

Chapter 12

Setting Up RADIUS Configuration

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. This chapter describes how to configure user authentication on a RADIUS server and in the JUNOScope software so that users with a RADIUS account can log in to the JUNOScope software.

The RADIUS system administrator configures one or more RADIUS servers to share user account information with the JUNOScope software. The JUNOScope software administrator, with superuser permissions, adds the RADIUS server host information in JUNOScope. The JUNOScope administrator then creates one or more template accounts in JUNOScope so that RADIUS users get the appropriate permissions after they log in.

This chapter includes the following topics:

- How RADIUS Configuration Works with JUNOScope on page 128
- Configuring the RADIUS Server on page 129
- Setting Up RADIUS Configuration in JUNOScope on page 133
- Configuring RADIUS Local and Remote Template Accounts in JUNOScope on page 141
- RADIUS User Login Scenarios on page 143

How RADIUS Configuration Works with JUNOScope

This section provides an overview of how JUNOScope RADIUS configuration works to enable remote users with RADIUS accounts to log in with appropriate permissions. The general sequence is as follows:

1. The RADIUS server administrator configures the RADIUS server(s) with Juniper Networks vendor-specific RADIUS attributes and user account records. (See “Configuring the RADIUS Server” on page 129.)
2. The RADIUS administrator ensures that all RADIUS servers are up and running.
3. The JUNOScope software administrator logs in to JUNOScope with superuser permissions, and adds the RADIUS server host information in JUNOScope. (See “Setting Up RADIUS Configuration in JUNOScope” on page 133.)
4. The JUNOScope administrator adds local and remote template accounts as needed in JUNOScope. (See “Configuring RADIUS Local and Remote Template Accounts in JUNOScope” on page 141.)
5. A user with a RADIUS account logs in to the JUNOScope software with username and password.
6. The JUNOScope software forwards a request to the RADIUS server to authenticate the user’s login name.
7. If authentication succeeds, the RADIUS server returns the local username attribute to the JUNOScope software.
8. The template account (user) set up in JUNOScope determines which permissions to provide for the RADIUS user.
9. The user logs in successfully to JUNOScope with the appropriate permissions.

Configuring the RADIUS Server

The sections that follow describe how to modify specific RADIUS server configuration files with Juniper Networks vendor-specific attributes and user account information. All RADIUS servers should comply with RFC 2865.

- Configuring an AAA Merit RADIUS server on page 129
- Configuring an SBR Server on page 130
- Configuring a FreeRADIUS Server on page 132

For other RADIUS servers, modify the configuration files required for that server according to RFC 2138.

Configuring an AAA Merit RADIUS server

This section describes how to configure the `clients`, `dictionary`, `users`, and `vendors` configuration files on an authentication, authorization, and accounting (AAA) Merit RADIUS server. To do so, follow these steps:

1. Modify the RADIUS server `'client'` configuration file as follows:

```
junoscope.server.name secret type=Juniper:nas
```

Replace `junoscope.server.name` with the name of the JUNOScope software server to which you want users to log in. Replace `secret` with the shared secret between the RADIUS server and the client. The Network Access Server (NAS) type is `Juniper`.

2. Modify the RADIUS server `'dictionary'` configuration file as follows:

```
# Juniper Extensions  
Juniper.attr Juniper-Local-User-Name 1 string (1, 0)
```

Where `Juniper-Local-User-Name` is a RADIUS vendor-specific attribute used by Juniper Networks.

3. Modify the RADIUS server `'users'` configuration file used to maintain the permitted users list. For example, to add user `'edward'` with password `'edward'` and local user template `'fritz'`, change the `'users'` configuration file as follows:

```
edward Password = "edward"  
Juniper:Juniper-Local-User-Name = "fritz"
```

The `Juniper:Juniper-Local-User-Name` is optional.

4. Modify the RADIUS server `'vendors'` configuration file as follows:

```
Juniper.attr Juniper.value 2636 Juniper
```

The Juniper Networks RADIUS Vendor ID attribute is `2636`.

Configuring an SBR Server

This section describes how to configure a Steel-Belted RADIUS (SBR) server version 4.7 and other versions of the server.

- Configuring an SBR Server Version 4.7 on page 130
- Configuring Other SBR Server Versions on page 131

Configuring an SBR Server Version 4.7

To modify an SBR server version 4.7, follow these steps:

1. Start the Steel-Belted RADIUS Enterprise Edition Administrator program. The Steel-Belted Radius Administrator window appears.
2. Click the Servers option button.
3. Click either the Local option button (if the server is running locally) or the Remote option button, and specify the IP address of the remote server.
4. Click the Connect option button. A message is displayed in the Status field indicating that the server started and displaying information about the server.
5. Click the RAS Clients option button.
6. Click Add.
7. In the Client Name text box, type a unique client name for the JUNOScope server. You can also use the JUNOScope server DNS name as the client name.
8. Click OK.
9. Type the IP address of the JUNOScope server in the IP Address text field.
10. Select the Juniper M/T Series Make/Model value.
11. Click Edit Authentication Shared Secret, and type the shared RADIUS server secret.
12. Click Set.
13. To add new user accounts, modify the RADIUS server **'users'** configuration. For example, to add a user **'edward'** with password **'edward'** and local user template **'fritz'**, follow these steps:
 - a. Click the Users option button in the SBR Administration window.
 - b. Click the Add option button, and type the RADIUS username **edward**.
 - c. Click OK.
 - d. Click the Set Password option button, and type the password **edward**.
 - e. Make sure that the Allow PAP or CHAP option button is selected.

- f. Click OK.
 - g. Click the Return List Attributes tab from the table.
 - h. Click the Ins option button at the bottom of the table. The Add New Attribute window appears.
 - i. Select the Juniper-Local-User-Name from the Attribute list, and type the corresponding local user template name `fritz` in the text field. The attribute is added to the Return List Attribute table.
14. Click Save to save the configuration.

Configuring Other SBR Server Versions



NOTE: If the RADIUS server you are configuring is other than SBR server version 4.7, perform the steps in this section before configuring the server as described in “Configuring an SBR Server Version 4.7” on page 130.

To configure an SBR server version other than 4.7 (if that version does not already support Juniper vendor-specific attributes) to make it capable of returning Juniper vendor-specific attributes in an “access-accept” packet, follow these steps:

1. Copy the custom dictionary text into the “radius/service/Juniper.dct” file:

```
#####
#
# This dictionary contains Juniper Vendor Specific Attributes
#
# (See README.DCT for more details on the format of this file)
#####

# Use the Radius specification attributes
#
@radius.dct

#
# Juniper specific parameters
#
MACRO Juniper-VSA(t,s) 26 [vid=2636 type1=%t% len1=+2 data=%s%]

ATTRIBUTE Juniper-Local-User-Name Juniper-VSA(1, string) r
ATTRIBUTE Juniper-Allow-Commands Juniper-VSA(2, string) r
ATTRIBUTE Juniper-Deny-Commands Juniper-VSA(3, string) r
ATTRIBUTE Juniper-Allow-Configuration Juniper-VSA(4, string) r
ATTRIBUTE Juniper-Deny-Configuration Juniper-VSA(5, string) r

#####

# Juniper.dct - Juniper Networks dictionary
#####
```

2. Copy the following text into the “radius/service/vendor.ini” file:

```
vendor-product = Juniper M/T Series
dictionary = Juniper
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```

3. Add the following line to the “radius/service/dictiona.dcm” file:

```
@juniper.dct
```

4. Restart the RADIUS server to add the changes. A new Juniper RAS client model appears in the Steel-Belted Radius Administrator window. The Juniper vendor-specific attributes are available in the Return List Attributes list under a particular user.

Configuring a FreeRADIUS Server

To configure a FreeRADIUS server, follow these steps:

1. Modify the RADIUS server ‘clients.conf’ configuration file as follows:

```
client junoscope.server.IPAddress {
    secret = junoscope
    shortname = junoscope.server.name
}
```

Replace `junoscope.server.IPAddress` with the IP address of the JUNOScope software server to which you want users to log in. Replace `junoscope` with the shared secret between the RADIUS server and the client. Replace `junoscope.server.name` with the DNS name of the JUNOScope software server to which you want users to log in.

2. Modify the RADIUS server 'dictionary.juniper' configuration file as follows:

```
# Juniper Extensions
ATTRIBUTE    Juniper-Local-User-Name        1        string    Juniper
```

Where `Juniper-Local-User-Name` is a RADIUS vendor-specific attribute used by Juniper Networks.

3. Modify the RADIUS server 'users' configuration file for maintaining the permitted users list. For example, to add user 'Edward' with password 'Edward' and local user template 'fritz', change the 'users' configuration file as follows:

```
Edward Auth-type:=Local, User-Password = "Edward"
Juniper-Local-User-Name = "fritz"
```

The `Juniper-Local-User-Name` is optional.

4. Modify the RADIUS server 'dictionary.juniper' configuration file as follows:

```
VENDOR Juniper 2636
```

The Juniper Networks RADIUS Vendor ID attribute is 2636.

Setting Up RADIUS Configuration in JUNOScope

For each RADIUS server with user accounts that should have access to JUNOScope, you must add that server host information in the JUNOScope software.

To set up RADIUS configuration in JUNOScope, see the following sections:

- Adding a RADIUS Configuration in JUNOScope on page 133
- Copying a RADIUS Configuration on page 135
- Editing a RADIUS Configuration on page 136
- Deleting a RADIUS Configuration on page 137
- Exporting RADIUS Configurations on page 138
- Importing RADIUS Configurations on page 139

Adding a RADIUS Configuration in JUNOScope

To add RADIUS server host information to JUNOScope, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. In JUNOScope, click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears. The message “No RADIUS configuration present” appears if you have not previously added a RADIUS configuration.
3. Click Add. The Add RADIUS Configuration dialog box appears.

The screenshot shows the JUNOScope web interface. The top navigation bar includes the Juniper Networks logo, the JUNOScope™ title, and links for Home, Help, About, and Logout. The user is logged in as 'admin'. The main navigation tabs are Looking Glass, Configuration, Inventory Management, Monitor, and Settings. The left sidebar shows a tree view of settings, with 'RADIUS Configuration' selected. The main content area displays the 'Add RADIUS Configuration' dialog box. The dialog box has the following fields:

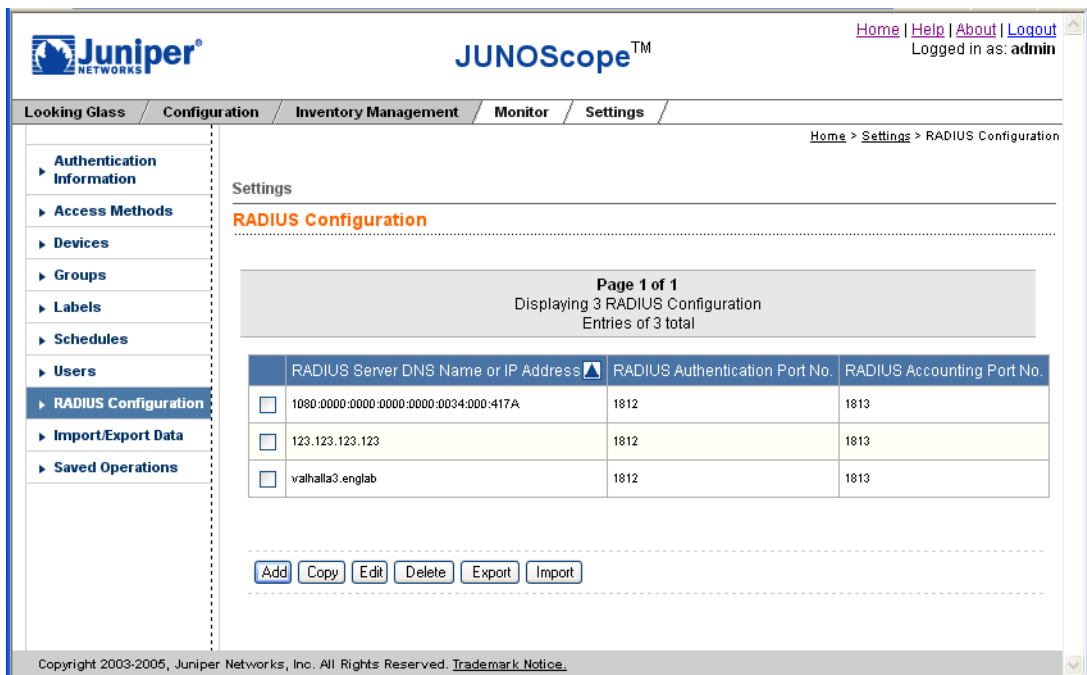
- RADIUS Server DNS Name or IP Address: 1080:0000:0000:0000:0000:0034:0000:417A
- RADIUS Authentication Port No.: 1812
- RADIUS Accounting Port No.: 1813
- RADIUS Server Secret: [masked]
- Confirm RADIUS Server Secret: [masked]

At the bottom of the dialog box are 'OK' and 'Cancel' buttons. The footer of the page contains the copyright notice: Copyright 2003-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.

4. Type the RADIUS server host DNS name or IP address in the text box. The name must be less than 40 characters.
5. Type the RADIUS server port number in the text box. The default port number is 1812. The port number value must be between 1 and 65,535.
6. Type the RADIUS accounting port number in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities that a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535.

The RADIUS server port and the RADIUS accounting ports are optional, however, you must supply at least one of them.

7. Type the RADIUS server secret in the text box. The secret must be less than 40 characters.
8. Type the RADIUS server secret again to confirm it.
9. Click OK. The RADIUS configuration record is listed in the RADIUS Configuration dialog box by RADIUS server DNS name or IP address and RADIUS server port number.



Copying a RADIUS Configuration

You can copy an existing RADIUS configuration record using the RADIUS Configuration Entry dialog box. To save the copied RADIUS configuration, you must change either the RADIUS server DNS name or the IP address and port number.

To copy a RADIUS configuration, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Select the RADIUS configuration record that you want to copy.
4. Click Copy. The Add RADIUS Configuration dialog box appears.

The screenshot shows the JUNOScope web interface. At the top, there is a navigation bar with 'Looking Glass', 'Configuration', 'Inventory Management', 'Monitor', and 'Settings'. The 'Settings' tab is active, and the breadcrumb trail shows 'Home > Settings > RADIUS Configuration'. The main content area displays the 'Add RADIUS Configuration' dialog box. The dialog box has the following fields:

- RADIUS Server DNS Name or IP Address: 1040:0000:0000:0000:0000:0034:0000:218B
- RADIUS Authentication Port No.: 1812
- RADIUS Accounting Port No.: 1813
- RADIUS Server Secret: [Redacted]
- Confirm RADIUS Server Secret: [Redacted]

At the bottom of the dialog box, there are 'OK' and 'Cancel' buttons. The footer of the page contains the copyright notice: 'Copyright 2003-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.'

5. Type the RADIUS server host DNS name or IP address in the text box. The name must be less than 40 characters.
6. Type the RADIUS server port number in the text box. The default port number is 1812. The port number value must be between 1 and 65,535.
7. Type the RADIUS accounting port number in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities that a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535.

The RADIUS server port and the RADIUS accounting ports are optional; however you must supply at least one of them.

8. Type the RADIUS server secret in the text box. The secret must be less than 40 characters.

9. Type the RADIUS server secret again to confirm it.
10. Click OK. The copied RADIUS configuration record is added in the RADIUS Configuration dialog box.

Editing a RADIUS Configuration

You can edit an existing RADIUS configuration record by changing the RADIUS server DNS name, IP address and port number, or RADIUS server secret.

To edit a RADIUS configuration, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Select the RADIUS configuration record that you want to edit.
4. Click Edit. The Edit RADIUS Configuration dialog box appears.

The screenshot shows the JUNOScope web interface. At the top, there is a Juniper logo and the text 'JUNOScope™'. On the right, there are links for 'Home | Help | About | Logout' and 'Logged in as: admin'. Below the header, there are navigation tabs: 'Looking Glass', 'Configuration', 'Inventory Management', 'Monitor', and 'Settings'. The 'Configuration' tab is selected. On the left, there is a sidebar with a tree view containing the following items: Authentication Information, Access Methods, Devices, Groups, Labels, Schedules, Users, RADIUS Configuration (highlighted), Import/Export Data, and Saved Operations. The main content area shows the 'Edit RADIUS Configuration' dialog box. The dialog box has a title bar 'Edit RADIUS Configuration' and contains the following fields:

- RADIUS Server DNS Name or IP Address: 1040:0000:0000:0000:0000:0034:0000:219B
- RADIUS Authentication Port No.: 1812
- RADIUS Accounting Port No.: 1813
- RADIUS Server Secret:
- Confirm RADIUS Server Secret:

 At the bottom of the dialog box, there are 'OK' and 'Cancel' buttons. The footer of the page contains the text: 'Copyright 2003-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.'

5. Type the RADIUS server host DNS name or IP address in the text box. The name must be less than 40 characters.
6. Type the RADIUS server port number in the text box. The default port number is 1812.

7. Type the RADIUS accounting port number in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities that a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535.

The RADIUS server port and the RADIUS accounting ports are optional; however, you must supply at least one of them.

8. Type the RADIUS server secret in the text box. The secret must be less than 40 characters.
9. Type the RADIUS server secret again in the text box to confirm it.
10. Click OK. The edited RADIUS configuration record appears in the RADIUS Configuration Entry dialog box.

Deleting a RADIUS Configuration

To delete a RADIUS Configuration, follow these steps:

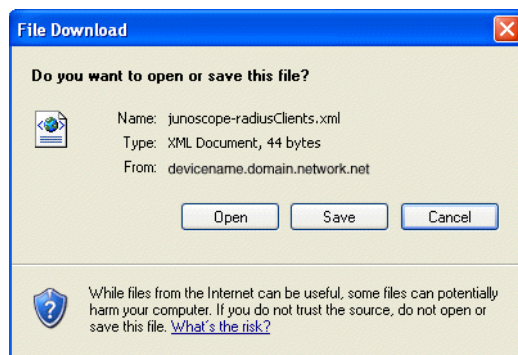
1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Select the RADIUS configuration record that you want to delete.
4. Click Delete. The RADIUS configuration record is deleted from the RADIUS Configuration dialog box and the JUNOScope database.

Exporting RADIUS Configurations

You can export RADIUS configuration information to the local file system or import to another JUNOScope server. You export all RADIUS configuration records to any XML file. The default filename is `radiusClients`.

To export RADIUS configuration records, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Click Export. The File Download dialog box appears.



4. Click Save to save the RADIUS configuration data and export it to the file system in a file named `junoscope-radiusClients.xml`. Click Open to view the contents of the export file.
5. Navigate in the local file system to where you want to save the RADIUS configuration records and click Save. The default RADIUS configuration entries export filename is `radiusClients`.
6. Click Open to view the export XML file content.



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 `radiusClients` filename.

Importing RADIUS Configurations

You can import RADIUS configuration records from another JUNOScope server. You can import any valid XML file.

Importing RADIUS configuration information is useful when you do not want to add RADIUS configuration records manually.

To import RADIUS configuration records, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Click Import. The Import RADIUS Configuration dialog box appears.

[Home](#) > [Settings](#) > [RADIUS Configuration](#)

Settings

RADIUS Configuration

Import RADIUS Configuration

File

Key (if not included in data)

Import Options

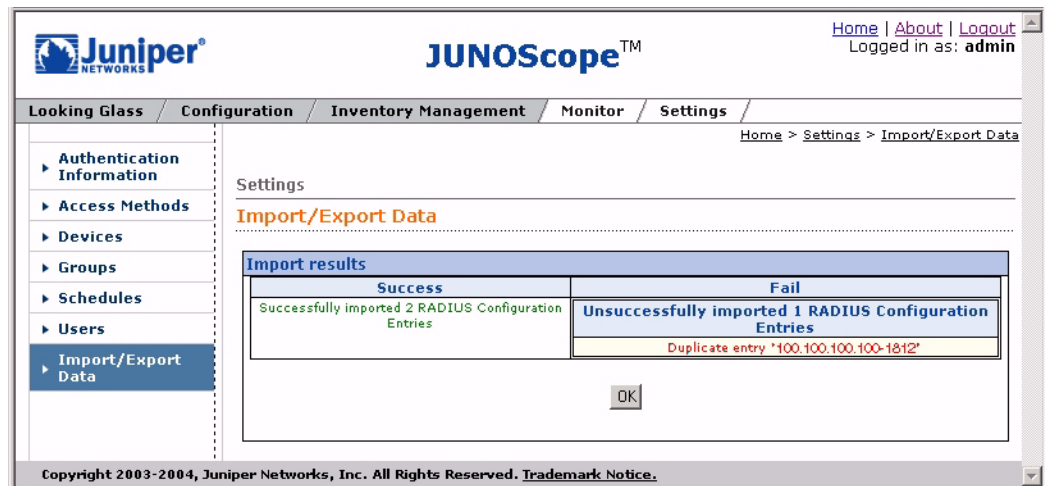
Ignore

Merge

Override

4. Click Browse and navigate to where the `radiusClients` RADIUS configuration file is located.
5. Type the key to decrypt the sensitive authentication information data that you want to import. The key is required if you selected not to include it when the data was exported. This key can be up to 16 characters long and was created during the JUNOScope installation.
6. 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.
7. Double-click the `radiusClients` RADIUS configuration file.
 8. The Import/Export Data dialog box appears confirming successful import of the RADIUS configuration records.



The Import/Export Data dialog box displays the RADIUS configuration records that have been successfully imported, how many records are duplicates, how many records did not import successfully, and any error descriptions.

9. Click OK. The imported RADIUS configuration records appear in the RADIUS Configuration dialog box.

The screenshot shows the JUNOScope web interface. The top header includes the JUNOScope logo and the text "JUNOScope™". On the right, there are links for "Home", "Help", "About", and "Logout", and it indicates the user is logged in as "admin". The main navigation bar includes "Looking Glass", "Configuration", "Inventory Management", "Monitor", and "Settings". The left sidebar contains a menu with options like "Authentication Information", "Access Methods", "Devices", "Groups", "Labels", "Schedules", "Users", "RADIUS Configuration", "Import/Export Data", and "Saved Operations". The main content area is titled "Settings" and "RADIUS Configuration". It shows "Page 1 of 1" and "Displaying 3 RADIUS Configuration Entries of 3 total". Below this is a table with the following data:

	RADIUS Server DNS Name or IP Address	RADIUS Authentication Port No.	RADIUS Accounting Port No.
<input type="checkbox"/>	1080:0000:0000:0000:0000:0034:000:417A	1812	1813
<input type="checkbox"/>	123.123.123.123	1812	1813
<input type="checkbox"/>	valhalla3.englab	1812	1813

Below the table are buttons for "Add", "Copy", "Edit", "Delete", "Export", and "Import". At the bottom of the page, there is a copyright notice: "Copyright 2003-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice."

Configuring RADIUS Local and Remote Template Accounts in JUNOScope

The JUNOScope software uses local password authentication. You set up a username, password, and permissions for each user allowed to log in to JUNOScope.

However, when you use RADIUS authentication, you must set up single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts.

A template account is a mapping between JUNOScope and the RADIUS server that allows RADIUS users to get the appropriate permissions. When a user with a RADIUS account logs in to JUNOScope, the software forwards the username and password to the RADIUS server for authentication. If authentication succeeds, the RADIUS server sends the `Juniper-Local-User-Name` attribute (if present for the user) to JUNOScope. Based on the received `Juniper-Local-User-Name` attribute and the configured template user accounts, JUNOScope determines the permissions for the user. The RADIUS account user gets the same permissions as the template user.

You set up template accounts the same way you create users in JUNOScope. To add a user in JUNOScope, see "Adding a User" on page 112. See also "RADIUS User Login Scenarios" on page 143.

Local Template Accounts

When you configure a local template and a user logs in, the JUNOScope software sends a request to the authentication server to authenticate the user's login name. When a user is authenticated, the RADIUS server returns the local username to JUNOScope. If a local username (for example, the `Juniper-Local-User-Name` attribute) is specified for that login name, the appropriate local template is selected. If no local template is returned by the RADIUS server or no corresponding local template exists in JUNOScope, JUNOScope will, by default, use the remote template (see “Remote Template Accounts” on page 142).

Table 10 shows the user account information that must exist on the RADIUS server and in the local template account or user set up in JUNOScope.

Table 10: Local Template Account

RADIUS Server User Account	JUNOScope Local Template Account
Username: "edward"	Username: fritz
Password: "edward"	Password: fritz
Juniper-Local-User-Name = "fritz"	Permissions: superuser

If a local user logs in to JUNOScope using username `fritz` and password `fritz`, the user will log in successfully with `superuser` permissions. However, if a RADIUS user “`edward`” logs in to JUNOScope successfully using username `edward`, that user gets the same permissions as `fritz`. In this case, user “`edward`” on successful login gets the `superuser` permissions. If you change the permission for `fritz` to `read-write`, user “`edward`”, on successful login, will also get `read-write` permissions.

Remote Template Accounts

There can be only one remote template account in JUNOScope. You configure a remote template in JUNOScope by creating a user with username `remote` and a password with any secure name. (See “Adding a User” on page 112.)

In JUNOScope, a remote template is for a user with username '`remote`' with a RADIUS account when either no `Juniper-Local-User-Name` attribute is specified for that user or the specified local user does not exist in JUNOScope (see Table 11).

For example:

- The `Juniper-Local-User-Name` attribute is not specified for the user on the RADIUS server (see Table 13 on page 144).
- The `Juniper-Local-User-Name` attribute is specified, but the corresponding username is not present in JUNOScope.

Table 11: Remote Template Account

RADIUS Server User Account	JUNOScope Local Template Account
edward password = "edward"	Username: remote
Juniper-Local-User-Name attribute is not specified	Password: remote
	Permissions: superuser

Username “edward” will get the same permissions as the remote template (for example, the same permissions as user `remote`) if configured in JUNOScope.

If neither the local nor remote template is configured in JUNOScope (for example, for RADIUS user “edward”, if both users `fritz` and `remote` do not exist in JUNOScope), the RADIUS user will not be able to log in.

For a user with an account in RADIUS to be able to successfully log in to JUNOScope, JUNOScope must have at least remote user template configured.

RADIUS User Login Scenarios

This section provides several scenarios that describe the user account and template account information that should be configured on the RADIUS server and in JUNOScope for a user to log in to JUNOScope with certain permissions.

All RADIUS servers should be up and running for RADIUS users to log in to JUNOScope successfully.

Scenario 1: Logging In to JUNOScope when a Remote Template Account Is Present

If a user account is present on the RADIUS server, the user should be able to log in to JUNOScope if either the `Juniper-Local-User-Name` attribute is not specified, or the username corresponding to the `Juniper-Local-User-Name` attribute does not exist in JUNOScope, but the username `remote` does (see Table 12). See also “Remote Template Accounts” on page 142.

Table 12: RADIUS Server Setup, JUNOScope User Information, and Login Results

RADIUS Server Configuration	JUNOScope User Setup Information	Successful Login Results
<code>bob password = 'bobpassword'</code>	Username: <code>remote</code>	Username: <code>bob</code>
<code>Juniper-Local-User-Name</code> is not specified	Password: <code>remote</code>	Password: <code>bobpassword</code>
	Permissions: <code>read-only</code>	Permissions: <code>read-only</code>

Scenario 2: Logging In to JUNOScope When a Local Template Account Is Present

If a user account is present on the RADIUS server, the user should be able to log in if the `Juniper-Local-User-Name` attribute is specified and the corresponding local user is set up in JUNOScope (see Table 13).

Table 13: RADIUS Server Setup, JUNOScope User Information, Login Results

RADIUS Server Configuration	JUNOScope User Setup Information	Successful Login Results
edward password = 'edward' Juniper-Local-User-Name = 'fritz'	Username: fritz	Username: fritz
	Password: fritz Permissions: superuser	Password: fritz Permissions: superuser
	Username: remote	Username: edward
	Password: remote	Password: edward
	Permissions: read-only	Permissions: superuser
		Username: edward
		Password: edward
		Permissions: read-only
		(If you delete user fritz first)

Scenario 3: Logging In to JUNOScope when the Same User Account Is Present on the RADIUS Server and in JUNOScope

If the same username and password are present on the RADIUS server and in JUNOScope, the user can log in to JUNOScope using the username and password combination. After login, the user has the permissions that exist in JUNOScope (see Table 14).

Table 14: RADIUS Server Setup, JUNOScope User Information, and Login Results

RADIUS Server Configuration	JUNOScope User Set Up Information	Successful Login Results
honda password = 'honda' Juniper-Local-User-Name = 'fritz'	Username: fritz	Username: fritz
	Password: fritz	Password: fritz
	Permissions: superuser	Permissions: superuser
	Username: honda	Username: honda
	Password: honda	Password: honda
	Permissions: read-only	Permissions: read-only
		Username: honda
		Password: honda
		Permissions: superuser
		(If you delete user honda first)

If the same username is present on the RADIUS server and in JUNOScope, but the passwords on the RADIUS server and in JUNOScope are different, the user can log in using the username and both passwords. After login, the user gets the same permissions as configured on the RADIUS server or locally in JUNOScope depending on whether the username and password combination exists on the RADIUS server or in JUNOScope (see Table 15).

Table 15: RADIUS Server Setup, JUNOScope User Information, Login Results

RADIUS Server Configuration	JUNOScope User Setup Information	Successful Login Results
honda password = 'honda' Juniper-Local-User-Name = 'fritz'	Username: fritz	Username: honda
	Password: fritz	Password: honda
	Permissions: superuser	Permissions: superuser
	Username: honda	Username: honda
	Password: honda123	Password: honda123
	Permissions: read-only	Permissions: read-only

