

Chapter 5

Setting Up Access Methods

This chapter describes how to set up the JUNOScope software to connect to routing platforms on your network for configuration operations.

You can specify the access method (JUNOScript access protocol to connect to the JUNOScript server running on a router) configured on a router for remotely connecting to that router from the JUNOScope software. The JUNOScope software supports secure sockets layer (SSL) and clear-text access protocols. We recommend that you set up access methods before you set up routers.

You can import access method information from another JUNOScope server or export it as backup or for importing to another server.

You must have superuser permissions to set up access methods.

This chapter includes the following topics:

- Understanding the JUNOScript API on page 48
- Supported JUNOScript Access Protocols on page 48
- Prerequisites for Establishing a JUNOScript Server Connection on page 49
- Understanding Authentication Information and Access Methods on page 51
- Adding an Access Method on page 52
- Viewing Access Methods on page 53
- Editing Access Method Information on page 54
- Importing Access Methods on page 55
- Exporting Access Methods on page 57
- Deleting Access Methods on page 57

Understanding the JUNOScript API

The JUNOScript application programming interface (API) is an Extensible Markup Language (XML) application that Juniper Networks routers use to exchange information with client applications. XML is a metalanguage for defining how to mark the organizational structures and individual items in a data set or document with tags that describe the function of the structures and items. The JUNOScript API defines tags for describing router components and configuration.

Client applications can configure or request information from a router by encoding the request with JUNOScript tags and sending it to the JUNOScript server on the router. (The JUNOScript server is a component of the management daemon [mgd process] running on the router and does not appear as a separate entry in process listings.) The JUNOScript server directs the request to the appropriate software modules within the router, encodes the response in JUNOScript tags or formatted ASCII as requested by the client application, and returns the result to the client application. For example, to request information about the status of a router's interfaces, a client application can send the JUNOScript `<get-interface-information>` tag element. The JUNOScript server gathers the information and returns it in the `<interface-information>` tag element. For more information about the JUNOScript server, see the *JUNOScript API Guide*.

Supported JUNOScript Access Protocols

The JUNOScope software uses SSL and clear-text JUNOScript access protocols (see Table 9), which also specify the associated authentication mechanism.

The SSL protocol is preferred because it encrypts security information (such as a password) before transmitting it across the network. The clear-text protocol does not encrypt security information.

Table 9: Supported Access Protocols and Authentication Mechanisms

Access Protocol	Authentication Mechanism
clear-text, a JUNOScript-specific protocol for sending unencrypted text over a Transmission Control Protocol (TCP) connection	JUNOScript-specific
SSL, a JUNOScript-specific protocol for sending encrypted text over a TCP connection	JUNOScript-specific

Prerequisites for Establishing a JUNOScript Server Connection

To create a connection, both the JUNOScript server and the client application must be able to access the software for the access protocol used by the client application. The JUNOScript server can access the protocols listed in Table 9 because the JUNOS software distribution includes them. On most operating systems, client applications can access the software for TCP (used by the JUNOScript-specific clear-text protocol) as part of the standard distribution. For information about obtaining SSL software, see <http://www.openssl.org>.

The following topics describe the prerequisites for establishing a connection with the JUNOScript server:

- Prerequisites for clear-text Connections on page 49
- Prerequisites for SSL Connections on page 50

When the prerequisites are satisfied, the client application connects to the JUNOScript server by opening a socket or other communications channel to the JUNOScript server machine (router) and invoking one of the remote-connection routines appropriate for the programming language and access protocol that the application uses.

Prerequisites for clear-text Connections

If the client application uses the clear-text protocol to send unencrypted text directly over a TCP connection without using any additional protocol (such as SSL), you must activate the `xnm-clear-text` service on port 3221 on the JUNOScript server machine. To do this, follow these steps:

1. Enter command-line interface (CLI) configuration mode on the JUNOScript server machine and issue the following command:

```
[edit]
user@host# set system services xnm-clear-text
```

2. Commit the configuration:

```
[edit]
user@host# commit
```

Prerequisites for SSL Connections

The SSL protocol uses public-private key technology, which requires a paired private key and authentication certificate. To enable a client application to establish SSL connections, follow these steps:

1. Install the SSL client on the machine where the client application runs.

Skip this step if the client application uses the JUNOScript Perl module described in “Write Perl Client Applications” in the *JUNOScript API Guide*. As part of the Perl module installation procedure, you install a prerequisites package that includes the necessary SSL software.

2. Use one of the following two methods to obtain an authentication certificate in privacy-enhanced mail (PEM) format:

- Request a certificate from a Certificate Authority; these agencies usually charge a fee.
- Issue the following `openssl` command to generate a self-signed certificate; for information about obtaining the `openssl` software, see <http://www.openssl.org>.

The command writes the certificate and an unencrypted 1024-bit RSA private key to the `certificate-file.pem` file. The command appears here on two lines only for legibility:

```
% openssl req -x509 -nodes -newkey rsa:1024 \  
-keyout certificate-file.pem -out certificate-file.pem
```

3. Enter CLI configuration mode on the JUNOScript server and issue the following commands to import the certificate. In the first command, substitute the certificate name for the `certificate-name` variable. In the second command, for the `URL-or-path` variable, substitute the name of the file that contains the paired certificate and private key, either as a URL or as a pathname on the local disk.

```
[edit]  
user@host# edit security certificates local certificate-name
```

```
[edit security certificates local certificate-name]  
user@host# set load-key-file URL-or-path
```



NOTE: The CLI expects the private key in the specified file (`URL-or-path`) to be unencrypted. If the key is encrypted, the CLI prompts for the passphrase associated with it, decrypts it, and stores the unencrypted version.

- Issue the following commands to activate the `xnm-ssl` service, which listens on port 3220. In the last command, substitute the same value for the `certificate-name` variable as in Step 3.

```
[edit security certificates local certificate-name]
user@host# top

[edit]
user@host# edit system services

[edit system services]
user@host# set xnm-ssl local-certificate certificate-name
```

- Verify that 127.0.0.1 is one of the IP addresses configured for the loopback interface, `lo0`, on the JUNOScript server machine. The output from the `show interfaces lo0` command must include an `address` statement similar to the following:

```
[edit system services]
user@host# top

[edit]
user@host# show interfaces lo0
unit 0 {
    family inet {
        address 127.0.0.1/32;
    }
}
```

If necessary, issue the following command to add the address at the `[edit interfaces lo0 unit 0 family inet]` hierarchy level:

```
[edit]
user@host# set interfaces lo0 unit 0 family inet address 127.0.0.1
```

- Commit the configuration:

```
[edit]
user@host# commit
```

Understanding Authentication Information and Access Methods

Setting up an access method requires that you add authentication information first, then add access method information.

If each router has the same username, password, and access protocol configured, you can set up one access method for all routers.

Different JUNOScope users can use the same authentication information to access a router if they all have the same permissions. If a user's permissions are different, you must create two different authentication information entries.

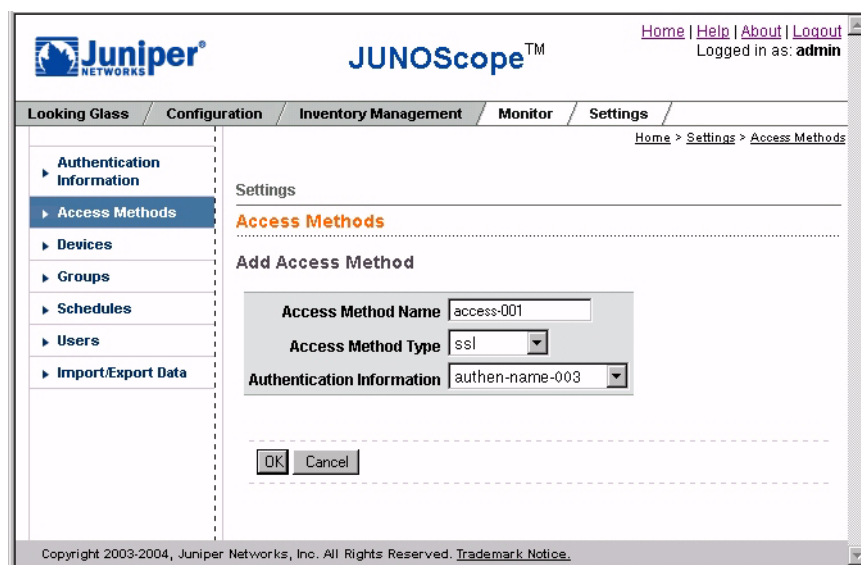
You can create two access methods using the same authentication information and different access protocols. Or you can create two access methods with the same selections but with a different access method name.

Adding an Access Method

You are not done setting up access methods without at least one authentication information entry. You can use the Add button to add a new entry, or edit or delete an existing entry.

To add an access method, follow these steps:

1. From the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Click Add. The Add Access Method dialog box appears.



3. In the Access Method Name text box, type a name for the remote router access method to use in the JUNOScope software. This is the access method name used in the Add Device dialog box. See “Adding a Device” on page 60.
4. In the Access Method Type drop-down list box, select a supported access protocol that is configured on the router, either SSL or clear-text.
5. In the Authentication Information drop-down list box, select an authentication name. This is the same name that you created in the Add Authentication Information dialog box.
6. Click OK. The new access method is listed in the Access Methods dialog box.

Viewing Access Methods

To view added access methods, follow these steps:

1. From the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.

The screenshot shows the JUNOScope web interface. The top navigation bar includes the Juniper logo, the title 'JUNOScope™', and links for 'Home | Help | About | Logout'. The user is logged in as 'admin'. The main navigation menu on the left includes 'Authentication Information', 'Access Methods', 'Devices', 'Groups', 'Labels', 'Schedules', 'Users', 'RADIUS Configuration', 'Import/Export Data', and 'Saved Operations'. The 'Access Methods' section is selected. The main content area shows the 'Settings' page for 'Access Methods'. It contains a table with the following data:

	Access Method Name	Connection Type	Authentication Information Name
<input type="checkbox"/>	access-method-001	ssl	authn-info-name003
<input type="checkbox"/>	access-method-002	clear-text	authn-info-name001

Below the table, there is a section for 'Export Data Encryption Format' with three radio button options:

- Encrypt sensitive data and provide key at import time
- Encrypt sensitive data and include decryption key
- Export sensitive data unencrypted

At the bottom of the table area, there are buttons for 'Add', 'Edit', 'Delete', 'Export', and 'Import'. The footer of the page contains the copyright notice: 'Copyright 2003-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.'

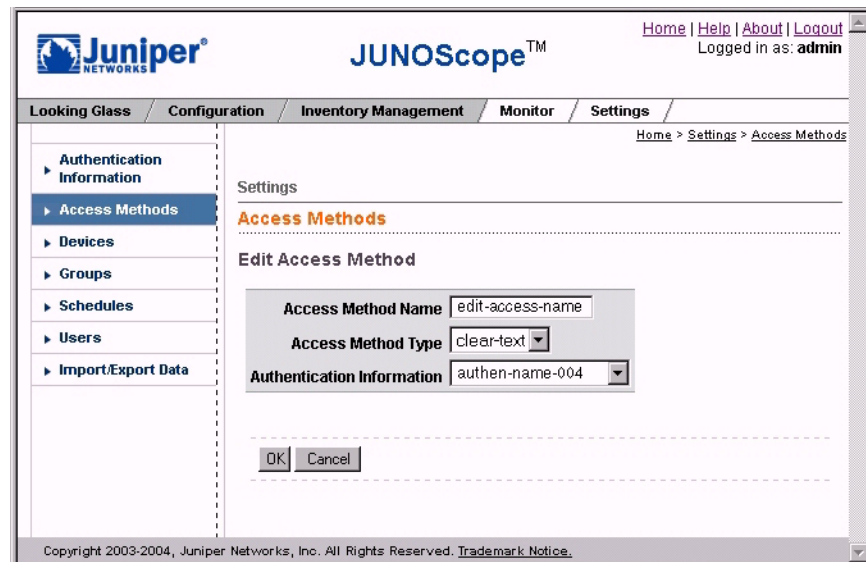
The access methods are listed alphabetically in the table by name, connection type, and authentication information name. The Access Methods dialog box, lets you add, edit, delete, export, or import data. Select the check box for the access method item to edit or delete.

2. Select one of the following ways to export authentication information from the JUNOScope software:
 - Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
 - Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export access methods information to another system.
 - Export sensitive data unencrypted—Sensitive data is not encrypted at export.

Editing Access Method Information

To edit access method information, follow these steps:

1. In the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Select the check box for the access method that you want to edit.
3. Click Edit. The Edit Access Method dialog box appears.



4. Edit the access method name, access method type, or authentication information.
5. Click OK. The edited access method information is listed in the Access Methods dialog box.

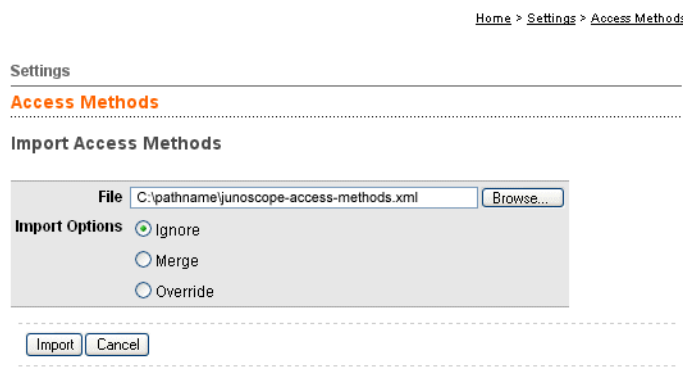
Importing Access Methods

You can import access method or authentication information from another JUNOScope server or by using the provided sample XML import file `export-import-sample.xml`, located on the JUNOScope server.

Importing an access method or authentication information is useful when you do not want to enter setup information manually.

To import access methods, follow these steps:

1. In the JUNOScope main window, click Settings > Access Methods. The Authentication Information or Access Methods dialog box appears.
2. Click Import. The Import Access Methods dialog box appears.



3. 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 `access.xml` file exported from another JUNOScope server, or use the `export-import-sample.xml` file as a guide to generate a file to import.

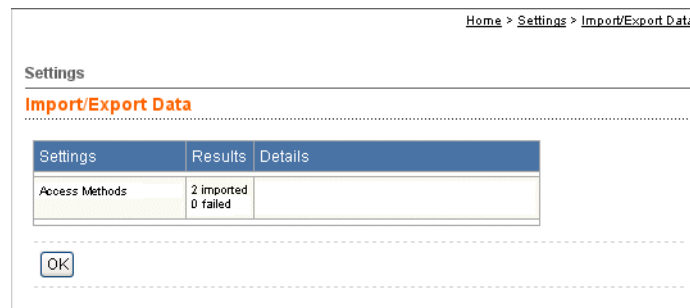


NOTE: The `junoscope-` XML file prefix is not generated if you use the Microsoft Internet Explorer 6.0 Web browser to export JUNOScope setup data. You will only see the `access-method` or `auth-info` filename.

4. 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.

5. 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.

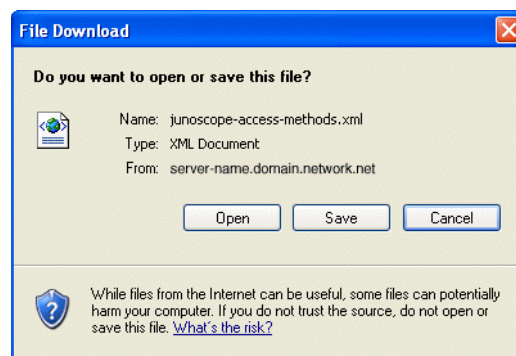
6. Click OK. The imported data is listed in the Access Methods dialog box.

Exporting Access Methods

You can export access methods that you want to back up or import to another JUNOScope server.

To export access methods, follow these steps:

1. In the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Click Export. The File Download dialog box appears.



3. Click Save to export the access methods data and save it to the local file system in a file named junoscope-access-methods.xml. Click Open to view the export file contents.

Deleting Access Methods



NOTE: You cannot delete authentication information that is currently being used by an access method. You must first delete the access method, then delete the authentication information. You cannot delete an access method if it is currently being used by a device. You must first delete the device, then delete the access method.

To delete an access method, follow these steps:

1. In the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Select the check box for the access method that you want to delete.
3. Click Delete. The access method is deleted from the Access Methods table or the Authentication Information table.

