

Chapter 11

Editing a User Authentication Policy

This chapter describes how to view and edit a user's authentication policy. An authentication policy determines the user access policy to the JUNOScope software.

A default authentication policy is automatically generated for all users already configured in JUNOScope, all remote RADIUS users who have successfully logged in to JUNOScope, and when a new user is created.

The JUNOScope administrator can edit a user's authentication policy, which includes the following information:

- Maximum login attempts—The number of consecutive login failure attempts allowed.
- Access window—A maximum time interval for the failure attempts, depending on the authentication policy.
- User account status— Either LOCKED or UNLOCKED. If a user account is LOCKED, that user is denied access to the system even if a user provides a valid username and password. The user is denied access until the JUNOScope administrator changes the status to UNLOCKED.

You must have superuser permission to edit an authentication policy for a user.

This chapter includes the following topics:

- Viewing User Authentication Policies on page 120
- Editing a User Authentication Policy on page 121
- Importing Authentication Policy Information on page 123
- Exporting Authentication Policy Information on page 125

Viewing User Authentication Policies

A user authentication policy is automatically generated and displayed in the Authentication Policy table for:

- All users already configured in the JUNOScope software using Settings > Users > Local Authentication
- All remote RADIUS users who have successfully logged in the JUNOScope software
- All new users created using Settings > Users > Local Authentication

To view user authentication policies, do the following:

1. From the JUNOScope main window, click Settings > Users > Authentication Policy. The Authentication Policy dialog box appears.

[Home](#) > [Settings](#) > [Users](#) > Authentication Policy

Users

Authentication Policy

Page 1 of 1
 Displaying 5 authentication policy records of 5 total

User Name	Status	Actions
admin	UNLOCKED	Edit
demo	UNLOCKED	Edit
donice	UNLOCKED	Edit
rouser	UNLOCKED	Edit
nuser	UNLOCKED	Edit

By default, user login information is listed alphabetically by username in the Authentication Policy table in descending order. The username is the name a user uses to log in to the JUNOScope software.

The Authentication Policy table also lists the user account status, either UNLOCKED (the default) or LOCKED. The default is UNLOCKED. If the user account status is UNLOCKED, the user can successfully log in to the JUNOScope software by providing a valid username and password. If the user account status is LOCKED, the user is denied access to the JUNOScope software, even if the user provides a valid username and password, and is redirected to the “The user account is currently locked. Please see the system administrator.” message. A user account remains locked until the JUNOScope administrator unlocks it.

You can edit a user authentication policy by clicking the Edit link in the Actions column. (See “Editing a User Authentication Policy” on page 121.)

Editing a User Authentication Policy

You can edit a user account authentication policy, which consists of the user status, maximum login attempts, and the access window time within which a user must successfully log in.

To edit a user authentication policy, follow these steps:

1. From the JUNOScope main window, click Setting > Users > Authentication Policy. The Authentication Policy dialog box appears.

Home > Settings > Users > Authentication Policy

Users

Authentication Policy

Page 1 of 1
Displaying 5 authentication policy records of 5 total

User Name	Status	Actions
admin	UNLOCKED	Edit
demo	UNLOCKED	Edit
donice	UNLOCKED	Edit
rouser	UNLOCKED	Edit
nuser	UNLOCKED	Edit

Export Import

2. In the Authentication Policy dialog box, click the Edit link in the Action column for the user authentication information you want to edit. The Edit Authentication Policy dialog box appears.

Home | Help | About | Logout
Logged in as: admin

Looking Glass Configuration Inventory Management Monitor Settings

Home > Settings > Users > Authentication Policy

Users

Authentication Policy

Edit Authentication Policy

User Name: demo

Status: UNLOCKED

Maximum Login Attempts: 0

Access Window: Hour(s): 0 Minute(s): 0 Second(s): 0

OK Cancel

Copyright 2003-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.

3. Edit the authentication policy settings that you want.

In the Edit Authentication Policy dialog box, the **User Name** display field displays the name the user uses to log in to the JUNOScope software.

You can modify the following information in the Edit Authentication Policy dialog box:

- **Status**—The user account status: either **UNLOCKED** (the default) or **LOCKED**. If a user account status is **UNLOCKED**, the user can successfully log in to the JUNOScope software by providing a valid username and password. If the account status is **LOCKED**, the user is denied access to the JUNOScope software, even if the user provides a valid username and password, and is redirected to the “The user account is currently locked. Please contact the system administrator.” message.
- **Maximum Login Attempts**—The maximum number of consecutive failure login attempts allowed within the access window for a user. If a user reaches the maximum number of login attempts, the user status automatically becomes **LOCKED**. This field can have a value from 0 to 100. If the maximum login attempts is 0, the authentication policy for the user will not be active, the user account will be assumed to be **UNLOCKED**, and the normal login mechanism will be applied. For the JUNOScope administrator (the initially configured user), the user account is always **UNLOCKED**.
- **Access Window**—The access window for a user account starts when the first login failure occurs for the user account and runs until one of the following occurs:
 - A user successfully logs in. The access window is then reset.
 - A user tries unsuccessfully to log in for the maximum login attempts. The user account is then **LOCKED** and the access window is reset.

The Access Window field can have a minimum value of 0 (for example, all the field minute(s), hour(s), second(s) having a value of 0) and a maximum value of 24 hours for example, the hour(s) field can have a maximum value of 24, while the minute(s) and second(s) fields have a value of 0). The default value is 0. However, individually, the hour(s) field can have a value from 0 to 24, the minute(s) field can have a value of from 0 to 59, and the second(s) field can have a value from 0 to 59. If the Access Window field is 0, the authentication policy for the user account will not be active, and the normal login mechanism will always be applied.

The timer for the access window starts when an invalid login attempt is made on a user account. If a user account is not locked and no further invalid login attempt is tried for that account, the timer for the access window is automatically reset either after a time period equal to the access window or if the user successfully logs in to JUNOScope within the access window period.

If the authentication policy for a user account is set up with 3 Maximum Login Attempts and a 1-hour Access Window, the clock for the Access Window starts at the first unsuccessful attempt when the user types an invalid password to login. If the user makes three unsuccessful attempts within 1 hour, then the user account will be **LOCKED** at the third unsuccessful attempt and will be redirected to the “The user account is currently locked. Please see the system administrator.” message. Any further attempts by the user to log in using the username, even with a valid password, will be denied.

4. Click OK.

Importing Authentication Policy Information

You can import authentication information from another JUNOScope server or you can use the sample XML export-import-sample.xml file as a guide.

Importing device information is useful then you do not want to enter information manually.

To import authentication policy information, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Authentication Policy. the Authentication Policy window appears.

Home > Settings > Users > Authentication Policy

Users

Authentication Policy

Page 1 of 1
Displaying 5 authentication policy records of 5 total

User Name	Status	Actions
admin	UNLOCKED	Edit
demo	UNLOCKED	Edit
donice	UNLOCKED	Edit
rouser	UNLOCKED	Edit
nuser	UNLOCKED	Edit

Export Import

2. Click Import. The Import dialog box appears.

Home > Settings > Users > Authentication Policy

Users

Authentication Policy

Import Authentication Policy

File

Import Options

Ignore

Merge

Override

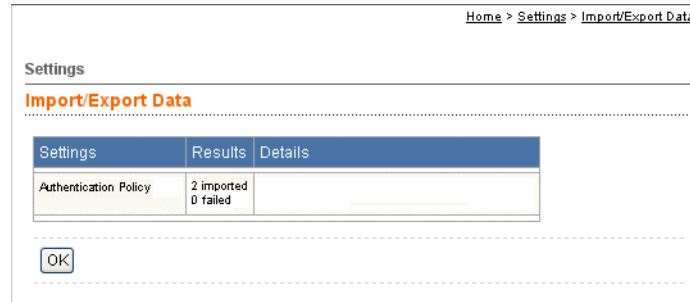
- In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default `schedules.xml` export file from another JUNOScope server or use the provided sample `export-import-sample.xml` XML file on the JUNOScope server to generate a file to import.



NOTE: The `junoscope-` XML file prefix is not generated if you use the Microsoft Internet Explorer 6.0 Web browser to export JUNOScope setup data. You will only see the `schedules` filename.

- To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
 - **Ignore**—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
 - **Merge**—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
 - **Override**—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

- Click Import. The Import status dialog box appears.



The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

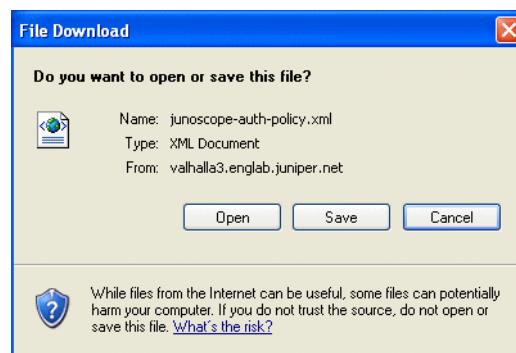
- Click OK. The imported data is listed in the Authentication Policy dialog box.

Exporting Authentication Policy Information

You can export schedule information that you want back up or import to another JUNOScope server.

To export schedule information, follow these steps:

- In the JUNOScope main window, click Settings > Users Authentication Policy. The Authentication Policy dialog box appears.
- Click Export. The File Download dialog box appears.



- Click Save to export the authentication policy information to the local file system in a file named `junoscope-auth-policy.xml`. Click Open to view the contents of the schedule export file.

