Import CAs** checkox.

7. Click **Save.**

   The Security Analytics server certificate with its private key is successfully added to Security Analytics.

Note: You can import multiple server certificates with its private keys.

Note: The Import Server Certificates dialog may not close on some browsers, however, the import will be successful. To view the imported certificate, refresh the page.

8. To specify a default server certificate, select a certificate and click **Use as Server Certificate**.

   The selected server certificate is highlighted in red.

9. You must SSH the Security Analytics server and run the following command:

   ```
   puppet agent -t
   ```

   This will automatically update the ***jetty-ssl.xml*** file with the appropriate server certificate.

10. Restart the Jetty service for changes to take effect.

Step 6. (Optional) Configure PKI Authentication

To configure PKI authentication, see Configure PKI Authentication.

Step 7. (Optional) Create a Customized Login Banner

This topic provides instructions for creating a login banner that is displayed before users log on to Security Analytics and the server title prefix that is displayed on the title bar when you log on to Security Analytics.

You can create and enable a customized banner asking users to agree to conditions before logging on. Users who do not agree are not able to log on. The server title prefix differentiates the Security Analytics server of the current tab, when you have deployed multiple Security Analytics in your system. This prefix will be prepended in the title on each page of Security Analytics server .

Create and Enable a Customized Login Banner

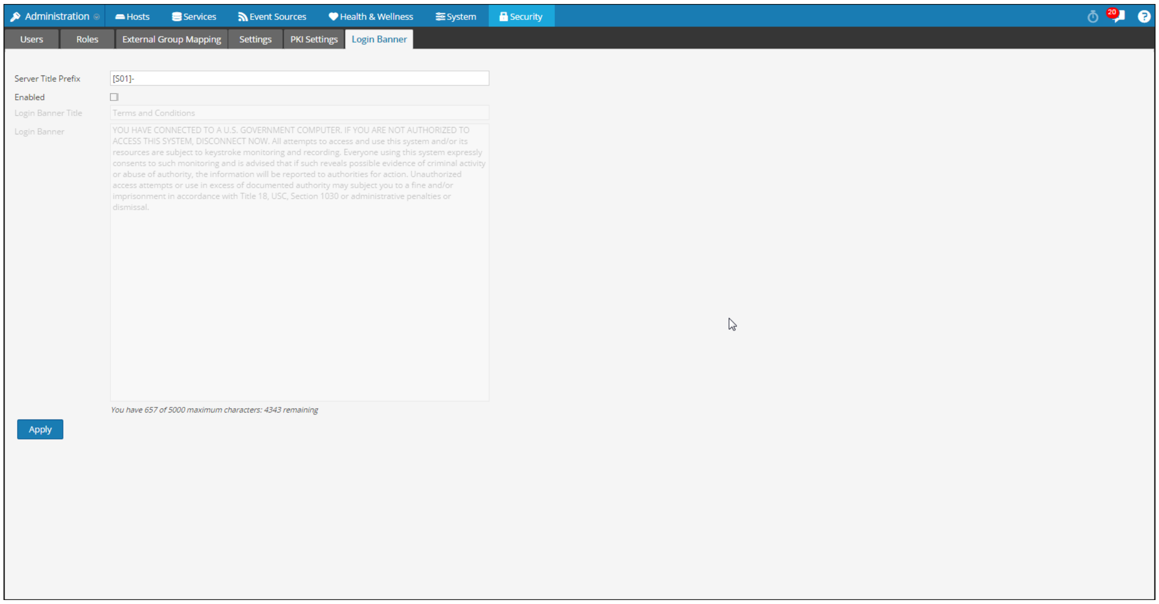
To create and enable a login banner for your instance of Security Analytics:

1. In the **Security Analytics** menu, select **Administration > Security.**

   The Security view is displayed with the Users tab open.

2. Click the **Login Banner** tab.

3. To differentiate the Security Analytics server of the current tab, in the **Server Prefix Title** field, enter the value of a prefix.



Server Title Prefix: [S01]-

Enabled: □

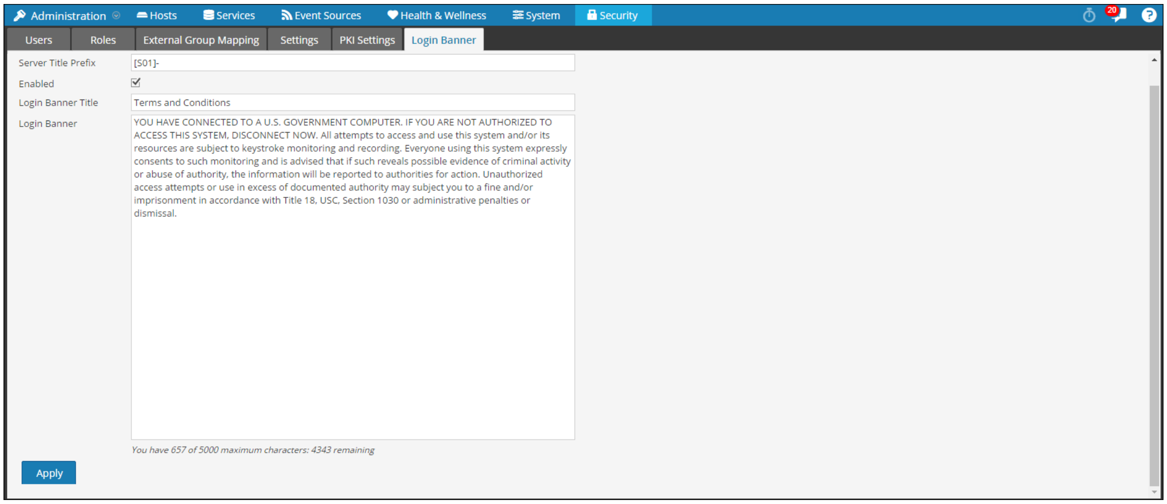
Login Banner Title: Terms and Conditions

Login Banner: YOU HAVE CONNECTED TO A U.S. GOVERNMENT COMPUTER. IF YOU ARE NOT AUTHORIZED TO ACCESS THIS SYSTEM, DISCONNECT NOW. All attempts to access and use this system and/or its resources are subject to keystroke monitoring and recording. Everyone using this system expressly consents to such monitoring and is advised that if such reveals possible evidence of criminal activity or abuse of authority, the information will be reported to authorities for action. Unauthorized access attempts or use in excess of documented authority may subject you to a fine and/or imprisonment in accordance with Title 18, USC, Section 1030 or administrative penalties or dismissal.

You have 657 of 5000 maximum characters: 4343 remaining

4. Select the **Enabled** checkbox to toggle between enabling and disabling the banner.

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



Server Title Prefix: [S01]-

Enabled: ☑

Login Banner Title: Terms and Conditions

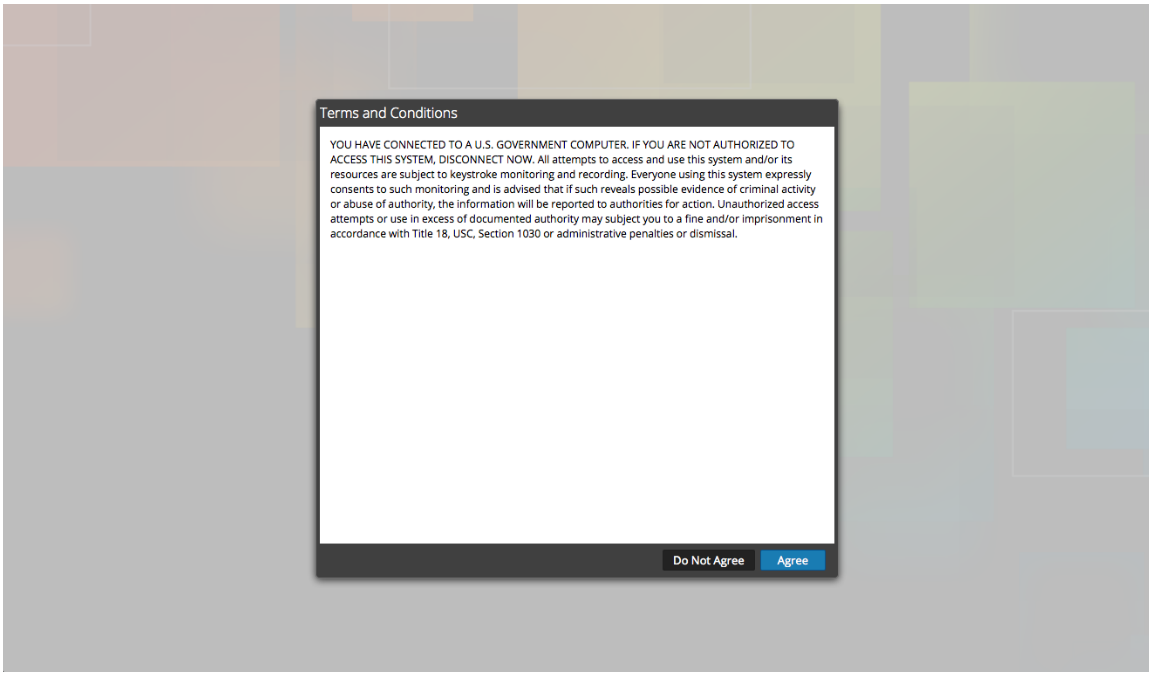
Login Banner: YOU HAVE CONNECTED TO A U.S. GOVERNMENT COMPUTER. IF YOU ARE NOT AUTHORIZED TO ACCESS THIS SYSTEM, DISCONNECT NOW. All attempts to access and use this system and/or its resources are subject to keystroke monitoring and recording. Everyone using this system expressly consents to such monitoring and is advised that if such reveals possible evidence of criminal activity or abuse of authority, the information will be reported to authorities for action. Unauthorized access attempts or use in excess of documented authority may subject you to a fine and/or imprisonment in accordance with Title 18, USC, Section 1030 or administrative penalties or dismissal.

You have 657 of 5000 maximum characters: 4343 remaining

5. Use the default content or type the custom title and content for your banner and click **Apply**.

   The banner is enabled and becomes active immediately.

6. To test the banner, log out. The banner is displayed in front of the fields for entering Security Analytics credentials.



Terms and Conditions

YOU HAVE CONNECTED TO A U.S. GOVERNMENT COMPUTER. IF YOU ARE NOT AUTHORIZED TO ACCESS THIS SYSTEM, DISCONNECT NOW. All attempts to access and use this system and/or its resources are subject to keystroke monitoring and recording. Everyone using this system expressly consents to such monitoring and is advised that if such reveals possible evidence of criminal activity or abuse of authority, the information will be reported to authorities for action. Unauthorized access attempts or use in excess of documented authority may subject you to a fine and/or imprisonment in accordance with Title 18, USC, Section 1030 or administrative penalties or dismissal.

7. Click **Agree**.

   The banner closes and you can log on.

Manage Users with Roles and Permissions

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

Topics

- Step 1. Review the Pre-Configured Security Analytics Roles
- Step 2. (Optional) Add a Role and Assign Permissions
- Step 3. Verify Query and Session Attributes per Role
- Step 4. Set Up a User
- Step 5. (Optional) Map User Roles to External Groups

Step 1. Review the Pre-Configured Security Analytics Roles

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

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
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 Security Analytics 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.

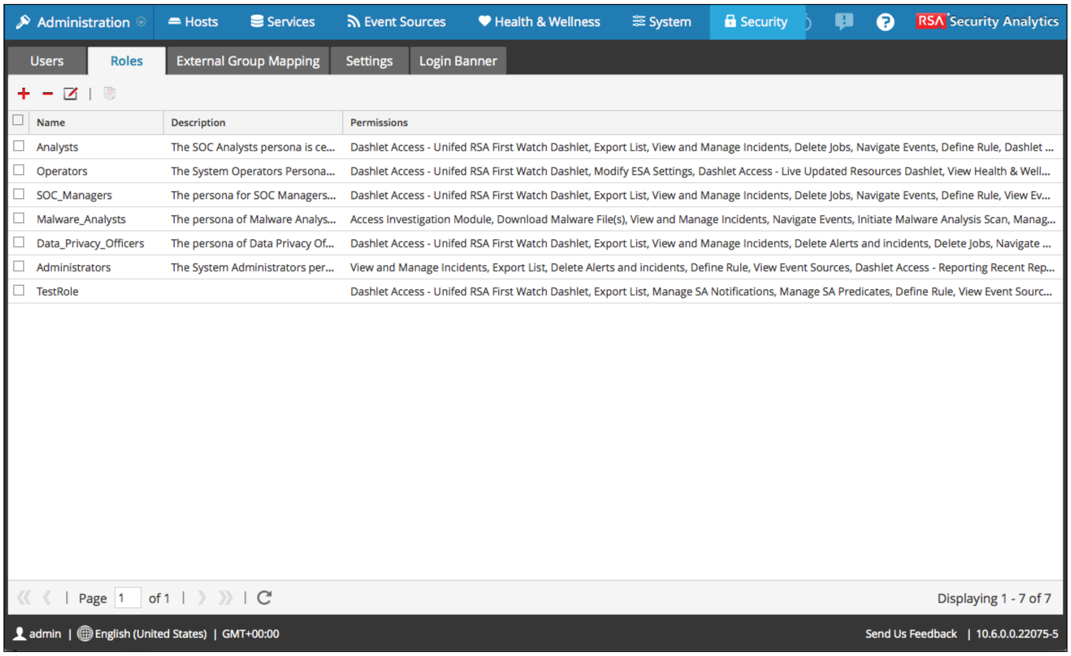
Each of the following procedures starts on the **Roles** tab.

To navigate to the Roles tab:

1. In the **Security Analytics** menu, select **Administration** > **Security**.

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

2. Click the **Roles** tab.



□	Name	Description	Permissions
□	Analysts	The SOC Analysts persona is ce...	Dashlet Access - Unifed RSA First Watch Dashlet, Export List, View and Manage Incidents, Delete Jobs, Navigate Events, Define Rule, Dashlet ...
□	Operators	The System Operators Persona...	Dashlet Access - Unifed RSA First Watch Dashlet, Modify ESA Settings, Dashlet Access - Live Updated Resources Dashlet, View Health & Well...
□	SOC_Managers	The persona for SOC Managers...	Dashlet Access - Unifed RSA First Watch Dashlet, Export List, View and Manage Incidents, Delete Jobs, Navigate Events, Define Rule, View Ev...
□	Malware_Analysts	The persona of Malware Analys...	Access Investigation Module, Download Malware File(s), View and Manage Incidents, Navigate Events, Initiate Malware Analysis Scan, Manag...
□	Data_Privacy_Officers	The persona of Data Privacy Of...	Dashlet Access - Unifed RSA First Watch Dashlet, Export List, View and Manage Incidents, Delete Alerts and incidents, Delete Jobs, Navigate ...
□	Administrators	The System Administrators per...	View and Manage Incidents, Export List, Delete Alerts and incidents, Define Rule, View Event Sources, Dashlet Access - Reporting Recent Rep...
□	TestRole		Dashlet Access - Unifed RSA First Watch Dashlet, Export List, Manage SA Notifications, Manage SA Predicates, Define Rule, View Event Sourc...

Page 1 of 1

Displaying 1 - 7 of 7

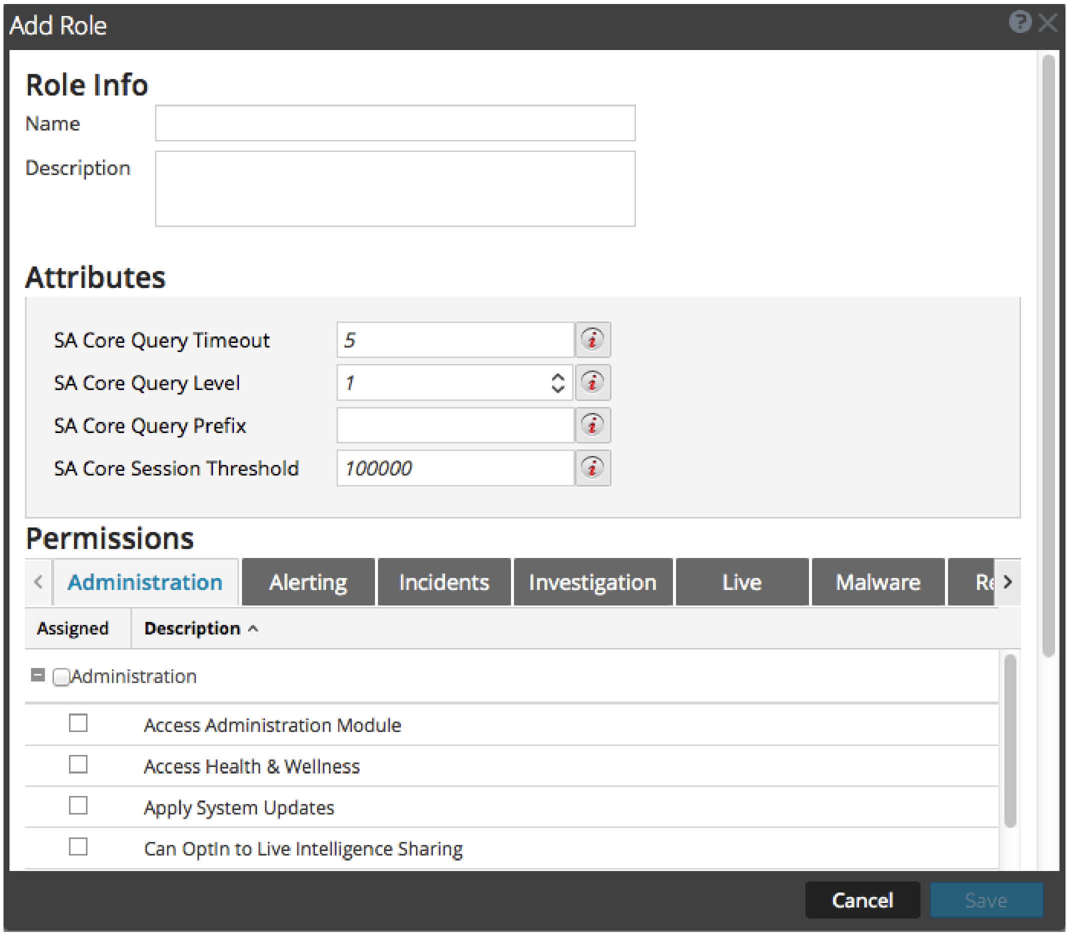
admin | English (United States) | GMT+00:00

Send Us Feedback | 10.6.0.0.22075-5

Add a Role and Assign Permissions

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

2. The **Add Role** dialog is displayed.



Add Role

Role Info

Name

Description

Attributes

SA Core Query Timeout	5
SA Core Query Level	1
SA Core Query Prefix	
SA Core Session Threshold	100000

Permissions

Assigned	Description ^
⊟ □Administration	
□	Access Administration Module
□	Access Health & Wellness
□	Apply System Updates
□	Can OptIn to Live Intelligence Sharing

3. In the **Role Info** section, type the following information for the role:

- **Name**
- (Optional) **Description**

4. 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. These attributes can be set for user roles and for individual users. If you set these attributes for individual users, the user settings override their assigned role settings.

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 unless these attributes are also set at the user level.

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

- **Query Timeout** is an optional setting that applies to Security Analytics 10.5 and later 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.
- **Query Level** is an optional setting that applies to Security Analytics 10.4 and earlier Core services. It defines the maximum query running time for a user based on three query levels: 1, 2, and 3. The default query levels are Query Level 1 = 60 minutes, Query Level 2 = 40 minutes, and Query Level 3 = 20 minutes. Query Level is deprecated for Core services starting with Security Analytics 10.5.
- **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 prepends to any queries run by the user and the user can only access meta of HTTP sessions.
- **Session Threshold** is a required setting. This value must be zero (0) or greater. If the threshold 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 query-handing attribute settings applied for a user depend on the role memberships of the user and whether these attributes have been set for the roles and the user. It is important to verify the query-handling attribute settings for your roles and users.

How Query-Handling Attribute Settings Apply to Individual Users

Query-handling attributes set for individual users override assigned role settings. If a user is a member of multiple roles, the following logic applies for the user:

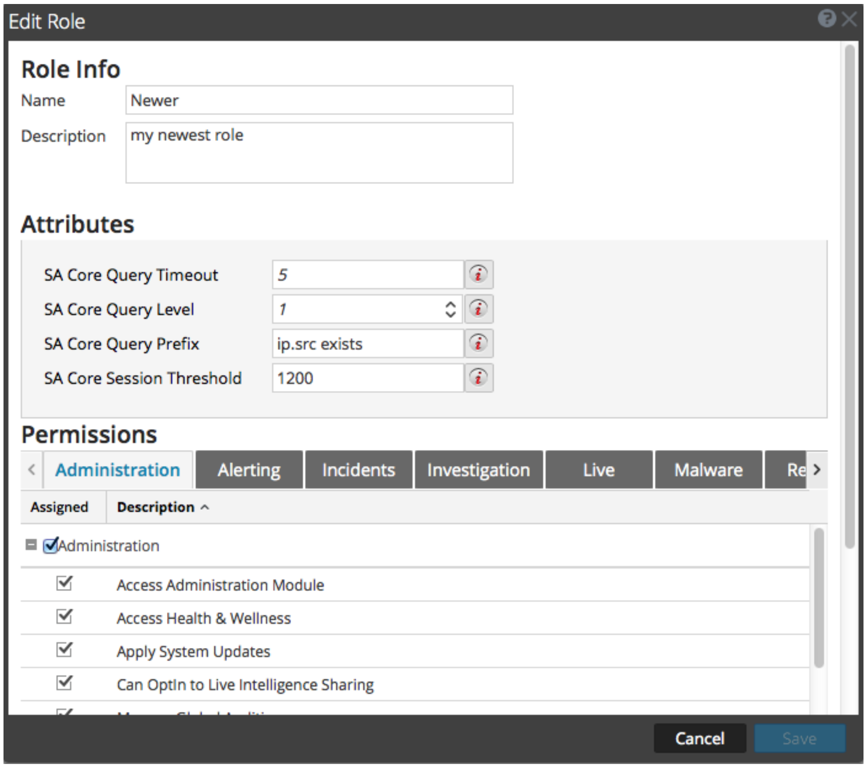
- **Query Timeout/Query Level:** Individual user settings override all role settings. If individual user settings are not set, the most permissive (highest) value of all assigned roles applies to the user.
- **Query Prefix:** Individual user settings override all role settings. If individual user settings are using defaults, which are shown in italics, the query prefixes of each of the user roles are OR'd together. If the query prefix is blank for both user and roles, no query prefix applies to the user.
- **Session Threshold:** Individual user settings override all role settings. The highest value of all the assigned roles applies to the user.

Procedure

To set query handling attributes for a user role:

1. In the **Security Analytics** menu, select **Administration > 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.



Role Info

Name: Newer

Description: my newest role

Attributes

SA Core Query Timeout: *5*

SA Core Query Level: *1*

SA Core Query Prefix: ip.src exists

SA Core Session Threshold: 1200

Permissions

Assigned	Description
☑	Administration
☑	Access Administration Module
☑	Access Health & Wellness
☑	Apply System Updates
☑	Can OptIn to Live Intelligence Sharing

3. To set the attributes for the role, in the **Attributes** section:

- (Optional) In the **SA Core Query Timeout** field, type 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. Security Analytics 10.5 and later Core services use this field.
  When migrating to Security Analytics 10.5 and later, if there is no value set in the roles, 5 minutes is set by default.
- (Optional) In the **SA Core Query Level** field, select the query level for the user. The default query levels are Query Level 1 = 60 minutes, Query Level 2 = 40 minutes, and Query Level 3 = 20 minutes. Security Analytics 10.4 and earlier Core services use this field. Query Level is deprecated for Core services starting with Security Analytics 10.5.
- (Optional) Type an **SA Core Query Prefix** to filter query results that the role members see. By default, this is blank.
- Type an **SA Core Session Threshold** for the system to stop its determination of the session count. The default is *`100000`*. The limit you specify here overrides the **Max Session Export** value defined in **Profile > Preferences > Investigation**.

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`.

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
- Verify Query and Session Attributes per User
- Enable, Unlock, and Delete User Accounts

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 Security Analytics 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 Security Analytics	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.
Security Analytics manages all user information.	Security Analytics manages user identification only. This includes Username, Full Name and Email.

Procedures

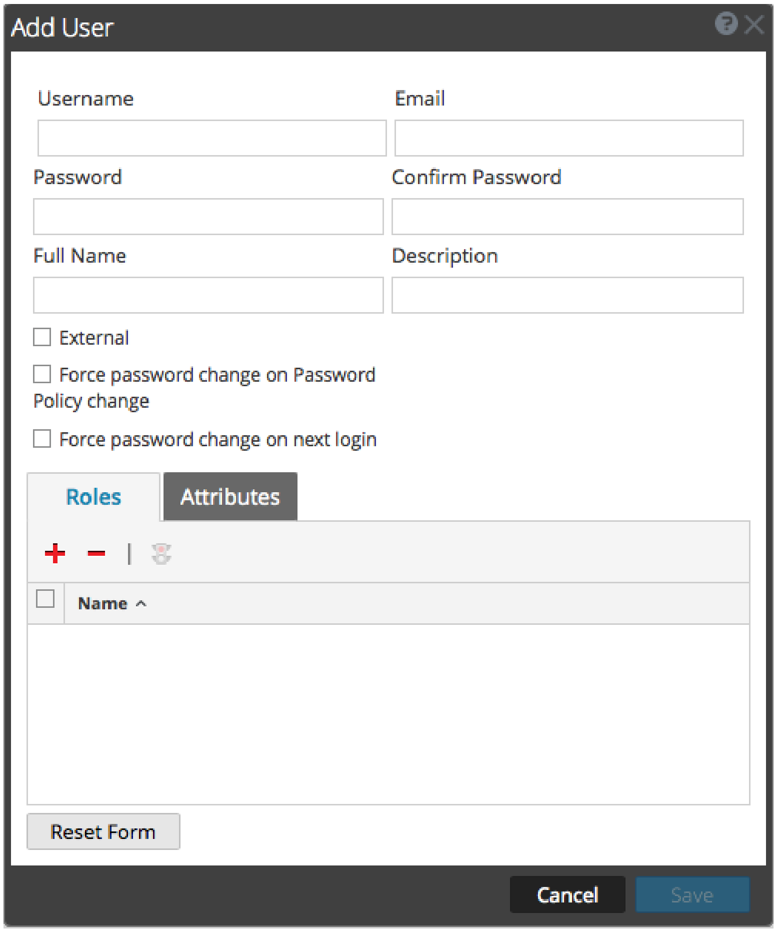
Each of the following procedures starts on the Users tab. To navigate to the Users tab, in the **Security Analytics** menu, select **Administration > Security**. The Security view is displayed with the Users tab open.

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.

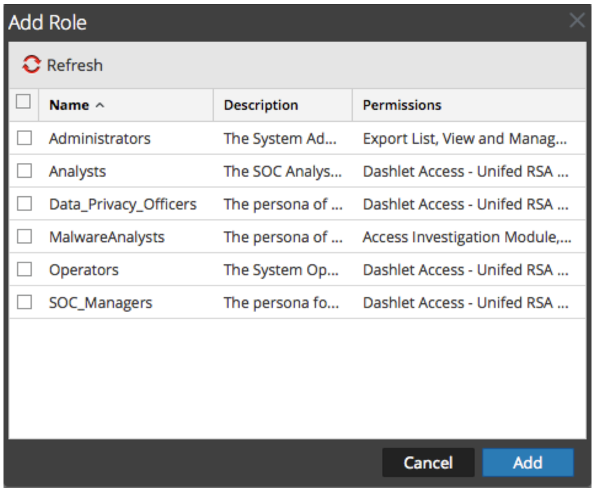


2. Type the following account information for the new user:
   - **Username** for logging on to Security Analytics
   - **Email** address
   - Password for logging on to Security Analytics, in the **Password** and **Confirm Password** fields
   - **Full Name** of the new user
   - (Optional) **Description** of the user account
3. To require the user to create a new password when there are changes to the password strength policy, select **Force password change on Password Policy change**.
4. 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.

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

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



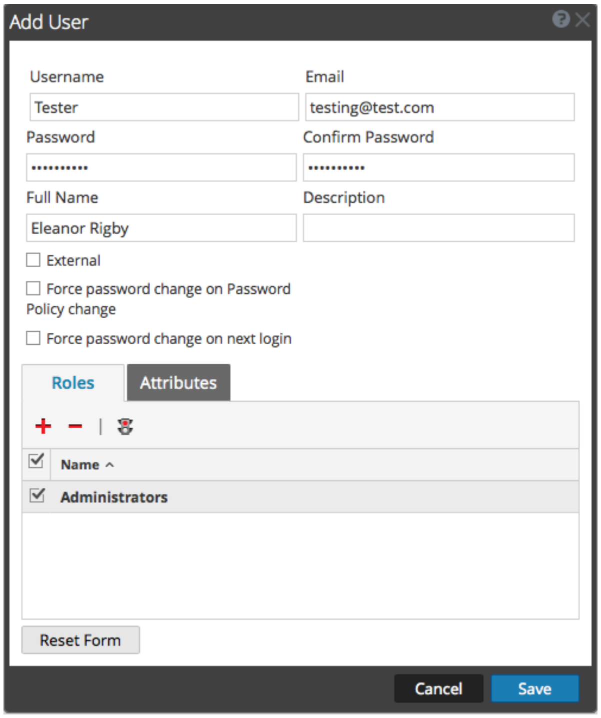
Add Role

Refresh

□	Name ^	Description	Permissions
□	Administrators	The System Ad...	Export List, View and Manag...
□	Analysts	The SOC Analys...	Dashlet Access - Unifed RSA ...
□	Data_Privacy_Officers	The persona of ...	Dashlet Access - Unifed RSA ...
□	MalwareAnalysts	The persona of ...	Access Investigation Module,...
□	Operators	The System Op...	Dashlet Access - Unifed RSA ...
□	SOC_Managers	The persona fo...	Dashlet Access - Unifed RSA ...

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

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



Add User

Username: Tester
Email: testing@test.com
Password: ••••••••••
Confirm Password: ••••••••••
Full Name: Eleanor Rigby
Description:

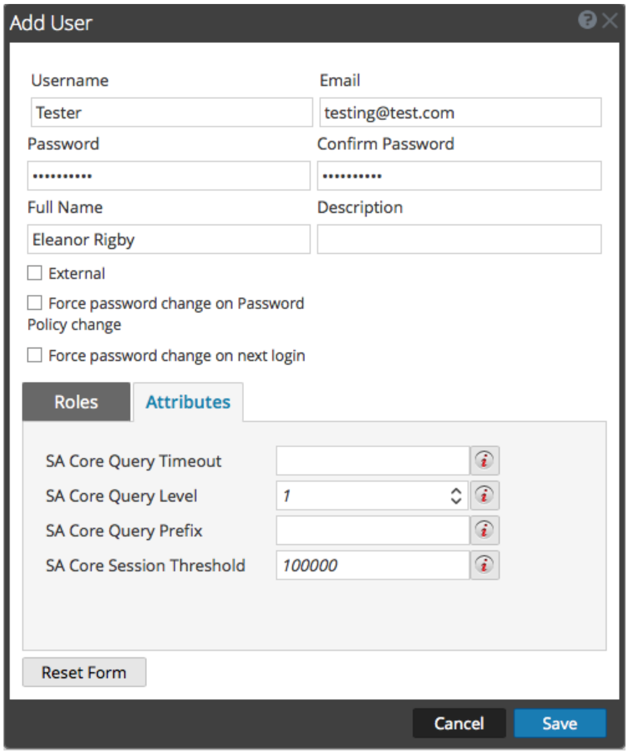
□ External
□ Force password change on Password Policy change
□ Force password change on next login

Roles | Attributes

☑	Name ^
☑	Administrators

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

8. (Optional) To specify query handling settings in the **Attributes** tab, see Verify Query and Session Attributes per User.



Username	Email
Tester	testing@test.com
Password	Confirm Password
••••••••••	••••••••••
Full Name	Description
Eleanor Rigby	

☐ External

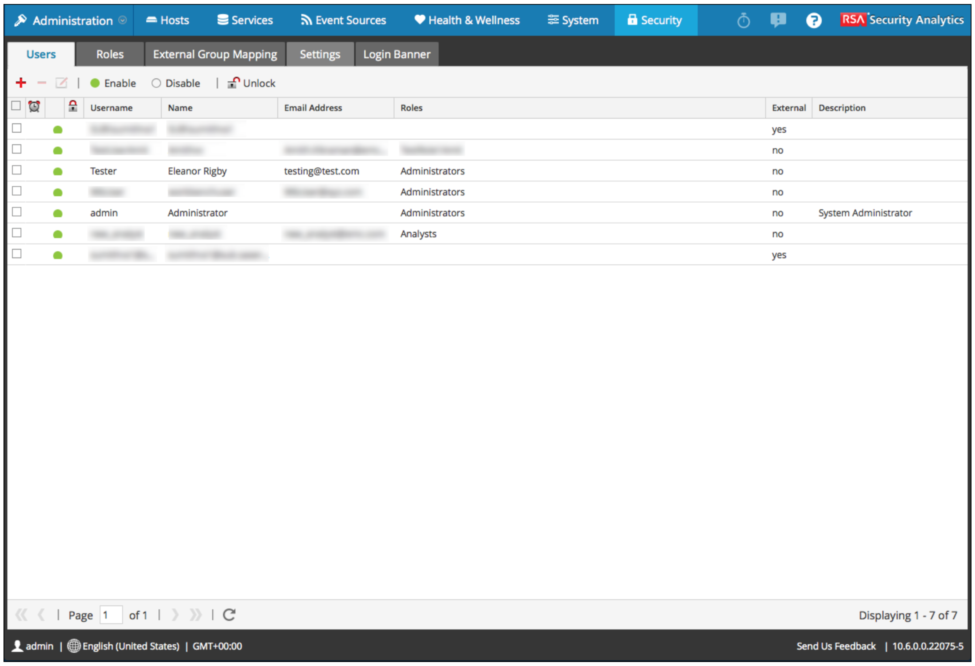
☐ Force password change on Password Policy change

☐ Force password change on next login

SA Core Query Timeout	
SA Core Query Level	1
SA Core Query Prefix	
SA Core Session Threshold	100000

9. Click **Save**.

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



☐				Username	Name	Email Address	Roles	External	Description
☐		●		[redacted]	[redacted]			yes	
☐		●		[redacted]	[redacted]	[redacted]	[redacted]	no	
☐		●		Tester	Eleanor Rigby	testing@test.com	Administrators	no	
☐		●		[redacted]	[redacted]	[redacted]	Administrators	no	
☐		●		admin	Administrator		Administrators	no	System Administrator
☐		●		[redacted]	[redacted]	[redacted]	Analysts	no	
☐		●		[redacted]	[redacted]			yes	

Page 1 of 1
Displaying 1 - 7 of 7
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.22075-5

Add a User for External Authentication

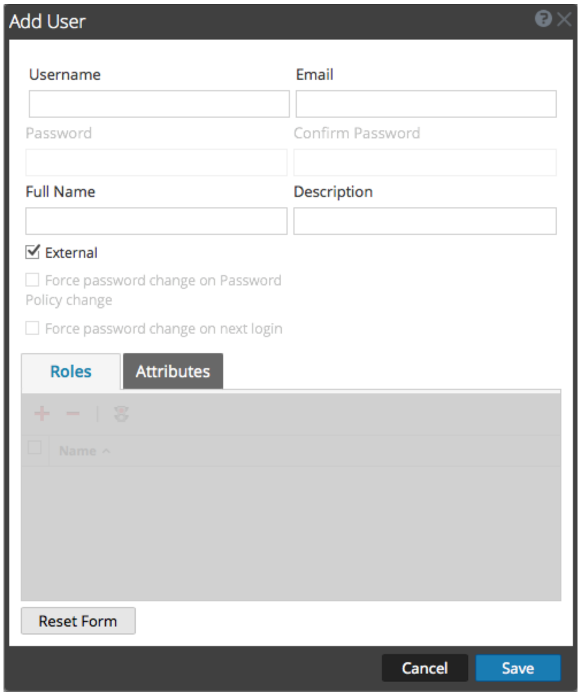
Prerequisite: External authentication must be configured. Refer to Step 4. (Optional) Configure External Authentication.

To add a user that is authenticated externally, outside of Security Analytics:

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

   The **Add User** dialog is displayed.

2. Select **External** to show only the fields required for external authentication.



3. Type the following information:
   - **Username** for logging on to Security Analytics
   - **Email** address
   - **Full Name** of the new user
   - (Optional) **Description** of the user account

4. (Optional) To specify query handling settings in the **Attributes** tab, see Verify Query and Session Attributes per User.

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

6. To map a role to the new user, see 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:

   - **Password**
   - **Email**
   - **Full Name**
   - **Description**

3. To change the account type, select or deselect **External**.

Note: If you change the account from local to external or vice versa, you must also change how the user receives permissions. For details, see the introduction to this topic.

4. To require an **internal** user to create a new password when there are changes to the password strength policy, select **Force password change on Password Policy change**.

5. 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.

6. 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.

Verify Query and Session Attributes per User

This topic provides instructions for setting query-handling attributes for individual users if you want to override the role settings.

Query-handling attributes determine how to handle the queries that a user runs. These attributes enable you to lock down the information that users can retrieve. You can specify the following query-handling attributes for a role or user:

- **Query Timeout** is an optional setting that applies to Security Analytics 10.5 and later 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.
- **Query Level** is an optional setting that applies to Security Analytics 10.4 and earlier Core services. It defines the maximum query running time for a user based on three query levels: 1, 2, and 3. The default query levels are Query Level 1 = 60 minutes, Query Level 2 = 40 minutes, and Query Level 3 = 20 minutes. Query Level is deprecated for Core services starting with Security Analytics 10.5.
- **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 prepends to any queries run by the user and the user can only access meta of HTTP sessions.
- **Session Threshold** is a required setting. This value must be zero (0) or greater. If the threshold 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

You should not set these query-handling attributes at the user level unless you want to override the role settings. Query-handling attributes set for individual users override assigned role settings. If you do not specify these settings for individual users, the settings are applied to users based on their role memberships. Step 3. Verify Query and Session Attributes per Role provides information on how the role settings impact individual user settings and what happens if a user is a member of multiple roles.

It is important to verify the query-handling attributes that are set for each user.

Procedure

Note: You should not set these query-handling attributes at the user level unless you want to override the role settings.

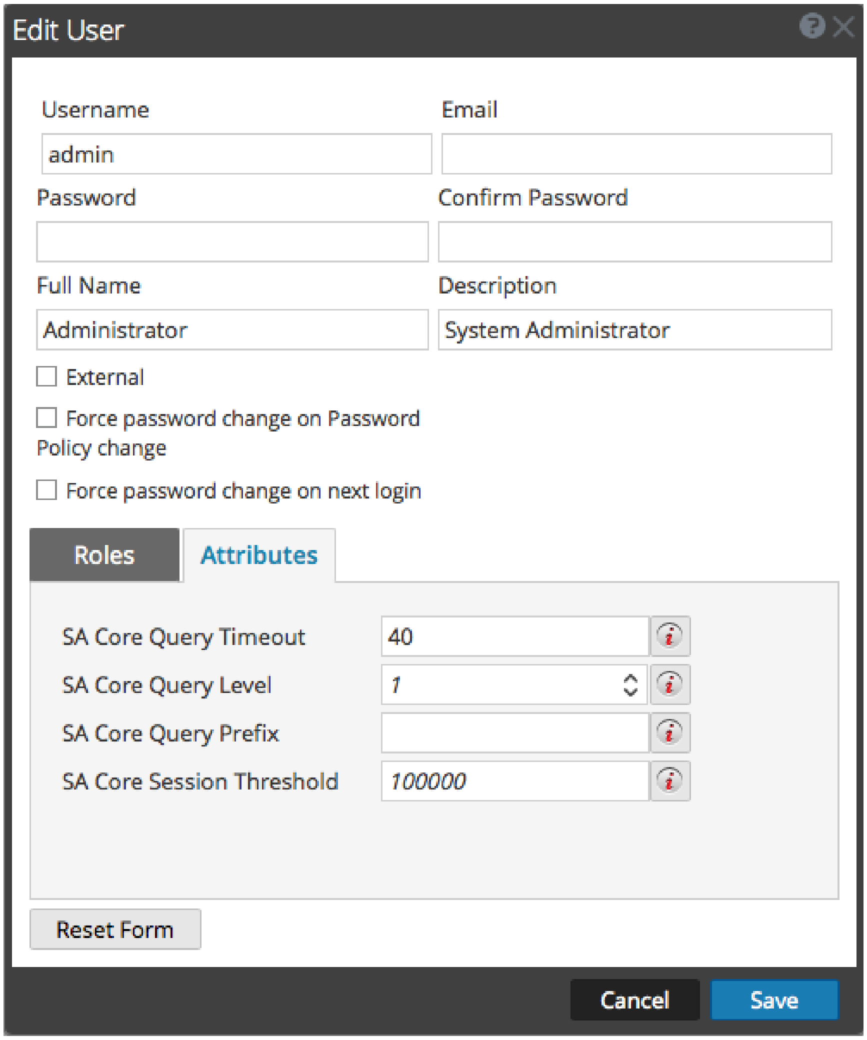
To set query-handling attributes for a user:

1. In the **Security Analytics** menu, select **Administration** > **Security**.

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

2. If you are adding a user, click +. If you are editing a user, select the user and click .✎

3. In the Add or Edit User dialog, select the **Attributes** tab.



Edit User

Username: admin

Email:

Password:

Confirm Password:

Full Name: Administrator

Description: System Administrator

□ External

□ Force password change on Password Policy change

□ Force password change on next login

SA Core Query Timeout	40
SA Core Query Level	1
SA Core Query Prefix	
SA Core Session Threshold	100000

4. To set an attribute for the user:

   - (Optional) In the **SA Core Query Timeout** field, type the maximum number of minutes that a user can run a query. This timeout only applies to queries performed from Investigation. This field is blank by default. If you do not want to override the assigned role settings, leave this field blank. Security Analytics 10.5 and later Core services use this field.

- (Optional) In the **SA Core Query Level** field, select the query level for the user. The default query levels are Query Level 1 = 60 minutes, Query Level 2 = 40 minutes, and Query Level 3 = 20 minutes. Security Analytics 10.4 and earlier Core services use this field. Query Level is deprecated for Core services starting with Security Analytics 10.5.
- (Optional) Type an **SA Core Query Prefix** to filter query results the user sees. By default, this is blank.
- Type an **SA Core Session Threshold** for the system to stop its determination of the session count. The default is `100000`*.* The limit you specify here overrides the **Max Session Export** value defined in **Profile > Preferences > Investigation**.

A value shown in italics indicates a default value, for example, *`100000`*. A value shown without italics indicates a change from the default value, for example, `40`.

5. (Optional) If you want to revert to the existing values, click **Reset Form**.
6. Click **Save.**

To verify the attributes assigned for a user, you can turn DEBUG logging on the **com.netwitness.platform.server.common.auth** package. When the user logs on to Security Analytics, a Debug log message is generated that shows the attributes applied for that user.

Enable, Unlock, and Delete User Accounts

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

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

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

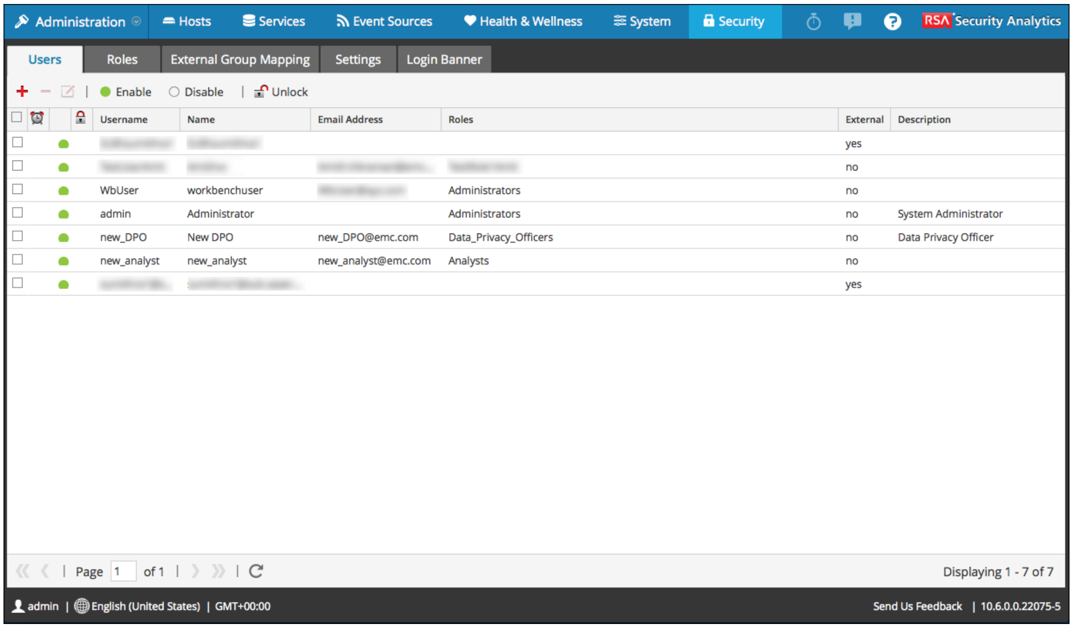
You can unlock locked accounts for both local and external users.

Enable Disabled Security Analytics U ser Accounts

To enable Security Analytics user accounts that have been disabled:

1. In the **Security Analytics** menu, select **Administration** > **Security.**

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



☐	⏰		🔒	Username	Name	Email Address	Roles	External	Description
☐		●		[redacted]	[redacted]			yes	
☐		●		[redacted]	[redacted]	[redacted]	[redacted]	no	
☐		●		WbUser	workbenchuser	[redacted]	Administrators	no	
☐		●		admin	Administrator		Administrators	no	System Administrator
☐		●		new_DPO	New DPO	new_DPO@emc.com	Data_Privacy_Officers	no	Data Privacy Officer
☐		●		new_analyst	new_analyst	new_analyst@emc.com	Analysts	no	
☐		●		[redacted]	[redacted]			yes	

Page 1 of 1

Displaying 1 - 7 of 7

admin | English (United States) | GMT+00:00

Send Us Feedback | 10.6.0.0.22075-5

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 Security Analytics.

Disable Security Analytics 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 Security Analytics 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 Security Analytics.

Unlock Locked Security Analytics User Accounts

A user is locked out for a period of time after a number of failed consecutive login attempts. To unlock Security Analytics 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 Security Analytics.

Delete Security Analytics User Accounts

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

To delete Security Analytics user accounts:

1. In the **Security Analytics** menu, select **Administration > Security**.

   The Security view is displayed with the **Users** tab open.
2. In the **Users** grid, 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 Security Analytics, and the users can no longer log in to Security Analytics.

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

This topic describes the method for mapping Security Analytics user roles to external groups.

In Security Analytics, external groups derive permissions for various modules and views from Security Analytics 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 Security Analytics.

Add Role Mapping for an External Group

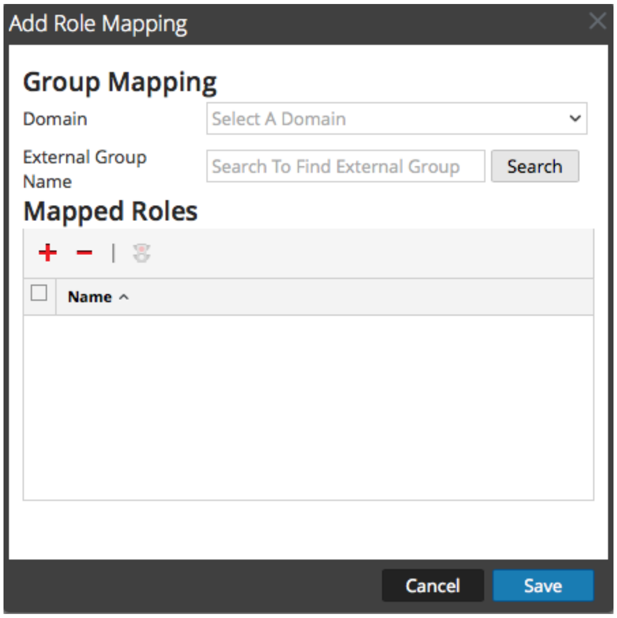
1. In the **Security Analytics** menu, select **Administration** > **Security**.

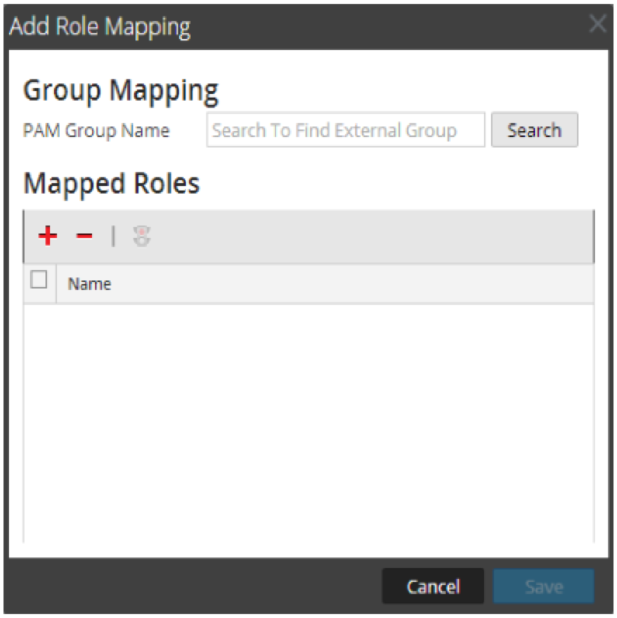
   The Security view is displayed with the **Users** tab open.

2. Click the **External Group Mapping** tab.

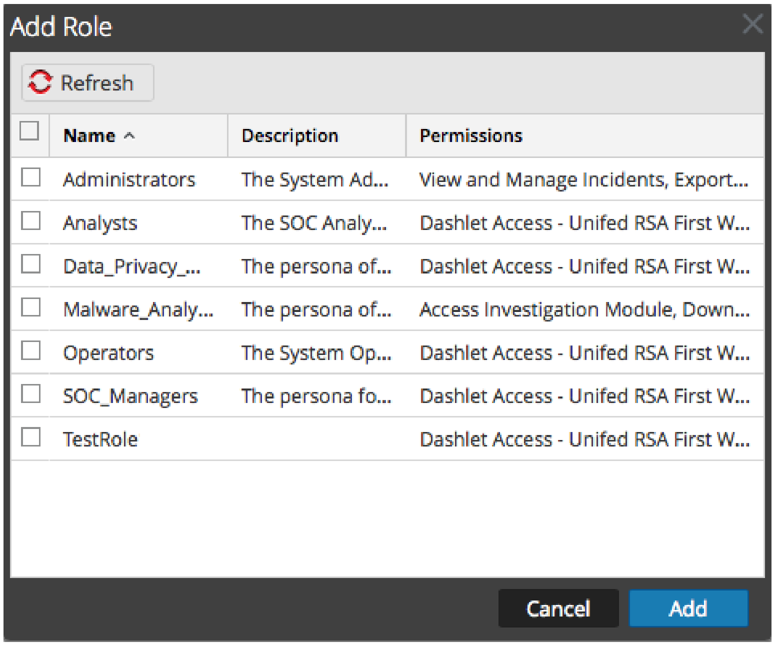
3. In the toolbar, click +.

   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 External Groups Dialog, 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.



□	Name ^	Description	Permissions
□	Administrators	The System Ad...	View and Manage Incidents, Export...
□	Analysts	The SOC Analy...	Dashlet Access - Unifed RSA First W...
□	Data_Privacy_...	The persona of...	Dashlet Access - Unifed RSA First W...
□	Malware_Analy...	The persona of...	Access Investigation Module, Down...
□	Operators	The System Op...	Dashlet Access - Unifed RSA First W...
□	SOC_Managers	The persona fo...	Dashlet Access - Unifed RSA First W...
□	TestRole		Dashlet Access - Unifed RSA First W...

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 grid.

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 grid.

Related Topic

- Search for External Groups

Search for External Groups

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

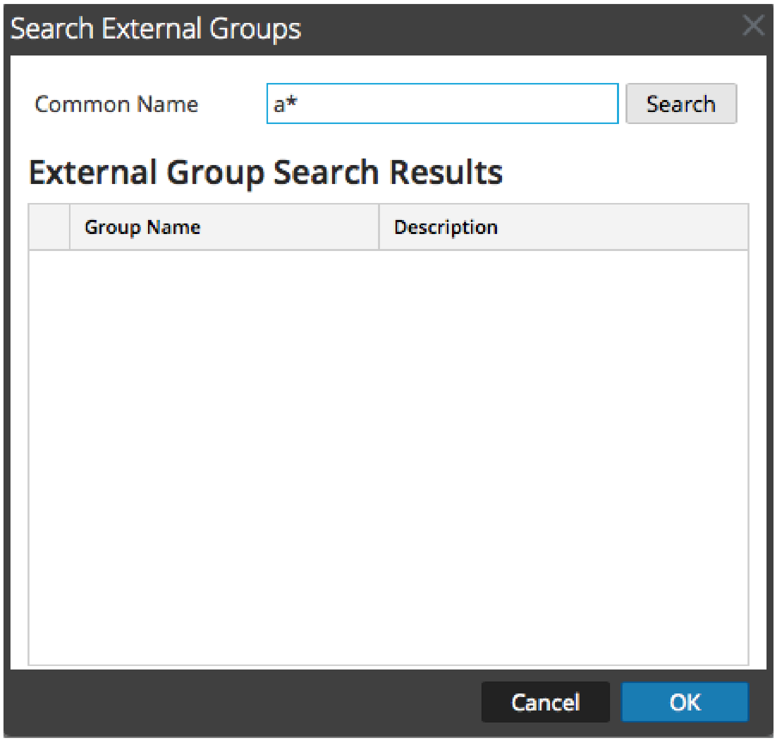
Prerequisites

A method for external user authentication must be enabled.

Procedure

To search for an external group:

1. In the **Security Analytics** menu, select **Administration > 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 🔍 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 (*).



Search External Groups

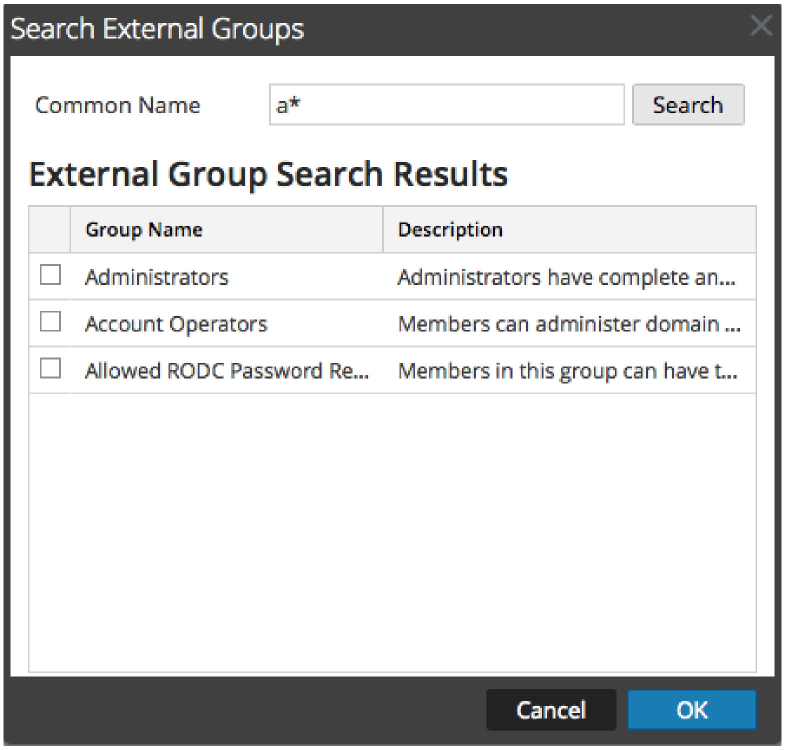
Common Name: a*

External Group Search Results

	Group Name	Description

6. Click **Search**.

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



Search External Groups

Common Name: a*

External Group Search Results

	Group Name	Description
□	Administrators	Administrators have complete an...
□	Account Operators	Members can administer domain ...
□	Allowed RODC Password Re...	Members in this group can have t...

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

Set Up Public Key Infrastructure (PKI) Authentication

This topic provides an overview of PKI authentication and detailed instructions to configure PKI authentication in Security Analytics.

Topics

- Overview
- Configure PKI Authentication

Overview

This topic provides an overview of PKI authentication and how it is used to access Security Analytics User Interface (UI).

In 10.5.0.2 or later, PKI authentication can be used to access the Security Analytics UI. PKI allows users to authenticate and access the Security Analytics UI using digital certificates.

Certificates are issued by a Third-Party Certificate Authority (CA) (external to Security Analytics server). The following categories of certificates are required for PKI authentication:

- Security Analytics server certificate (private key and its chain)
- Trusted CA certificates
- User certificate (issued by CA)

Security Analytics Server Certificate

This certificate is used by Security Analytics server to present its identity. This certificate is issued by a trusted CA. When a user accesses the Security Analytics UI using HTTPS, this certificate is presented to the user in the web browser.

Trusted CA Certificates

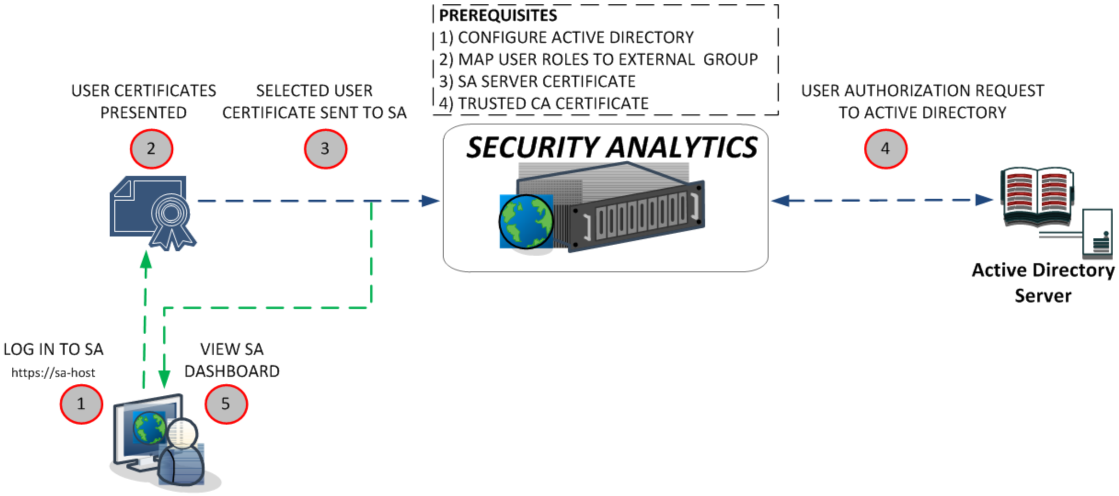
These are collection of CA certificates. Security Analytics server uses these certificates as the trusted authorities to validate the certificate provided by the user. If the user does not have a certificate signed by one of these CA(s), the user is not allowed to access the Security Analytics UI.

User Certificate

This certificate is used by the Security Analytics user to present the user's identity. This certificate is issued by a CA that is trusted by the users. The user certificates, by default, are identified by most browsers. In case the certificates are not identified, the user must import the certificates into browser certificates store.

Security Analytics PKI Authentication Workflow

The following figure shows how the user can access Security Analytics using PKI authentication.


PREREQUISITES
1) CONFIGURE ACTIVE DIRECTORY
2) MAP USER ROLES TO EXTERNAL GROUP
3) SA SERVER CERTIFICATE
4) TRUSTED CA CERTIFICATE
USER CERTIFICATES PRESENTED
SELECTED USER CERTIFICATE SENT TO SA
USER AUTHORIZATION REQUEST TO ACTIVE DIRECTORY
2
3
4
SECURITY ANALYTICS
Active Directory Server
LOG IN TO SA
https://sa-host
VIEW SA DASHBOARD
1
5

The following points explain the workflow of the above figure.

1. User tries to access the Security Analytics UI using the web browser. For example, https://sa-host/login.
2. The user is prompted to select the user certificate.

Note: The certificate prompt may appear differently depending on the browser.

3. User selects the certificate. The browser sends the selected certificate to the Security Analytics server for authentication.
4. If the authentication is successful, the Security Analytics server authorizes the user based on the user groups configured on the Active Directory Server(s).
5. If the user authentication and authorization are successful, the Security Analytics dashboard is displayed.

Note: If the certificate validation fails, the user cannot access the Security Analytics Dashboard.

Configure PKI Authentication

This topic provides the step-by-step procedure to configure PKI authentication on Security Analytics. Follow the steps in order to configure PKI on Security Analytics.

Note: PKI authentication is supported from SA versions 10.5.0.2 or later.

Note: PAM is not supported for PKI authentication.

Topics

- Step 1. Configure Active Directory
- Step 2. Map User Roles to External Groups
- Step 3. Import Server Certificate and Trusted CA Certificate
- Step 4. Configure User Principal Settings
- Step 5. Import Certificate Revocation List
- Step 6. Enable PKI

Step 1. Configure Active Directory

See Configure Active Directory for instructions on how to use Active Directory to authenticate external user logins.

Next Step:

Step 2. Map User Roles to External Groups

Step 2. Map User Roles to External Groups

See Step 5. (Optional) Map User Roles to External Groups for instructions on how to map user roles to external groups to provide necessary access.

Next Step:

Step 3. Import Server Certificate and Trusted CA Certificate

Step 3. Import Server Certificate and Trusted CA Certificate

This topic describes the procedure to import a Security Analytics server certificate with its key and trusted Certificate Authority (CA) certificate required to enable Public Key Infrastructure (PKI) authentication.

Prerequisites

Make sure that you have:

- Configured Active Directory to enable authentication for external groups. For more information, see Configure Active Directory.
- Mapped external groups to Security Analytics user roles. For more information, see Step 2. Map User Roles to External Groups.
- The Security Analytics server certificate with its private key. For more information, see Step 5. (Optional) Use Custom Server Certificate.
- The trusted CA certificates. This can be the root CA's or Intermediate CA's certificate up to root CA.
- The Security Analytics user certificate signed by one of the trusted CAs in the Security Analytics server.

Next Step:

Step 4. Configure User Principal Settings

Step 4. Configure User Principal Settings

This topic describes how you can specify an attribute in a certificate to uniquely identify the user for Public Key Infrastructure (PKI) authentication.

You must specify an attribute with user name or user id, in a certificate, to uniquely identify the user. A certificate may contain user name or user id in **Extension (Non standard custom attributes)**, **Subject DN** or **Subject Alternative Name** field and Security Analytics server must be configured to read the value of this attribute. The Security Analytics server uses the extracted value of this attribute for authorization and retrieves the user groups from an Active Directory (AD) server. By default, Security Analytics server extracts the entire value of the selected attribute, without filtering any characters. You can use regular expression (REGEX) to refine the value extracted.

To configure user principal settings:

1. In the **Security Analytics** menu, select **Administration** > **Security.**

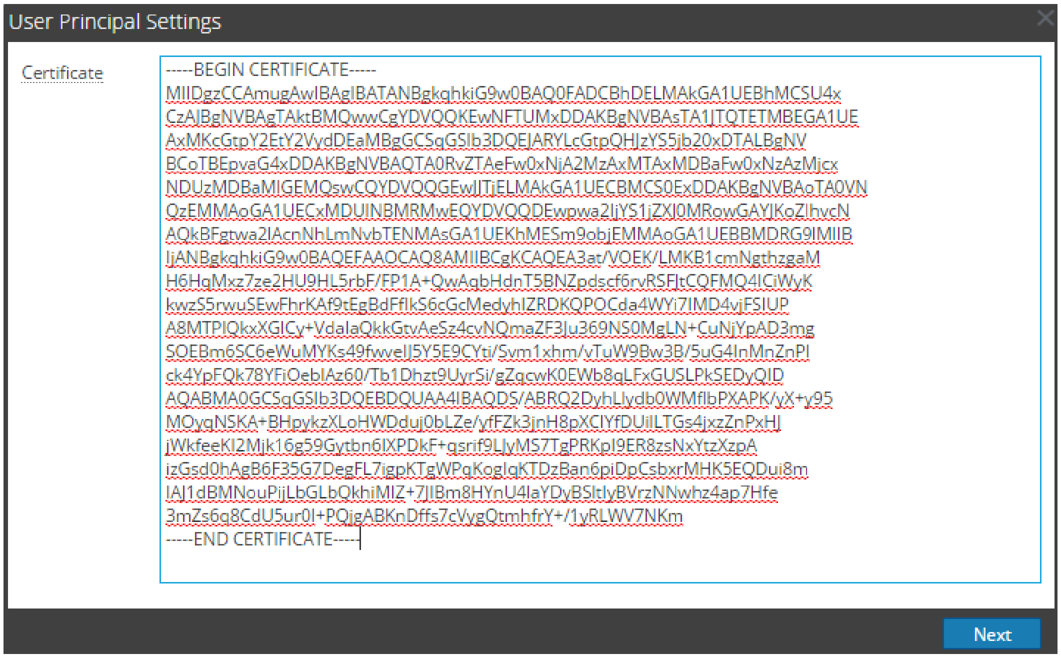
   The Security view is displayed with the **Users** tab open.

2. Click the **Settings** tab.

3. In the **User Principal settings**, click **Configure**.

   The User Principal Settings dialog is displayed.

4. In the **Certificate** field, paste the BASE64 encoded user certificate.

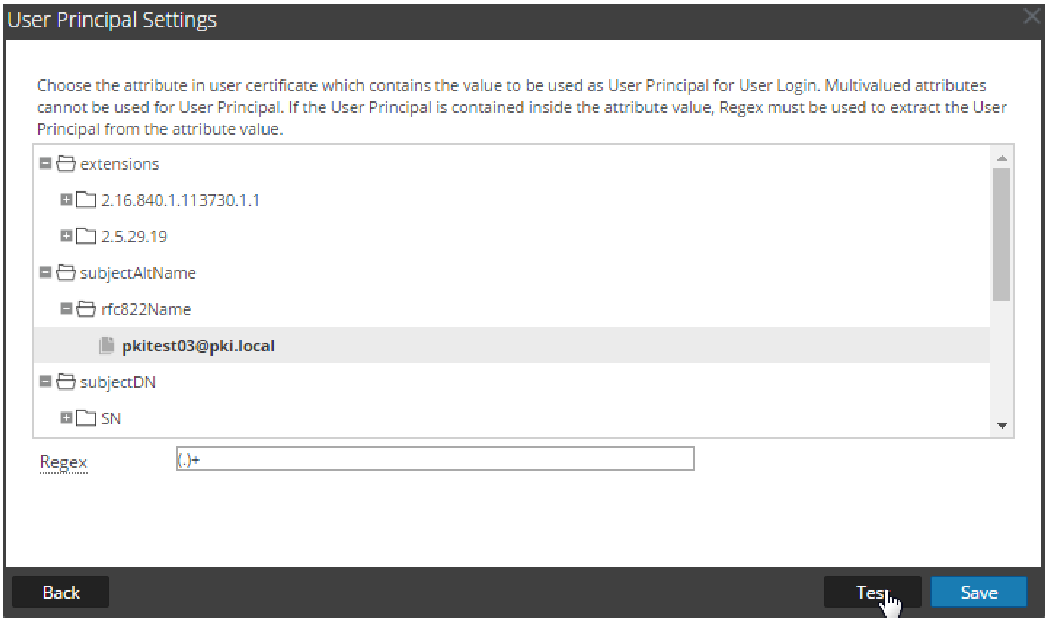


```
-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgIBATANBgkqhkiG9w0BAQ0FADCBhDELMAkGA1UEBhMCSU4x
CzAJBgNVBAgTAktBMQwwCgYDVQQKEwNFTUMxDDAKBgNVBAsTA1JTQTETMBEGA1UE
AxMKcGtpY2EtY2VydDEaMBgGCSqGSIb3DQEJARYLcGtpQHJzYS5jb20xDTALBgNV
BCoTBEpvaG4xDDAKBgNVBAQTA0RvZTAeFw0xNjA2MzAxMTAxMDBaFw0xNzAzMjcx
NDUzMDBaMIGEMQswCQYDVQQGEwJJTjELMAkGA1UECBMCS0ExDDAKBgNVBAoTA0VN
QzEMMAoGA1UECxMDUINBMRMwEQYDVQQDEwpwa2ljYS1jZXJ0MRowGAYJKoZIhvcN
AQkBFgtwa2lAcnNhLmNvbTENMAsGA1UEKhMESm9objEMMAoGA1UEBBMDRG9lMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3at/VOEK/LMKB1cmNgthzgaM
H6HqMxz7ze2HU9HL5rbF/FP1A+QwAqbHdnT5BNZpdscf6rvRSFJtCQFMQ4ICiWyK
kwzS5rwuSEwFhrKAf9tEgBdFflkS6cGcMedyhIZRDKQPOCda4WYi7IMD4vjFSIUP
A8MTPIQkxXGICy+VdaIaQkkGtvAeSz4cvNQmaZF3Ju369NS0MgLN+CuNjYpAD3mg
SOEBm6SC6eWuMYKs49fwveIJ5Y5E9CYti/Svm1xhm/vTuW9Bw3B/5uG4InMnZnPl
ck4YpFQk78YFiOeblAz60/Tb1Dhzt9UyrSi/gZqcwK0EWb8qLFxGUSLPkSEDyQID
AQABMA0GCSqGSIb3DQEBDQUAA4IBAQDS/ABRQ2DyhLlydb0WMflbPXAPK/yX+y95
MOyqNSKA+BHpykzXLoHWDduj0bLZe/yfFZk3jnH8pXCIYfDUilLTGs4jxzZnPxHJ
jWkfeeKI2Mjk16g59Gytbn6IXPDkF+qsrif9LJyMS7TgPRKpI9ER8zsNxYtzXzpA
izGsd0hAgB6F35G7DegFL7igpKTgWPqKogIqKTDzBan6piDpCsbxrMHK5EQDui8m
IAJ1dBMNouPijLbGLbQkhiMIZ+7JIBm8HYnU4IaYDyBSItlyBVrzNNwhz4ap7Hfe
3mZs6q8CdU5ur0I+PQjgABKnDffs7cVygQtmhfrY+/1yRLWV7NKm
-----END CERTIFICATE-----
```

5. Click **Next**.

   The Extensions, SubjectDN and Subject Alternative name fields are displayed.

6. Select a unique field that reflects the user name or user id.

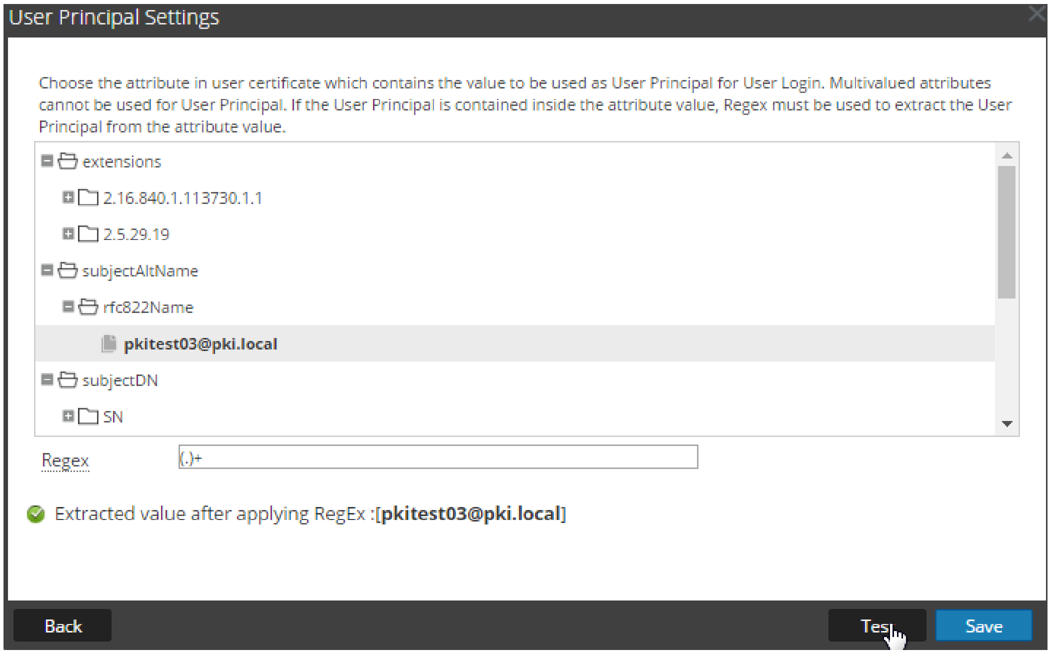


User Principal Settings

Choose the attribute in user certificate which contains the value to be used as User Principal for User Login. Multivalued attributes cannot be used for User Principal. If the User Principal is contained inside the attribute value, Regex must be used to extract the User Principal from the attribute value.

7. Click **Test.**

The user name or user principal name is extracted and displayed within square brackets.



User Principal Settings

Choose the attribute in user certificate which contains the value to be used as User Principal for User Login. Multivalued attributes cannot be used for User Principal. If the User Principal is contained inside the attribute value, Regex must be used to extract the User Principal from the attribute value.

✓ Extracted value after applying RegEx :[**pkitest03@pki.local**]

- If the extracted user principal name does not match the AD user name, you can modify the Regex to extract the exact user name and click **Test**.

  If the extracted value does not contain the Active Directory user name as a unique value and if it contains a uniquely identifiable attribute of the user such as EmpNo or EmpID. You must configure the custom LDAP filter in the Active Directory which uniquely identifies the user object. For more information to configure custom LDAP filter, see Step 1. Configure Active Directory.

8. Click **Save** to update the Security Analytics server.

Note: If the User Principal Setting is incorrect, Security Analytics server will not allow you to access Security Analytics UI. In this case, to access the Security Analytics UI you must revert or disable PKI from the backend. For more information to disable PKI, see Disable PKI.

Next Step:

Step 5. Import Certificate Revocation List

Step 5. Import Certificate Revocation List

This topic describes the procedure to import a Certificate Revocation List (CRL) to Security Analytics server.

A CRL is a file that contains a list of revoked certificates with details such as the serial number and revocation date of each certificate. Typically a certificate is revoked to avoid any compromise of the certificate by unauthorized users. For example, if a Security Analytics user resigns from an organization, then the user's certificate must be revoked by the issuing CA to avoid any certificate compromise.

You can import the CRL issued by your trusted CA, so that Security Analytics can use the CRL to block unauthorized users from accessing Security Analytics. You can specify or import a CRL to Security Analytics using the below options:

- **HTTP server** - This is the most common CRL Location where CA publishes the CRL to external applications using a HTTP server. The Security Analytics server reads the CRL using the HTTP URL.
- **Local CRL** - This allow you to manually download the CRL for a CA and upload it to the Security Analytics server. For automation, you can write a Cron job to copy the CRL to the `/var/lib/netwitness/uax/pki/crl`directory in the Security Analytics server. The Security Analytics server uses the updated CRL from the disk when the CRL is refreshed (every 5 minutes).
- **LDAP Resource** - This is mostly used by Windows Systems. You must specify an LDAP URL with the username and password to access the LDAP Object. The Security Analytics server reads the CRL from the LDAP URL.
- **OCSP Responder** - To specify a OCSP Responder, you need to provide the HTTP URL and OCSP Responder's Signing certificate. Make sure the OCSP Responder is online while adding the entry. In case OCSP Responder Signing Certificate is updated, you need to manually update the certificate in Security Analytics server.

Procedure

Specify CRL file on HTTP server

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

To specify CRL file on HTTP server:

1. In the Security Analytics menu, select **Administration** > **Security**.
   The Security view is displayed with the **Users** tab open.

2. Click the **PKI Settings** tab.
3. In the **CRLs** section, click +.
4. In the **CRL Type**, select **CRL is located on a HTTP Server** from the drop-down list.
5. In the **URL** field, specify the HTTP URL to access the CRL.
6. Click **Test**.
   The Security Analytics UI displays the extracted information from the CRL.

   Note: If the HTTP URL is located on HTTPS location, the Security Analytics server do not validate the Web Server certificate of the HTTP server on which the CRL is located.
7. Click **Save**.

   The CRL file is successfully added to the Security Analytics server.

Import Local CRL file using Security Analytics UI

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

To import Local CRL file using Security Analytics UI:

1. In the Security Analytics menu, select **Administration** > **Security**.

   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.
3. In the **CRLs** section, click +.

   The CRL Settings dialog is displayed.
4. In the **CRL Type**, select **CRL is available as a File** from the drop-down list.
5. In the CRL file, click Browse to upload the CRL file.

   Note: The CRL file extension should be .crl.
6. Click **Test**.

   The Security Analytics UI displays the extracted information from the CRL.
7. Click **Save**.

   The CRL file is successfully added to the Security Analytics server.

Specify CRL as LDAP Resource using Security Analytics UI

Note: Make sure that the CRL is available and LDAP server is accessible from Security Analytics server.

1. In the Security Analytics menu, select **Administration** > **Security**.

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

2. Click the **PKI Settings** tab.
3. In the **CRLs** section, click +.

   The CRL Settings dialog is displayed.

4. In the **CRL Type**, select **CRL is published as LDAP Resource** from the drop-down list.
5. In the **URL** field, specify the LDAP URL to access the CRL.

   > **Note:** If the LDAP URL contains white spaces, for example, CN=EMC Root CA it is escaped as CN=EMC%20Root%20CA.

6. In the **Username** field, enter the username in the format of Domain/Username.
7. In the **Password** field, enter the password to access the CRL.
8. Click **Test**.

   The Security Analytics UI displays the information extracted from the CRL.

9. Click **Save**.

   The CRL is successfully added to the Security Analytics server.

Specify OCSP Responder using Security Analytics UI

> **Note:** Make sure that the OCSP Responder is reachable from Security Analytics server.

To specify OCSP Responder using Security Analytics UI:

1. In the Security Analytics menu, select **Administration > Security**.

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

2. Click the **PKI Settings** tab.
3. In the **CRLs** section, click +.

   The CRL Settings dialog is displayed.

4. In the **CRL Type,** select H**TTP URL for OCSP Responder** from the drop-down list.
5. In the **URL** field, specify the HTTP URL.
6. In the **Certificate** field, click **Browse** to upload the OCSP Responder Signing certificate.
7. Click **Test**.

The Security Analytics UI displays the information extracted from the OCSP responder signing certificate.

8. Click **Save**.

   The OCSP responder is successfully added to the Security Analytics server.

Configure CRL Settings

You must configure CRL settings to validate the CRL for certificate revocation.

To configure CRL settings:

1. In the Security Analytics menu, select **Administration** > **Security**.

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

2. Click the **PKI Settings**]tab.
3. In the **CRL Settings** section, select any one of the following **Failure Mode** option.
   - Allow Users to login if Revocation check fails - This allows user to access the Security Analytics server if:
     - The CRL is not found for a user certificate issuer.
     - The user certificate is not revoked but the CRL is expired.
     - The OCSP server is not reachable.
   - Block Users to login if Revocation Check fails - This allows user to login if :
     - CRL is available for user certificate issuer.
     - User certificate is revoked and CRL is valid.
     - OCSP server is reachable and user certificate is valid.
4. In the **Revocation Check Mode** field, select the mode on how the user certificate should be validated.
   - If you select a **CRL only** mode, the CRL is considered valid if the following criteria are met:
     - There should exist a CRL which is issued by the same issuer of a user certificate.
     - The CRL is not expired.
     - The CRL is properly signed by the issuer.
   - If you select a **O CSP only** mode, the OCSP is considered valid if the following criteria are met:

    - There should exist OCSP Responder which is issued by the same issuer of a user certificate.
    - The OCSP Responder is not expired.
    - The OCSP Responder is properly signed by the issuer.

- If you select a **CRL then OCSP**, the following criteria should be met:
    - The user certificate should be valid.
    - If the user certificate is valid in the above step then the user certificate is validated using OCSP Responder.
    - You will be consider valid only if it is not revoked in CRL and is valid using OCSP Responder.

5. In the **Multi CRL Mode** field, select the CRL mode on how the CRL is to be processed when a user has multiple CRLs from the same issuer.
    - Check Revocation in Most Recently Issued CRL - The CRL that has the highest issue date is considered as most recently used CRL.
    - Check Revocation in Last Expiring CRL - The CRL that has the highest expiry date is considered as last expiring CRL.
    - Combine All CRLs for Revocation Check - All the revoked certificate in the CRLs is considered revoked.

    Note: If there are more than one CRL, a CRL is considered unique on the basis of:
     - The date when a CRL is published.
     - The date when a CRL expires.

Next Step:

Step 6. Enable PKI

Step 6. Enable PKI

This topic describes the procedure to enable Public Key Infrastructure (PKI) authentication on Security Analytics.

Prerequisites

To enable PKI, make sure that:

- At least one Active Directory (AD) is configured and enabled on Security Analytics. This AD must be reachable and the roles must be mapped.

> **Note:** PAM is not supported for PKI authentication.

- One Server Certificate is configured and set as 'Use as Server Certificate'.
- One Trusted CA certificate is configured.

Procedure

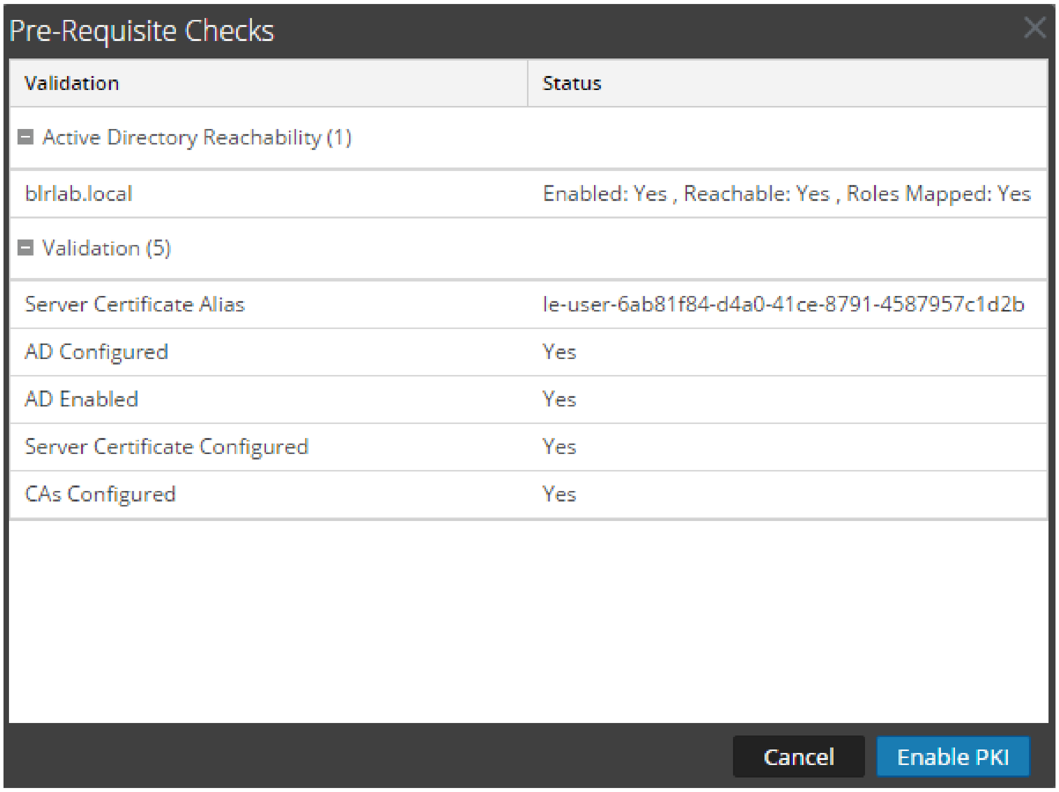
Enable PKI Authentication

To enable PKI authentication:

1. In the **Security Analytics** menu, select **Administration > Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **Settings** tab.
3. In the **Enable PKI** section, select the **Enable PKI** checkbox.

4. Click **Apply**.

   The Pre-Requisite Checks dialog is displayed.



Pre-Requisite Checks

Validation	Status
⊟ Active Directory Reachability (1)	
blrlab.local	Enabled: Yes , Reachable: Yes , Roles Mapped: Yes
⊟ Validation (5)	
Server Certificate Alias	le-user-6ab81f84-d4a0-41ce-8791-4587957c1d2b
AD Configured	Yes
AD Enabled	Yes
Server Certificate Configured	Yes
CAs Configured	Yes

5. Click **Enable PKI**.

Note: If all the prerequisites are met, only then you click on **E nable PKI**.

6. Refresh the puppet agent on the Security Analytics host using the following command:

```
puppet agent -t
```

Note: After the puppet refresh, the default Administrator account is disabled and you will be ONLY authenticated using the certificate.

After you enable PKI:

1. Make sure you do not delete the AD configuration and external group mapping that corresponds to the user certificate's domain.
2. To log out from a PKI based session, you must close the browser used to access Security Analytics.
3. If audit log is enabled, the user login and activity is logged using the user DN.

System Security and User Management: Additional P rocedures

Use this section when you are looking for instructions to perform a specific task after you enable PKI authentication on Security Analytics (SA).

Topics

- Delete Certificate Revocation List
- Delete Server Certificate and Trusted CA Certificate
- Disable PKI

Delete Certificate Revocation List

This topic describes the procedure to delete a Certificate Revocation List (CRL) file in the Security Analytics.

Delete CRL

To delete a CRL file:

1. In the **Security Analytics** menu, select **Administration > Security**.

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

2. Click the **PKI Settings** tab.

3. In the **CRLs** section, select the CRL file to delete.

4. Click −.

   The CRL file is successfully deleted.

5. Restart Security Analytics server for changes to take effect.

Delete Server Certificate and Trusted CA Certificate

This topic describes the procedure to delete a Security Analytics server certificate with its private key and trusted Certificate Authority (CA) certificate.

Procedures

Delete a Security Analytics Server Certificate with its Private Key

- For a server certificate currently used by Security Analytics:

  1. In the **Security Analytics** menu, select **Administration** > **Security**.
     The Security view is displayed with the **Users** tab open.
  2. Click the **Settings** tab.
  3. Replace the server certificate currently used by Security Analytics, perform the following steps:

     a. In the **Server Certificates** section, import a new server certificate with its private key. For instructions, see Step 3. Import Server Certificate and Trusted CA Certificate.

     b. Select the new server certificate.

     c. Click **Use as Server Certificate**.

     d. Refresh puppet agent using the following command:

     ```
     puppet agent -t
     ```

  5. Delete the old server certificate, click —.

- For a server certificate not used by Security Analytics:

  1. In the **Security Analytics** menu, select **Administration** > **Security**.
     The Security view is displayed with the **Users** tab open.
  2. Click the **Settings** tab.
     In the **Server Certificates** section, select the certificate to delete.
  3. Delete the server certificate, click —.

Delete a Trusted CA Certificate

1. In the **Security Analytics** menu, select **Administration** > **Security**.
   The Security view is displayed with the **Users** tab open.

2. Click the **Settings** tab.
3. In the **CA Certificates** section, select the certificate to delete.
4. Click −.

Disab le PKI

This topic describes the procedure to disable Public Key Infrastructure (PKI) authentication.

For some reason if you (Security Analytics user or Administrator) are unable to access the Security Analytics UI and would like to revert to user name and password based authentication, you must disable PKI using the command line.

Disable PKI

1. From the command line, stop the jetty server:
   ```
   stop jettysrv
   ```
2. Stop the puppet agent:
   ```
   service puppet stop
   ```
3. Edit the `/etc/puppet/hieradata/common.yaml` file and set
   ```
    jetty_pki_enabled: false.
   ```
4. Remove the security configuration file.
   ```
   rm
   /var/lib/
   netwitness/uax/conf/securityConfiguration.cfg
   ```
   However, this resets the **Security Settings** in the **Settings tab** to default values.
5. Restart the jetty server:
   ```
   start jettysrv
   ```
6. Restart the puppet agent:
   ```
   service puppet start
   ```
7. Reconfigure the **Security Settings** in the Settings tab. For more information, see the **Settings Tab** topic in the *Hosts and Services Configuration Guides*.

System Security and User Management: References

This topic is a collection of references for system security and user management in Security Analytics.

Topics

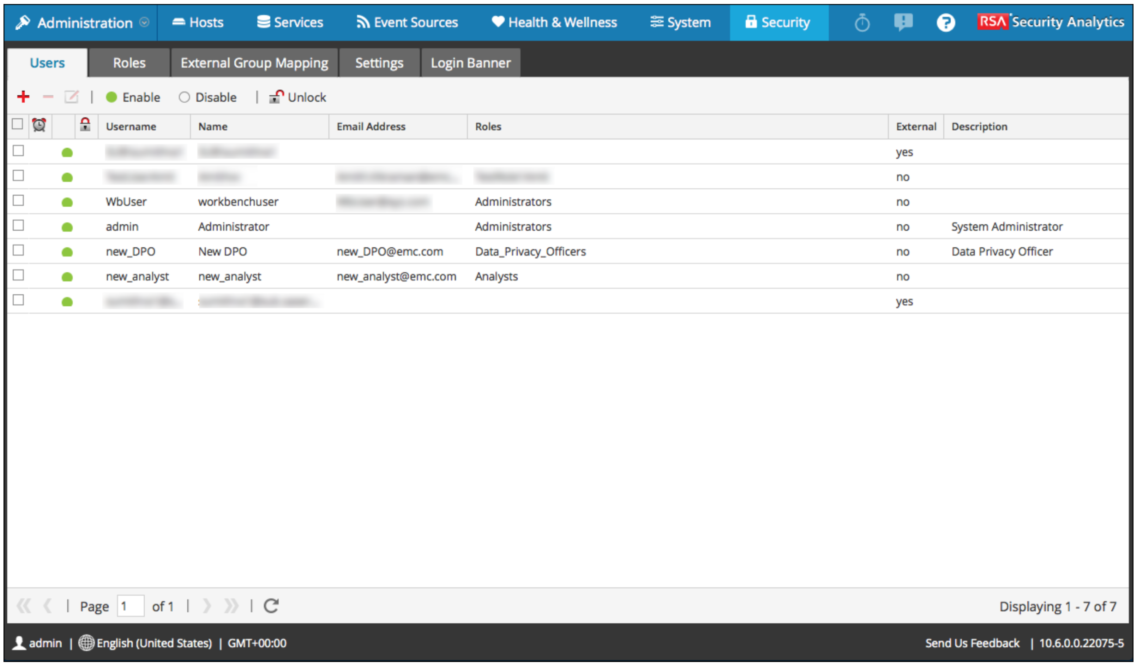
- Administration Security View
- Certificate Attributes

Administration Security V iew

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

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

To display this view, in the **Security Analytics** menu, select **Administration > Security**.



□	⏰		🔒	Username	Name	Email Address	Roles	External	Description
□		●		[redacted]	[redacted]			yes	
□		●		[redacted]	[redacted]	[redacted]	[redacted]	no	
□		●		WbUser	workbenchuser	[redacted]	Administrators	no	
□		●		admin	Administrator		Administrators	no	System Administrator
□		●		new_DPO	New DPO	new_DPO@emc.com	Data_Privacy_Officers	no	Data Privacy Officer
□		●		new_analyst	new_analyst	new_analyst@emc.com	Analysts	no	
□		●		[redacted]	[redacted]			yes	

The **Administration Security** view has five 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 Security Analytics users and to configure system behavior due to failed logins and inactivity. It also provides a way to configure external authentication.
- The **Login Banner** tab provides a way to set conditions which must be agreed to before gaining access to the login screen.

Topics

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

Add or Edit Role Dialog

This topic introduces the Add User and Edit User dialogs accessible from the **Administration** > **Security** > **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.

To access this view:

1. In the **Security Analytics** menu, select **Administration** > **Security**.

   The Security view opens to the **Users** tab by default.

2. Click the **Roles** tab.

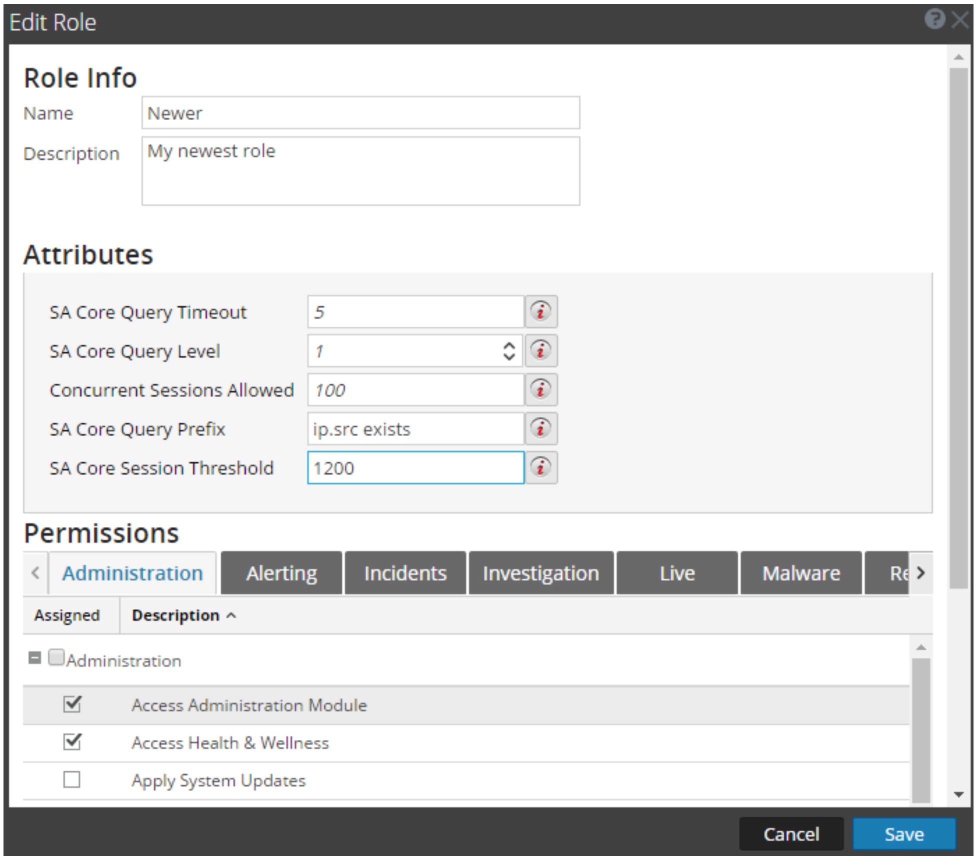
3. Do one of the following:

   - 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.



Role Info

Name: Newer

Description: My newest role

Attributes

SA Core Query Timeout	*5*
SA Core Query Level	*1*
Concurrent Sessions Allowed	*100*
SA Core Query Prefix	ip.src exists
SA Core Session Threshold	1200

Permissions

Administration | Alerting | Incidents | Investigation | Live | Malware | Re

Assigned	Description
□	Administration
☑	Access Administration Module
☑	Access Health & Wellness
□	Apply System Updates

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
SA 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 Security Analytics 10.5 and later, if there is no value set in the roles, 5 minutes is set by default. **Note:** Security Analytics 10.5 and later Core services use this field.
SA Core Query Level	(Optional) Specifies the maximum number of minutes that a user can run a query. There are three query levels: 1, 2, and 3. The default query levels are Query Level 1 = 60 minutes, Query Level 2 = 40 minutes, and Query Level 3 = 20 minutes. **Note:** Security Analytics 10.4 and earlier Core services use this field. Query Level is deprecated for Core services starting with Security Analytics 10.5.
Concurrent Sessions Allowed	Specifies the maximum number of Concurrent Sessions Allowed for a user. The default value is 100. If this value is set, it must be 1 or greater.
SA 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.

Feature	Description
SA 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 **Profile > Preferences > Investigation**.

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.

Add or Edit User Dialog

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

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

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

1. In the **Security Analytics** menu, select **Administration > Security**.

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

2. Do one of the following:

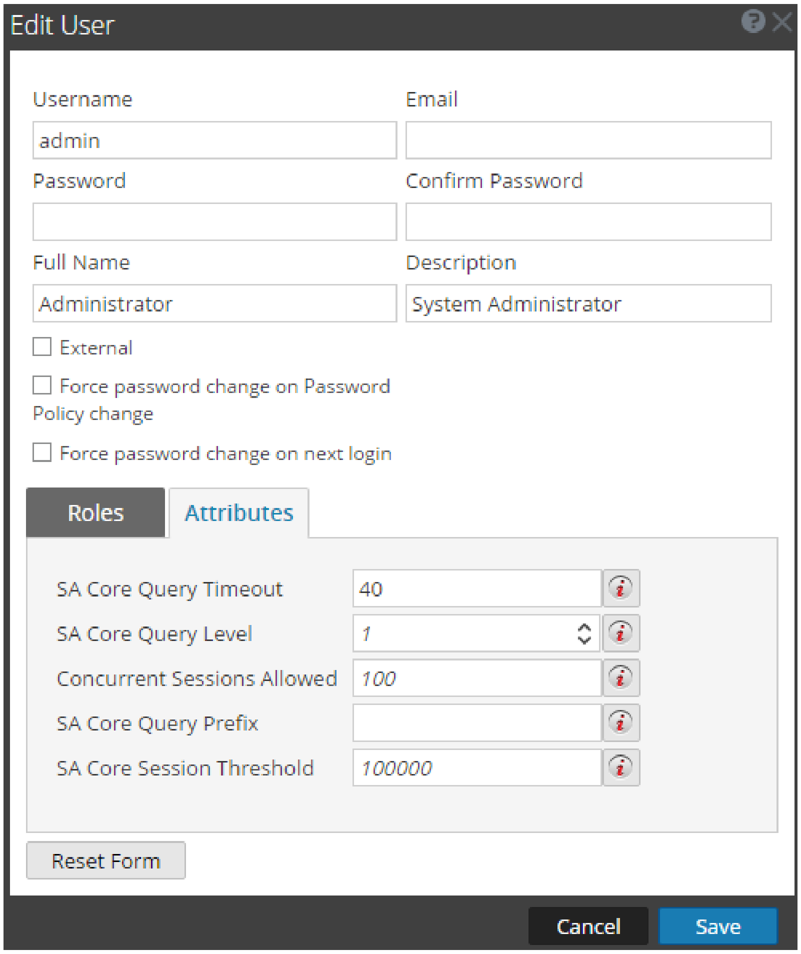
   - In the action bar, click ✚.

     The **Add User** dialog is displayed.

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

     The **Edit User** dialog is displayed.

The Add User dialog is identical to the Edit User dialog shown here.



Username	admin
Email	
Password	
Confirm Password	
Full Name	Administrator
Description	System Administrator

□ External

□ Force password change on Password Policy change

□ Force password change on next login

SA Core Query Timeout	40
SA Core Query Level	1
Concurrent Sessions Allowed	100
SA Core Query Prefix	
SA Core Session Threshold	100000

The Add User and Edit User dialogs show:

- User information
- Roles to which the user belongs
- Security settings for queries

User Information

The following table provides descriptions of the user information.

Field	Description
Username	Username for the Security Analytics user account.
Full Name	Name of the user.

Field	Description
Password and Confirm Password	Password to log on to Security Analytics.
Email	Address of the user.
Description	(Optional) Description of the user.
External	Indicates the user is authenticated externally by Active Directory or PAM, rather than internally by Security Analytics.
Force password change on Password Policy change	Requires the user to change their password (at the next log on) when there are changes to the Security Analytics password strength policy. This field applies only to internal users.
Force password change on next login	Expires the user password the next time the user logs on to Security Analytics. 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.
Cancel	Closes the dialog.
Save	Saves changes.

Roles Tab

The following table provides descriptions of the Roles tab features.

Feature	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.

Attributes Tab

The following table describes fields on the Attributes tab. You should not set these query-handling attributes at the user level unless you want to override assigned role settings. If you do not specify these settings for individual users, the settings are applied to users based on their role memberships. Step 3. Verify Query and Session Attributes per Role and Verify Query and Session Attributes per User provide additional information.

A value shown in italics indicates a default value, for example, *100000*. A value shown without italics indicates a change from the default value, for example, 40.

Field	Description
SA Core Query Timeout	(Optional) Specifies the maximum number of minutes that a user can run a query. This timeout only applies to queries performed from Investigation. By default, this is blank. If you specify a value, it overrides the assigned role settings. If this value is set, it must be zero (0) or greater. A value of zero represents no timeout. **Note:** Security Analytics 10.5 and later Core services use this field.
SA Core Query Level	(Optional) Specifies the maximum number of minutes that a user can run a query. There are three query levels: 1, 2, and 3. The default query levels are Query Level 1 = 60 minutes, Query Level 2 = 40 minutes, and Query Level 3 = 20 minutes. **Note:** Security Analytics 10.4 and earlier Core services use this field. Query Level is deprecated for Core services starting with Security Analytics 10.5.
Concurrent Sessions Allowed	Specifies the maximum number of Concurrent Sessions Allowed for a user. The default value is 100. If this value is set, it must be 1 or greater.
SA Core Query Prefix	(Optional) Filters query results to restrict what the user sees. 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.

Field	Description
SA 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 limit you specify here overrides the **Max Session Export** value defined in Profile > Preferences > Investigation. The default value is `100000`.

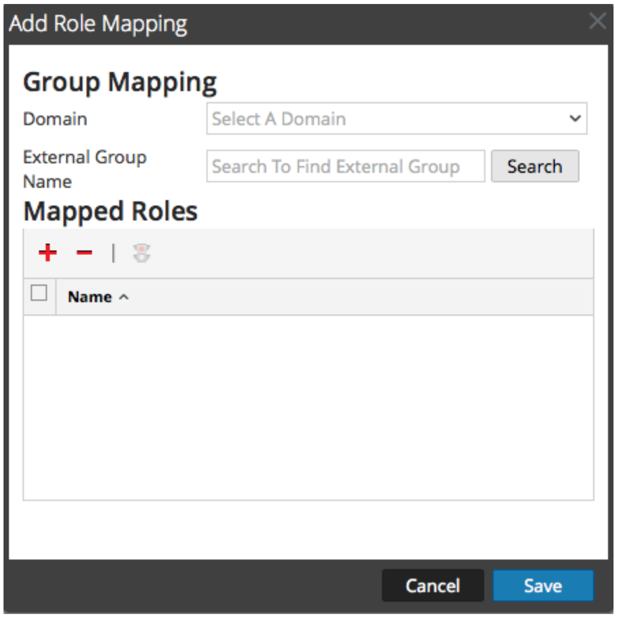
Add Role Mapping Dialog

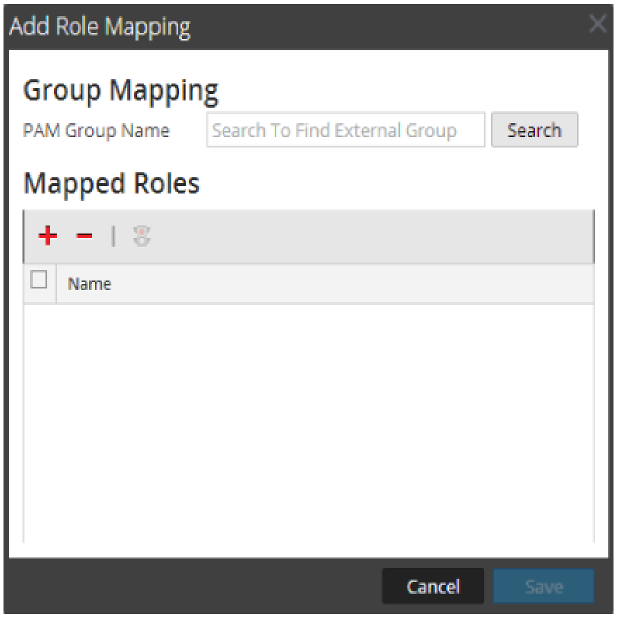
This topic introduces the features of the **Administration** > **Security** view > **External Group Mapping** tab > **Add Role Mapping** dialog.

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

1. In the **Security Analytics** menu, select **Administration > 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.
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 Security Analytics user roles to add are listed.
−	Removes selected roles from the Mapped Roles grid.
Name	Displays the name of the Security Analytics user role.
Permissions	Displays the permissions associated with the Security Analytics 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.

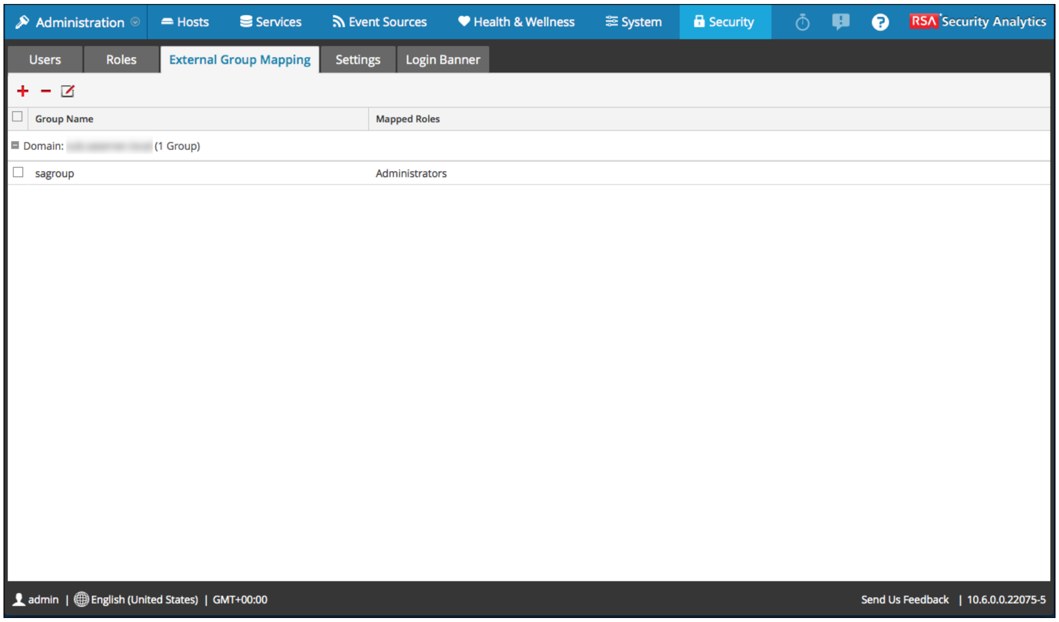
External Group Mapping Tab

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

1. In the **Security Analytics** menu, select **Administration > Security**.

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

2. Click the **External Group Mapping** tab.



□ Group Name	Mapped Roles
Domain: [redacted] (1 Group)	
□ sagroup	Administrators

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

The **grid** has the following features.

Feature	Description
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 Security Analytics.
Mapped Roles	Displays the Security Analytics 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 Security Analytics role.
−	Displays a warning message and asks for confirmation to remove all Security Analytics roles mapped to the external group.
✎	Displays the Edit Role Mapping dialog in which you can add or remove Security Analytics roles from the external group.

Login Banner Tab

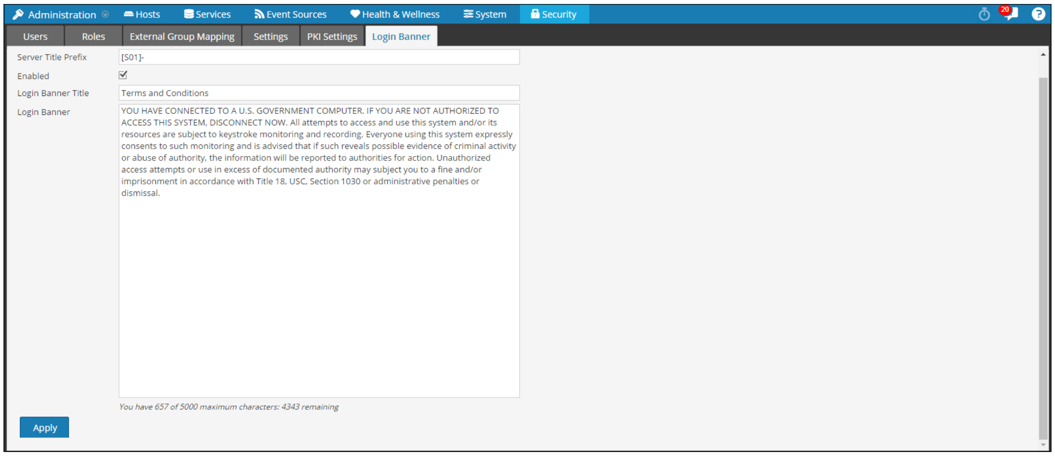
The Login Banner tab provides a way to add a banner to the Security Analytics login screen, which will prevent a user from logging on until they agree to the conditions. And, the server title prefix to differentiate the Security Analytics server of the current tab, when you have deployed multiple Security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

To access the Login Banner tab:

1. In the **Security Analytics** menu, select **Administration** > **Security**.

   The Security view opens to the **Users** tab by default.

2. Click the **Login Banner** tab.



Server Title Prefix: [S01]-

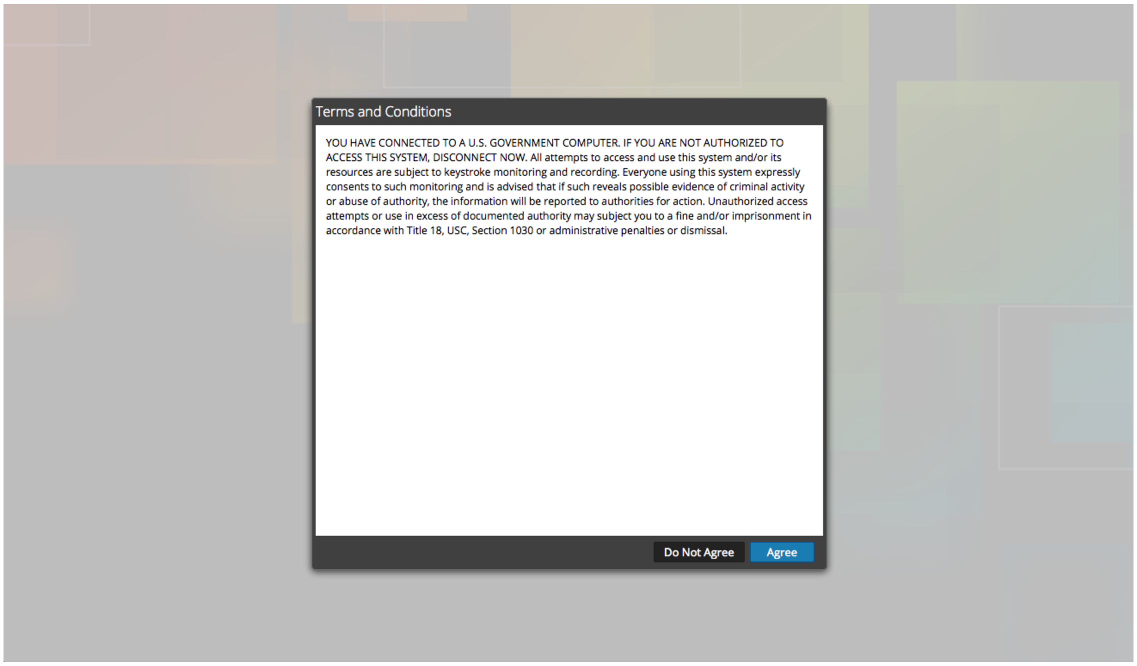
Enabled: ☑

Login Banner Title: Terms and Conditions

Login Banner: YOU HAVE CONNECTED TO A U.S. GOVERNMENT COMPUTER. IF YOU ARE NOT AUTHORIZED TO ACCESS THIS SYSTEM, DISCONNECT NOW. All attempts to access and use this system and/or its resources are subject to keystroke monitoring and recording. Everyone using this system expressly consents to such monitoring and is advised that if such reveals possible evidence of criminal activity or abuse of authority, the information will be reported to authorities for action. Unauthorized access attempts or use in excess of documented authority may subject you to a fine and/or imprisonment in accordance with Title 18, USC, Section 1030 or administrative penalties or dismissal.

You have 657 of 5000 maximum characters: 4343 remaining

When enabled, the banner appears on the Security Analytics login screen.



Terms and Conditions

YOU HAVE CONNECTED TO A U.S. GOVERNMENT COMPUTER. IF YOU ARE NOT AUTHORIZED TO ACCESS THIS SYSTEM, DISCONNECT NOW. All attempts to access and use this system and/or its resources are subject to keystroke monitoring and recording. Everyone using this system expressly consents to such monitoring and is advised that if such reveals possible evidence of criminal activity or abuse of authority, the information will be reported to authorities for action. Unauthorized access attempts or use in excess of documented authority may subject you to a fine and/or imprisonment in accordance with Title 18, USC, Section 1030 or administrative penalties or dismissal.

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

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

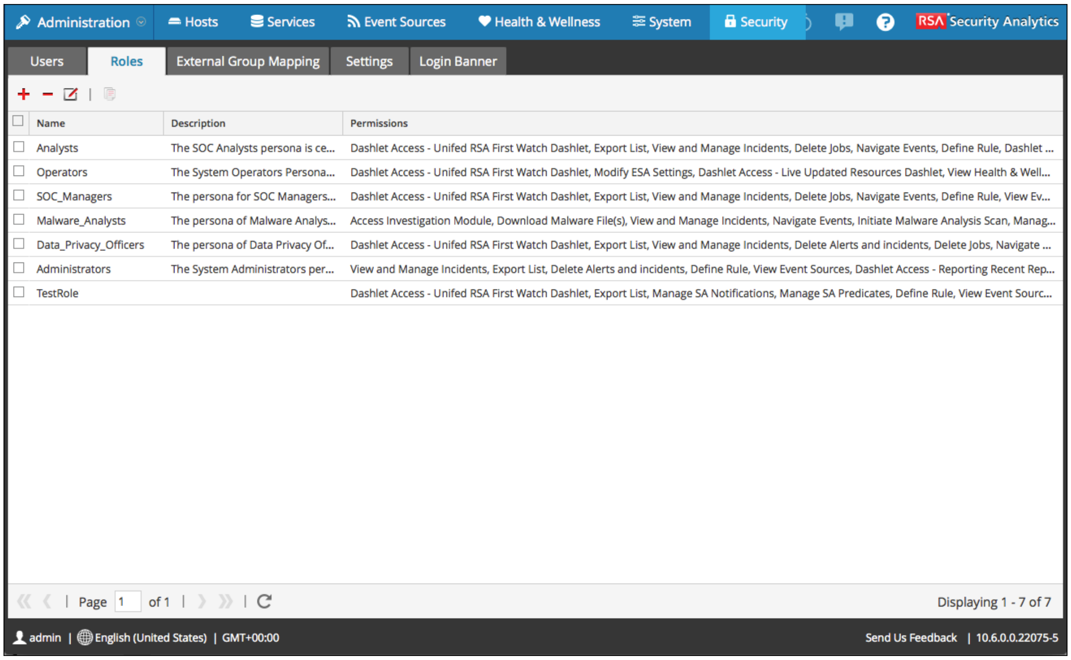
Roles Tab

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

Roles are assigned to all Security Analytics 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.

To access this view:

1. In the **Security Analytics** menu, select **Administration > Security**.
   The Security view opens to the **Users** tab by default.
2. Click the **Roles** tab.



□	Name	Description	Permissions
□	Analysts	The SOC Analysts persona is ce...	Dashlet Access - Unifed RSA First Watch Dashlet, Export List, View and Manage Incidents, Delete Jobs, Navigate Events, Define Rule, Dashlet ...
□	Operators	The System Operators Persona...	Dashlet Access - Unifed RSA First Watch Dashlet, Modify ESA Settings, Dashlet Access - Live Updated Resources Dashlet, View Health & Well...
□	SOC_Managers	The persona for SOC Managers...	Dashlet Access - Unifed RSA First Watch Dashlet, Export List, View and Manage Incidents, Delete Jobs, Navigate Events, Define Rule, View Ev...
□	Malware_Analysts	The persona of Malware Analys...	Access Investigation Module, Download Malware File(s), View and Manage Incidents, Navigate Events, Initiate Malware Analysis Scan, Manag...
□	Data_Privacy_Officers	The persona of Data Privacy Of...	Dashlet Access - Unifed RSA First Watch Dashlet, Export List, View and Manage Incidents, Delete Alerts and incidents, Delete Jobs, Navigate ...
□	Administrators	The System Administrators per...	View and Manage Incidents, Export List, Delete Alerts and incidents, Define Rule, View Event Sources, Dashlet Access - Reporting Recent Rep...
□	TestRole		Dashlet Access - Unifed RSA First Watch Dashlet, Export List, Manage SA Notifications, Manage SA Predicates, Define Rule, View Event Sourc...

The Roles tab consists of the Roles **grid** 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.

Feature	Description
🗐	Duplicates a role to save with a different name.

The following table describes the grid 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.

Search External Groups Dialog

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

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

To access this dialog:

1. In the **Security Analytics** menu, select **Administration > Security**.

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

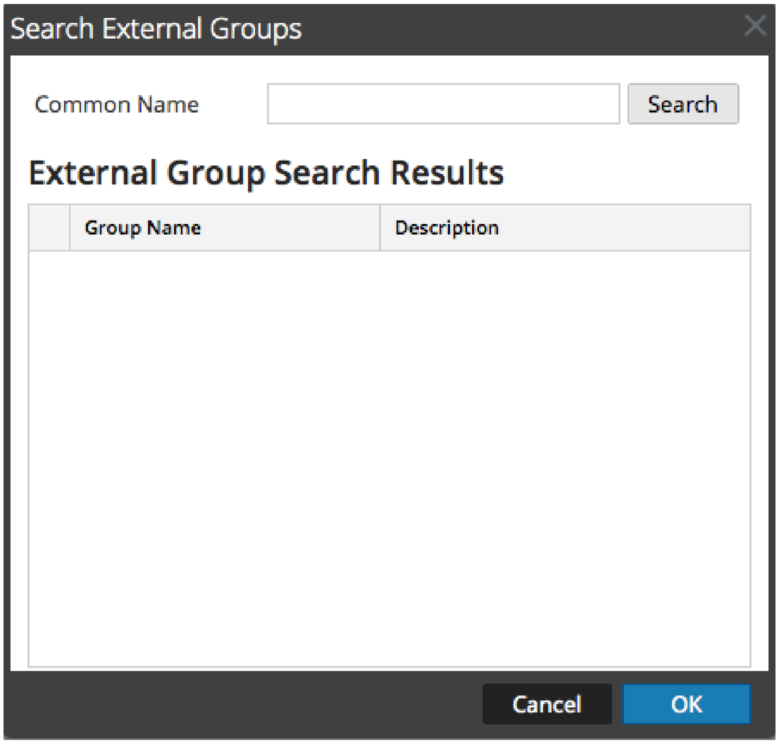
2. Click the **External Group Mapping** tab.

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 Administration Security view > Settings tab. In the Settings tab, you configure password complexity for internal Security Analytics users and system-wide security parameters.

For information on configuring these parameters, 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.

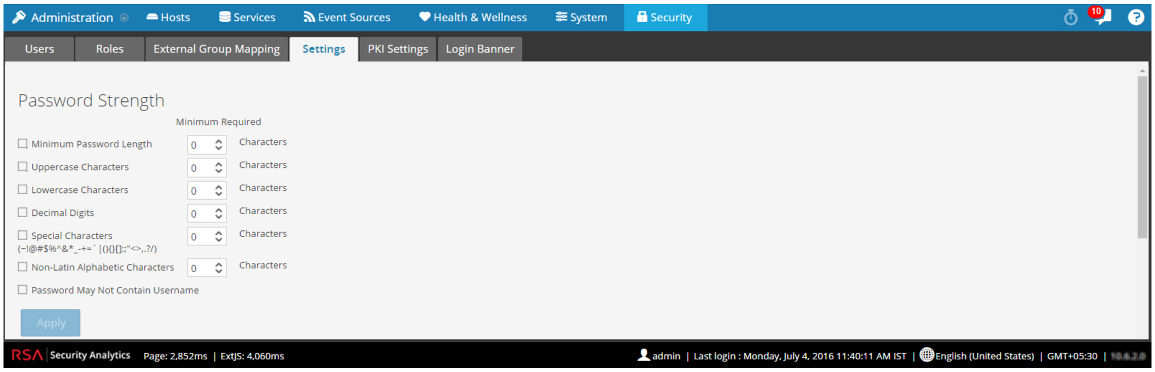
To access the Settings tab:

1. In the **Security Analytics** menu, select **Administration > Security**.

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

2. Click the **Settings** tab.

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

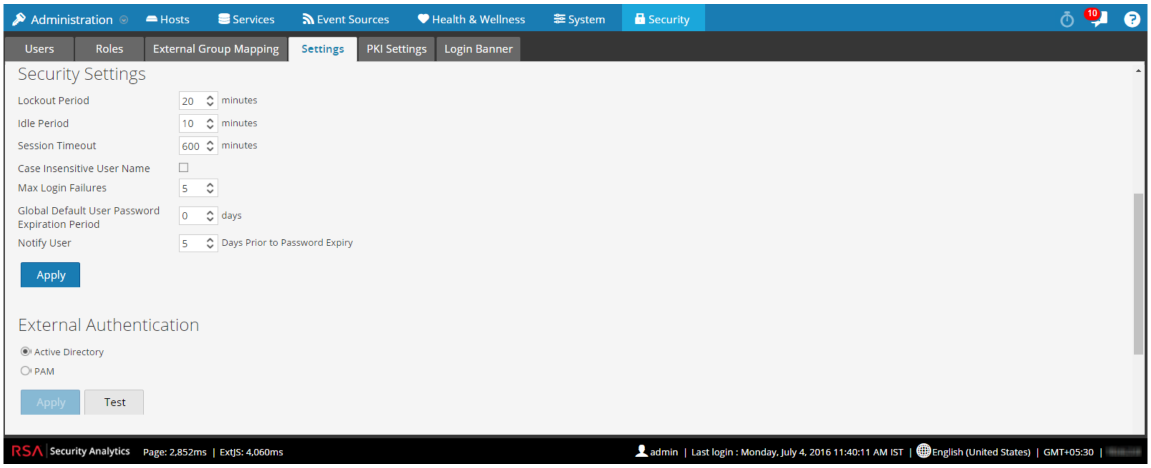


Password Strength

	Minimum Required	
□ Minimum Password Length	0	Characters
□ Uppercase Characters	0	Characters
□ Lowercase Characters	0	Characters
□ Decimal Digits	0	Characters
□ Special Characters (~!@#$%^&*_-+=`|(){}[]:;"<>,.?/)	0	Characters
□ Non-Latin Alphabetic Characters	0	Characters
□ Password May Not Contain Username		

Page: 2,852ms | ExtJS: 4,060ms   admin | Last login : Monday, July 4, 2016 11:40:11 AM IST | English (United States) | GMT+05:30 | [redacted]

The following figure shows the Security Settings and External Authentication sections of the Settings tab.



Security Settings

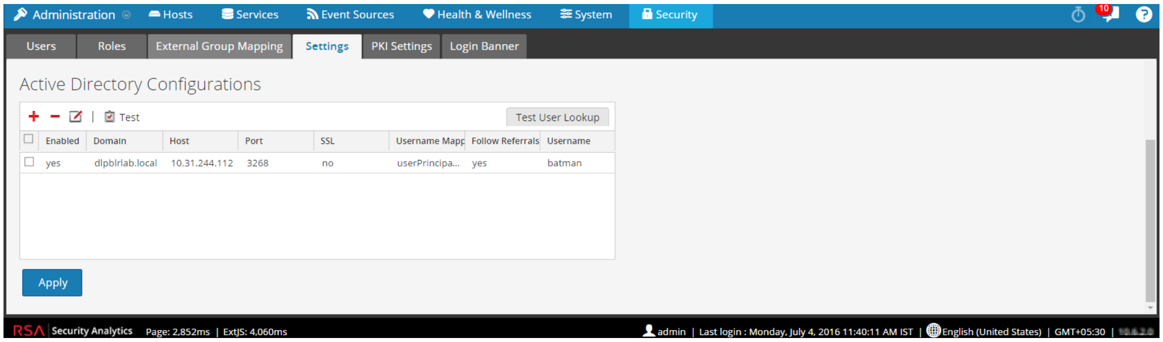
Lockout Period	20	minutes
Idle Period	10	minutes
Session Timeout	600	minutes
Case Insensitive User Name	□	
Max Login Failures	5	
Global Default User Password Expiration Period	0	days
Notify User	5	Days Prior to Password Expiry

External Authentication

● Active Directory
○ PAM

Page: 2,852ms | ExtJS: 4,060ms   admin | Last login : Monday, July 4, 2016 11:40:11 AM IST | English (United States) | GMT+05:30 | [redacted]

The following figure shows the Active Directory Configurations section of the Settings tab.



Active Directory Configurations

□	Enabled	Domain	Host	Port	SSL	Username Mapp	Follow Referrals	Username
□	yes	dlpblrlab.local	10.31.244.112	3268	no	userPrincipa...	yes	batman

Page: 2,852ms | ExtJS: 4,060ms admin | Last login : Monday, July 4, 2016 11:40:11 AM IST | English (United States) | GMT+05:30 | [redacted]

Password Strength

The Password Strength section enables you to configure password complexity requirements for internal Security Analytics users when they set their passwords.

Feature	Description
Minimum Password Length	Specifies a minimum password length requirement for Security Analytics user passwords. A minimum password length prevents users from using short passwords that are easy to guess.
Uppercase Characters	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 Characters	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
Base 10 Digits	Specifies a minimum number of decimal characters (0 through 9) for the password.

Feature	Description
Special Characters (~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/)	Specifies a minimum number of special characters for the password: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
Non-Latin Alphabetic Characters	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.
Apply	Provides the option to force all internal users to change their passwords the next time they log on to Security Analytics. The confirmation dialog shows the following question: Do you want to force all internal users to change their passwords on the next login? • Selecting **Yes** forces all internal users to change their passwords the next time they log on to Security Analytics and overrides any individual user account settings. • Selecting **No** forces only those internal users with the **Force password change at next login** option enabled in their individual user account settings to change their password the next time they log on to Security Analytics. Password strength settings take effect when Security Analytics users create or change their passwords.

Security Settings

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

Feature	Description
Lockout Period	Number of minutes to lock a user out of Security Analytics after the configured number of failed logins is exceeded. The default value is 20 minutes.
Idle Period	Number of minutes of inactivity before a session times out. The default value is 60. If the value is 0, the session will not timeout.
Session Timeout	The maximum duration of a user session before timing out 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.
Case Insensitive User Name	Specifies that the RSA Security Analytics Username field on the login screen is case insensitive. For example, you could use Admin or admin to log on to Security Analytics.
Max Login Failures	The maximum number of unsuccessful login attempts before a user is locked out. The default value is 5.
Global Default User Password Expiration Period	The default number of days before a password expires for all internal Security Analytics users. A value of zero (0) disables password expiration. For upgrades and new installations, the default value is zero (0).
Notify User <n> Days Prior to Password Expiry	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 Security Analytics. A value of zero (0) disables automatic password expiration notification. If you set the Global Default User Password Expiration Period to zero (0), users do not receive automatic password expiration notifications.
Apply	Makes the settings become effective immediately.

External Authentication

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

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

Active Directory Configurations

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

Feature	Description
Enabled	Enables Active Directory authentication for Security Analytics 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 SSL.
Username Mapping	Indicates the Active Directory search field to use for username mapping. You can specify userPrincipalName (UPN) or sAMAccountName.
User Lookup Filter	This is used to find a username in the Active Directory.

Feature	Description
Follow Referrals	Indicates whether Security Analytics will follow LDAP referrals made by Active Directory.
Username	If Username is provided here, it binds to the Active Directory Service while searching Active Directory groups. This credential is not used for any other purpose.
Apply	Makes settings become effective immediately.

PKI Settings Tab

This topic explains the Public Key Infrastructure (PKI) Settings tab that enables you to configure PKI authentication for Security Analytics. In PKI Settings tab, you can perform the following tasks:

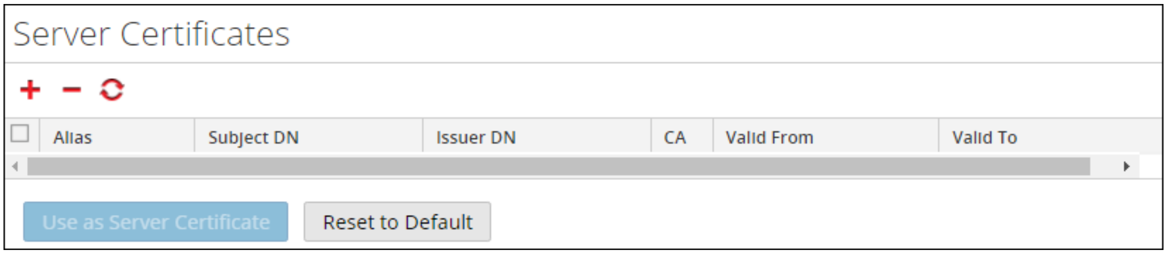
- Import server certificate and trusted CA certifcate
- Import Certificate Revocation List (CRL)
- Configure CRL settings
- Configure user principal settings
- Enable PKI

To access the PKI Settings tab:

1. In the **Security Analytics** menu, select **Administration** > **Security**.
   The Security view is displayed with the **Users** tab open.
2. Click the **PKI Settings** tab.

Server Certificates

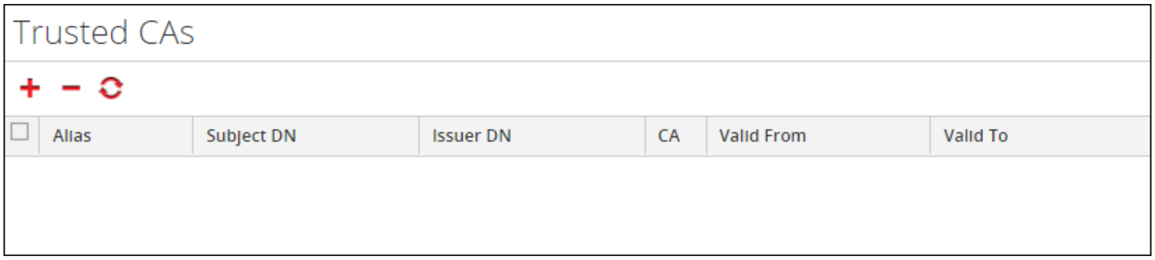
The Server Certificates section enables you to import a server certificate with its private key to Security Analytics server. The following figure shows the Server Certificates of the PKI Settings.



Feature	Description
Alias	A user-friendly name which is used to identify a certificate in a **store**.
Subject DN	The entity to which the certificate is issued.
Issuer DN	The entity which issued the certificate.
CA	Indicates whether the certificate is Certificate Authority (CA).
Valid Form	The start date for the certificate validity.
Valid Till	The end date till when a certificate is valid.
Use as Server Certificate	Uses a server certificate as a default server certificate.
Reset to Default	Restore the default server certificate.

Trusted CAs

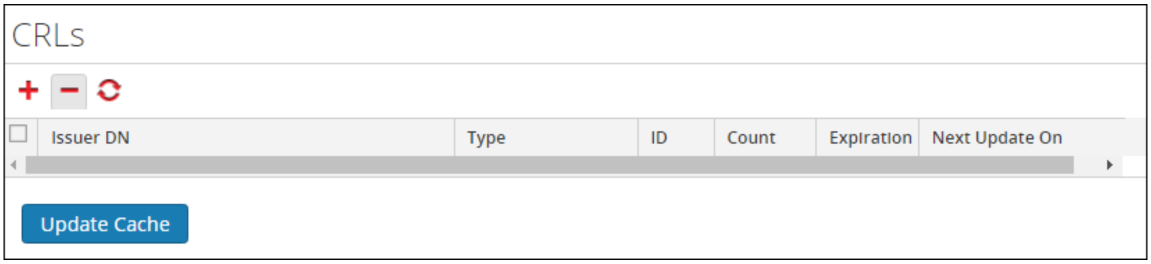
The Trusted CAs section enables you to import a Certificate Authority (CA) certificate to Security Analytics server. The following figure shows the Trusted CAs sections of the PKI Settings.



Feature	Description
Alias	A user-friendly name which is used to identify a certificate in a **store**.
Subject DN	The entity to which the certificate is issued.
Issuer DN	The entity which issued the certificate.
CA	Indicates whether the certificate is Certificate Authority (CA).
Valid Form	The start date for the certificate validity.
Valid Till	The end date till when a certificate is valid.

CRLs

The CRLs allows you to import Certificate Revocation List (CRL) to Security Analytics (SA) server. The following figure shows the CRLs of the PKI Settings.

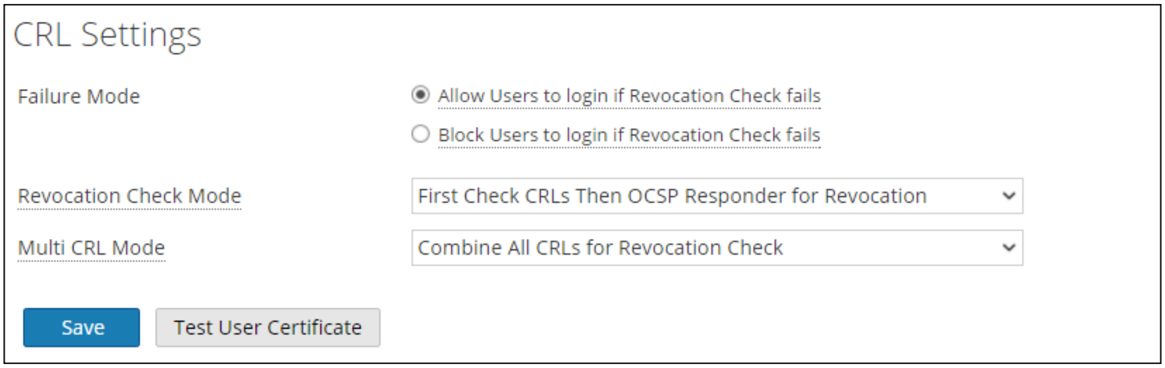


Feature	Description

Feature	Description
Issuer DN	The entity which issued the certificate.
Type	The CRL type which can be a HTTP server, LDAP resource, LOCAL CRL, OCSP Responder.
ID	This is a unique id assigned to the CRLs which is useful in identifying a CRL in the alerts and messages.
Count	The total number of unique revoked certificates in the CRL.
Expiration	Status of the CRL. The values can be Expired, Soon expiring, and Vaild. • Expired - The CRL or OCSP Responder certificate is expired. • Soon expiring - The CRL or OCSP Responder certificate will expire in less than 24 hours. • Vaild - The CRL or OCSP Responder certificate is valid atleast for 24 hours.
Next Update on	The date on which CRL will be updated.
Update Cache	Manually updates all the CRLs from the source location.

CRL Settings

This allows you to configure CRL settings to validate the CRL for certificate revocation. The following figure shows the CRL Settings sections of the PKI Settings.



CRL Settings

Failure Mode
● Allow Users to login if Revocation Check fails
○ Block Users to login if Revocation Check fails

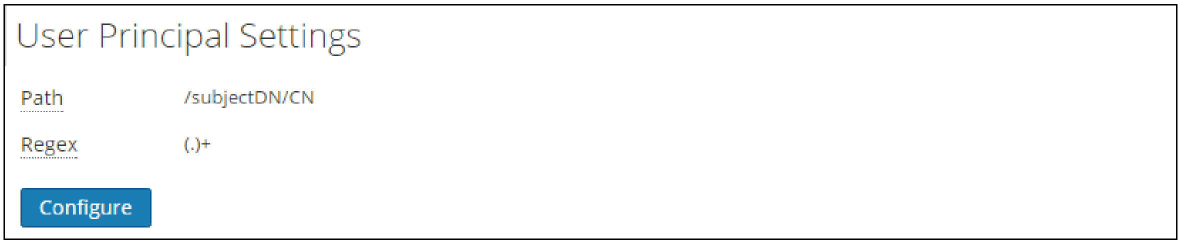
Revocation Check Mode: First Check CRLs Then OCSP Responder for Revocation

Multi CRL Mode: Combine All CRLs for Revocation Check

Feature	Description
Failure Mode	Determines whether a user is allowed to login if the validation fails.
Revocation check Mode	Validates the user certificate for revocation.
Multi CRL Mode	Determines how to process multiple CRLs of the same issuer.
Test User Certificate	This is used to check the certificate revocation based on the CRL and settings applied for the CRL.
Save	Click Save to apply the CRL settings.

User Principal Settings

The User Principal Settings section enables you to specify a field in a certificate to uniquely identify the user for PKI authentication. The following figure shows the Notification Settings, User Principal Settings of the PKI Settings.



User Principal Settings

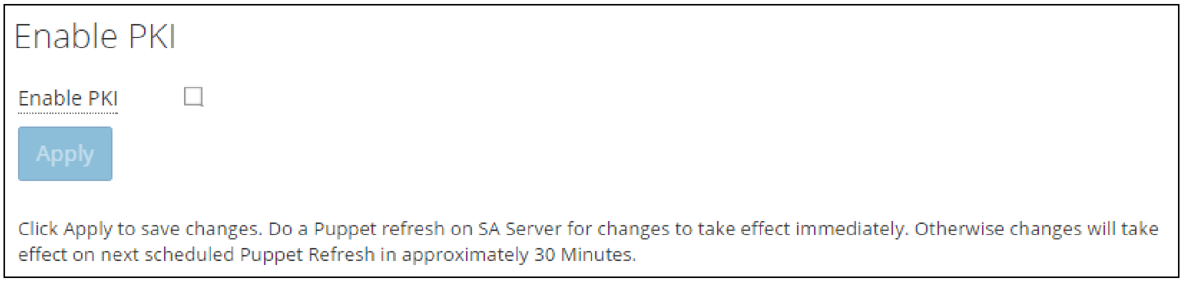
Path /subjectDN/CN

Regex (.)+

Feature	Description
Path	The path to a field in a certificate which is used to extract a username or userid.
Regex	A regular expression that is used to extract the final username or userid from the value in a certificate at a given path.
Configure	Allows you to configure the user principal settings to extract a username or userid.

Enable PKI

The Enable PKI section enables you to enable PKI authentication in Security Analytics. PKI section enables you to enable PKI authentication in Security Analytics. The following figure shows the Enable PKI sections of the PKI Settings.



Click Apply to save changes. Do a Puppet refresh on SA Server for changes to take effect immediately. Otherwise changes will take effect on next scheduled Puppet Refresh in approximately 30 Minutes.

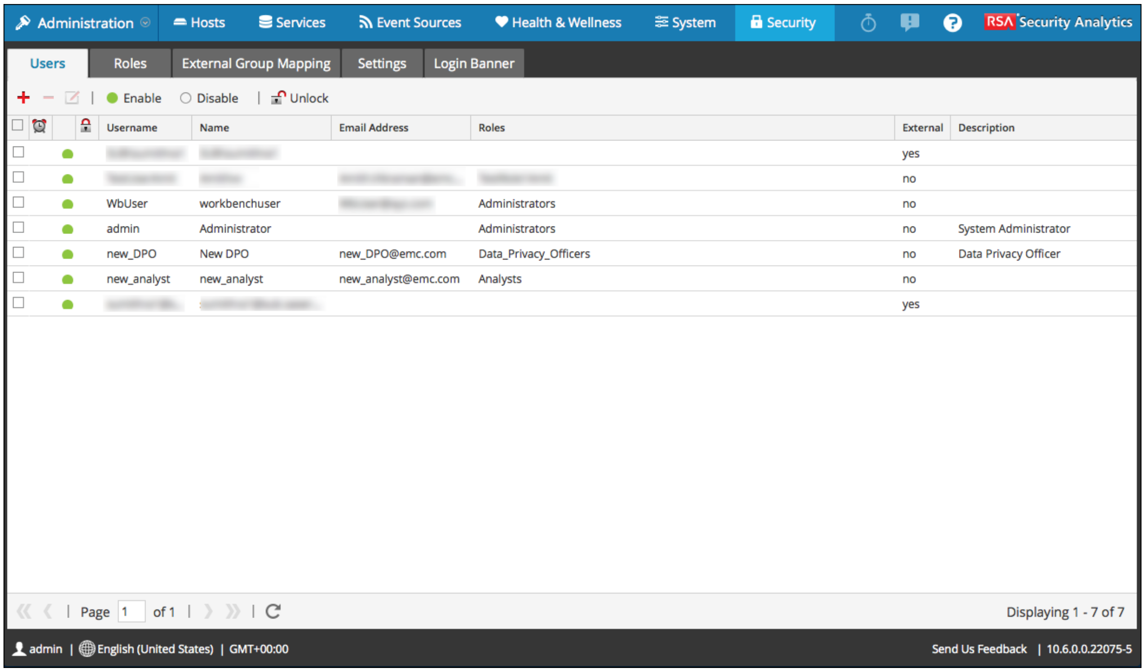
Feature	Description
Enable PKI	Select the option to enable PKI.
Apply	Enables PKI authentication for Security Analytics users.

Users Tab

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

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

To access this view, in the **Security Analytics** menu, select **Administration > Security**. The Security view opens to the **Users** tab by default.



□	⏰		🔒	Username	Name	Email Address	Roles	External	Description
□		●		[redacted]	[redacted]			yes	
□		●		[redacted]	[redacted]	[redacted]	[redacted]	no	
□		●		WbUser	workbenchuser	[redacted]	Administrators	no	
□		●		admin	Administrator		Administrators	no	System Administrator
□		●		new_DPO	New DPO	new_DPO@emc.com	Data_Privacy_Officers	no	Data Privacy Officer
□		●		new_analyst	new_analyst	new_analyst@emc.com	Analysts	no	
□		●		[redacted]	[redacted]			yes	

The Users tab consists of the User grid 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.
● Enable	Enables a disabled user account with all user preferences intact.
○ Disable	Blocks user access without deleting user preferences so that upon re-enabling users, user preferences are intact.

Feature	Description
🔓 **Unlock**	Unlocks a user account that has been locked due to too many failed login attempts.

The **Users** grid 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 Security Analytics.
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 Security Analytics.
Description	Description of the user account.

Certificate Attributes

This topic describes the attributes of a certificate. A certificate contains the following attributes:

- Key Usage
- Enhanced Key Usage

The following table lists the attributes for the user and server certificates.

Certificate Type	Key Usage	Enhanced Key Usage
User Certificate	Digital Signature, Key Encipherment	Client Authentication
Server Certificate	Digital Signature, Key Encipherment	Server Authentication

Note: If the user or server certificate does not contain any of the above mentioned attribute values, RSA recommends that you obtain a new certificate with these attribute values.

System Security and User Management: Troubleshooting

This topic provides information about possible issues that you may encounter when configuring or using Public Key Infrastructure (PKI) authentication.

Possible Issues

This table describes possible problems that you may encounter when you use PKI and solutions to resolve the issues.

Problem	Possible Causes	Solutions
Unable to import `.pfx` file when FIPS is enabled.	Some `.pfx` files may not be built with FIPS compliant algorithm.	Create a `.pfx` file that is built using a FIPS compliant algorithm.
Certificate pop-up is not displayed on the IE browser.	The TLS protocol may not be enabled in the Internet Explorer.	To enable TLS, perform the following steps: 1. In the Internet Explorer, Go to **Tools > Internet Options > Advanced > Settings > Security**. 2. Enable **Use TLS 1.2**.

Problem	Possible Causes	Solutions
Certificate pop-up is not displayed on other browsers.	Certificate is not present in the browser's certificate store.	You must import a certificate to browser's certificate store. For example: To import a certificate on a Mozilla Firefox browser, perform the following steps: 1. Go to **Menu** > **Options** > **Advanced** > **Certificates** tab. 2. Click **View Certificates.** 3. Click the **Authorities** tab. 4. Click **Import.** 5. Browse to select the certificate and click **Open.**