

Chapter 13

Importing and Exporting All Settings Data

This chapter describes how to import JUNOScope software settings data for all authentication information, access methods, devices, groups, schedules, users, labels, and saved operations at once into the database using an Extensible Markup Language (XML) data file exported from another JUNOScope server.

This chapter also describes how to export settings data from the database to an XML data file for backup or for importing to another JUNOScope server.

You must have superuser permissions to import or export all JUNOScope data.

For information about importing and exporting individual access methods, devices, groups, schedules, or user data, see the following chapters in this guide:

- Setting Up Access Methods on page 47
- Setting Up Devices on page 59
- Setting Up Groups on page 71
- Setting Up Labels on page 93
- Setting Up Schedules on page 103
- Setting Up User Local Authentication on page 111

You must have superuser permission to import and export all setup data.

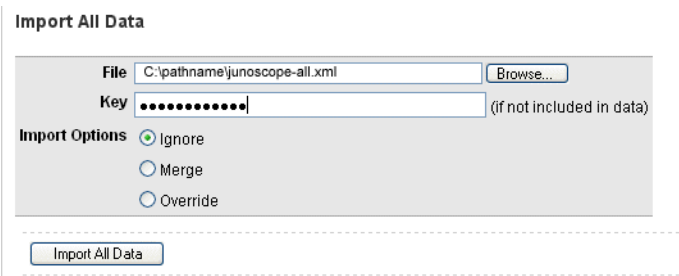
This chapter includes the following topics:

- Importing All Settings Data on page 148
- Exporting All Settings Data on page 151

Importing All Settings Data

To import all JUNOScope settings data at once, follow these steps:

1. In the JUNOScope main window, click Settings > Import/Export Data. The Import/Export Data dialog box appears.



2. In the Import All Data area, type the XML filename or browse to the XML file you want to import.

For example, you can import the default junoscope-all.xml XML file from another JUNOScope server or modify the sample export-import-sample.xml file on the JUNOScope server accordingly. The contents of the sample XML file are as follows:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <all-records xmlns:cinclude="http://apache.org/cocoon/include/1.0">
- <junoscope:users xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:user>
  <junoscope:login>admin</junoscope:login>

<junoscope:password>@S@20954@D2A1C46FC4830C53@1B3568CD62D615C9</junoscope:password>
  <junoscope:user-role>superuser</junoscope:user-role>
</junoscope:user>
</junoscope:users>
- <junoscope:groups xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:group>
  <junoscope:name>my-group</junoscope:name>
  <junoscope:criteria>SELECT DISTINCT dev.name FROM devices dev WHERE (
dev.deleted_on = 0 ) AND ( ( dev.name LIKE '%delhi%' ) )</junoscope:criteria>
  <junoscope:pretty>NAME does contain "delhi"</junoscope:pretty>
  <junoscope:comment>my group</junoscope:comment>
</junoscope:group>
</junoscope:groups>
- <junoscope:labels xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:label>
  <junoscope:name>my-label</junoscope:name>
  <junoscope:category>core</junoscope:category>
  <junoscope:comment />
</junoscope:label>
</junoscope:labels>
- <junoscope:devices xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:device>
  <junoscope:name>munch</junoscope:name>
  <junoscope:hostname>munch</junoscope:hostname>
  <junoscope:priority>0</junoscope:priority>
  <junoscope:model>J4300</junoscope:model>
  <junoscope:comment />
```

```

<junoscope:default-access-method>my-access</junoscope:default-access-method>
<junoscope:device-label>my-label</junoscope:device-label>
</junoscope:device>
- <junoscope:device>
  <junoscope:name>delhi</junoscope:name>
  <junoscope:hostname>delhi</junoscope:hostname>
  <junoscope:priority>0</junoscope:priority>
  <junoscope:model>T320</junoscope:model>
  <junoscope:comment />
  <junoscope:default-access-method>my-access</junoscope:default-access-method>
  <junoscope:device-label>my-label</junoscope:device-label>
</junoscope:device>
- <junoscope:device>
  <junoscope:name>fivestar</junoscope:name>
  <junoscope:hostname>fivestar</junoscope:hostname>
  <junoscope:priority>0</junoscope:priority>
  <junoscope:model>J6300</junoscope:model>
  <junoscope:comment />
  <junoscope:default-access-method>my-access</junoscope:default-access-method>
  <junoscope:device-label>my-label</junoscope:device-label>
</junoscope:device>
</junoscope:devices>
- <junoscope:schedules xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:schedule>
  <junoscope:name>my-sched</junoscope:name>
  <junoscope:start-time utc-milliseconds="1138645800653">Tue Jan 31 00:00:00 IST
2006</junoscope:start-time>
  <junoscope:period>every minute</junoscope:period>
  <junoscope:comment />
</junoscope:schedule>
</junoscope:schedules>
- <junoscope:access-methods
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">

<junoscope:encryption-format>encrypted-and-key-included</junoscope:encryption-format>

<junoscope:encryption-key>@S@9DAA03366CD26456EFBC333E44620CA9</junoscope:encryption-key>
- <junoscope:authentication-information>
  <junoscope:name>my-auth</junoscope:name>
  <junoscope:login>regress</junoscope:login>
  <junoscope:password>@S@14095E0A0A8999C6F8C35FA5F797795C</junoscope:password>
</junoscope:authentication-information>
- <junoscope:access-method>
  <junoscope:name>my-access</junoscope:name>
  <junoscope:type>clear-text</junoscope:type>
  <junoscope:authentication>my-auth</junoscope:authentication>
</junoscope:access-method>
</junoscope:access-methods>
- <junoscope:radius-clients-config
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:radius-server-entry>
  <junoscope:server-name>10.209.148.102</junoscope:server-name>
  <junoscope:port-no>1812</junoscope:port-no>
  <junoscope:acct-port-no>1813</junoscope:acct-port-no>

<junoscope:shared-secret>@S@6DE028955F902AB28F435E9C314C38219490246BB894C586E582
6E93F712E90A3C9D8D53EE6AB4FE4B10FE0FAF25F636</junoscope:shared-secret>
</junoscope:radius-server-entry>
</junoscope:radius-clients-config>
</all-records>

```

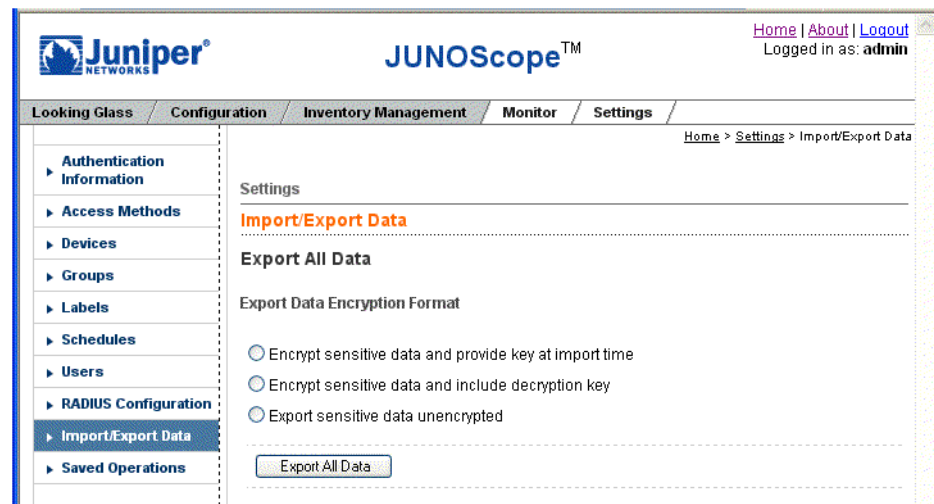
3. Type the key to decrypt the sensitive data that you want to import if the key was not included when the data was exported.
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope 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. In the Import All Data area, click Import All Data. All setup information in the database is saved to the local file system with the filename that you specified.

Exporting All Settings Data

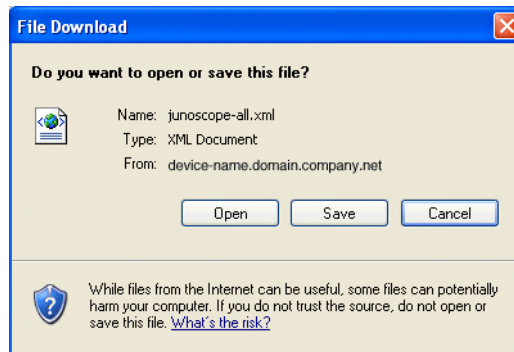
You can export all JUNOScope settings data at once to an export XML file for importing later to another JUNOScope server.

To export all setup data at once, follow these steps:

1. In the JUNOScope main window, click Settings > Import/Export Data. The Import/Export Data dialog box appears.



2. Select how you want sensitive data in authentication information exported from the JUNOScope software. Sensitive authentication information can be exported in one of the following ways:
 - 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 all settings data to another system.
 - Export sensitive data unencrypted—Sensitive password data is not encrypted at export.
3. In the Export All Data area, click Export All Data. The File Download dialog box appears.



4. Click Save to export all of the setup data in the database to a default export XML file named `junoscope-all.xml`. Click Open to view the contents of the export XML file.



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