

Chapter 4

Managing VPNs

This chapter describes how to manage virtual private networks (VPNs) in the directory and contains the following sections:

- Overview on page 133
- Adding VPNs on page 134
- Modifying VPNs on page 136
- Adding Extranet Clients to VPNs on page 136
- Removing Extranet Clients on page 139
- Validating VPN Data in the Directory on page 139
- Deleting VPNs on page 140

Overview

For SDX configurations that support JUNOS routers, retailers and enterprises can support one or more VPNs. A VPN is an object in the directory that represents a virtual private network in an organization and has the object class `umcVpn`, which can be subordinate to the object classes `umcRetailer` and `umcEnterprise`. For information about the object classes and their associated attributes, see the LDAP schema in the SDX software distribution in the folder `SDK/doc/ldap` or on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/sdx>

Adding VPNs

The administrator of a retailer can add and modify VPNs with an LDAP client, a data integrator, or SDX Admin. IT managers with the appropriate privileges can modify VPN properties through Enterprise Manager Portal (see *SDX Components Guide, Vol. 2, Chapter 9, Managing Services with Enterprise Manager Portal*).

Adding VPNs with a Data Integrator

You can develop a data integrator that reads data from a storage medium, such as a database or a directory that does not use the SDX LDAP schema and that writes the data to the directory in a format that complies with the LDAP schema.

We provide a sample data integrator, VPN Directory Updater, which reads data about VPNs from a database and writes the data to a directory. If you want to use this data integrator, you need to understand how it works, and customize it for your specific application.

For information about data integrators and VPN Directory Updater, see *SDX Integration Guide, Chapter 9, Data Integration*.

Adding VPNs with SDX Admin

To add a VPN with SDX Admin:

1. In the navigation pane, highlight the retailer or enterprise to which you want to add the new VPN, and right-click.
2. Select New > VPN.

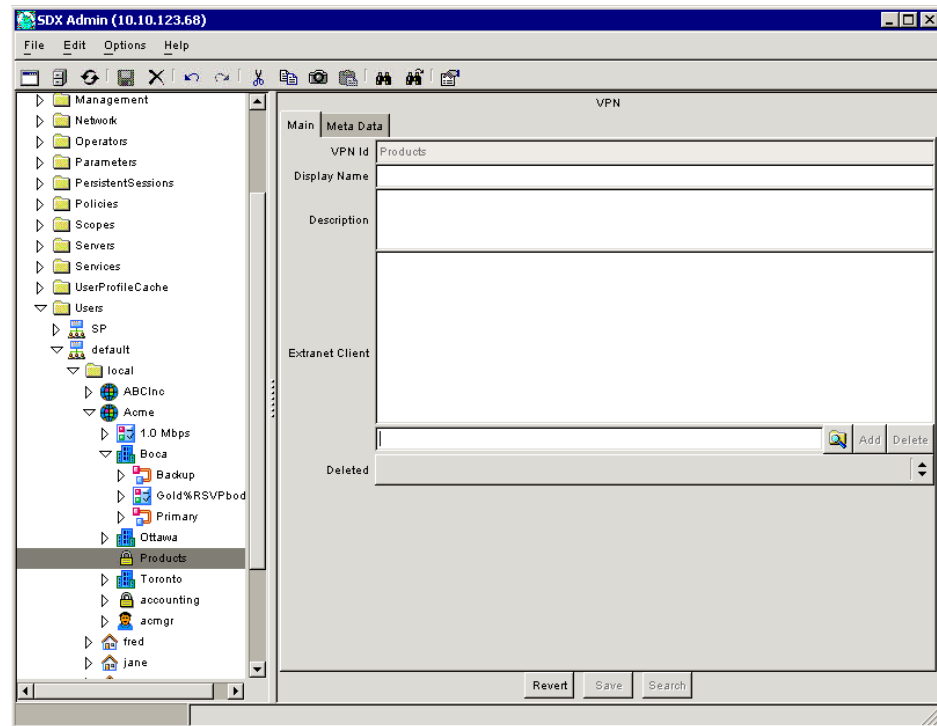
The New VPN dialog box appears.

3. Enter the names of the routing instances, as defined on the JUNOS routing platform, that implement the VPN in the network, and click OK.

For more information about routing instances and JUNOS routing platforms, see the JUNOS Internet Software documentation.

The VPN pane appears.

Figure 7: VPN Pane



4. Use the field descriptions in *VPN Fields* on page 135 to configure the VPN, and then click Save.

VPN Fields

Use the fields in this section to configure VPNs.

Display Name

- Name of the VPN that appears in other SDX components, such as the Enterprise Manager Portal.
- Value—Text string
- Default—No value
- Example—Products VPN

Description

- Description of the VPN.
- Value—Text string
- Default—No value
- Example—VPN for sales representatives

Extranet Client

- Extranet client for this VPN.
- Value—Retailer or enterprise
- Default—No value
- Guidelines —For information about completing this field, see *Adding Extranet Clients to VPNs* on page 136.

Deleted

- Availability of this entry to other SDX components connected to the directory.
- Value—Blank or True or False
 - Blank—Other SDX components can access this entry in the directory.
 - True—Other SDX components cannot use this entry in the directory, although the object still exists.
 - False—Other SDX components can access this entry in the directory.
- Default—Blank

Modifying VPNs

IT managers with the appropriate permissions can display names and modify the descriptions of VPNs through the Enterprise Manager portal. Service providers can modify VPNs with an LDAP client or SDX Admin.

Adding Extranet Clients to VPNs

Retailers and enterprises can be extranet clients. IT managers add extranet clients to their VPNs through Enterprise Manager Portal (see *SDX Components Guide, Vol. 2, Chapter 9, Managing Services with Enterprise Manager Portal*). Service providers can add extranet clients to VPNs with an LDAP client or SDX Admin.

Two LDAP attributes specify information about extranet clients:

- The object classes `umcRetailer` and `umcEnterprise` have an LDAP attribute called `ImportedExtranet` that defines the DNs of the imported VPNs.
- The object class `umcVPN` has an attribute called `extranetClient` that defines the DNs of extranet clients of the VPN.

Adding Extranet Clients with SDX Admin

To add an extranet client with SDX Admin:

1. In the navigation pane, highlight the VPN you want to export to the extranet client.

The VPN pane appears (see Figure 7 on page 135).

2. Click the magnifying glass below the Extranet Client field.

The Select Object dialog box appears and displays a list of subscribers.

3. Navigate to the retailer or enterprise who will be the extranet client.
 - To navigate to a subordinate subscriber, double-click on a subscriber in the list.
 - To navigate to a subscriber at a higher level in the directory, use the menu at the top of the Select Object dialog box.
 - To select multiple options, shift-click or control-click the subscribers.

4. Click OK.

The extranet clients appear in the VPN pane.

5. Click Add.

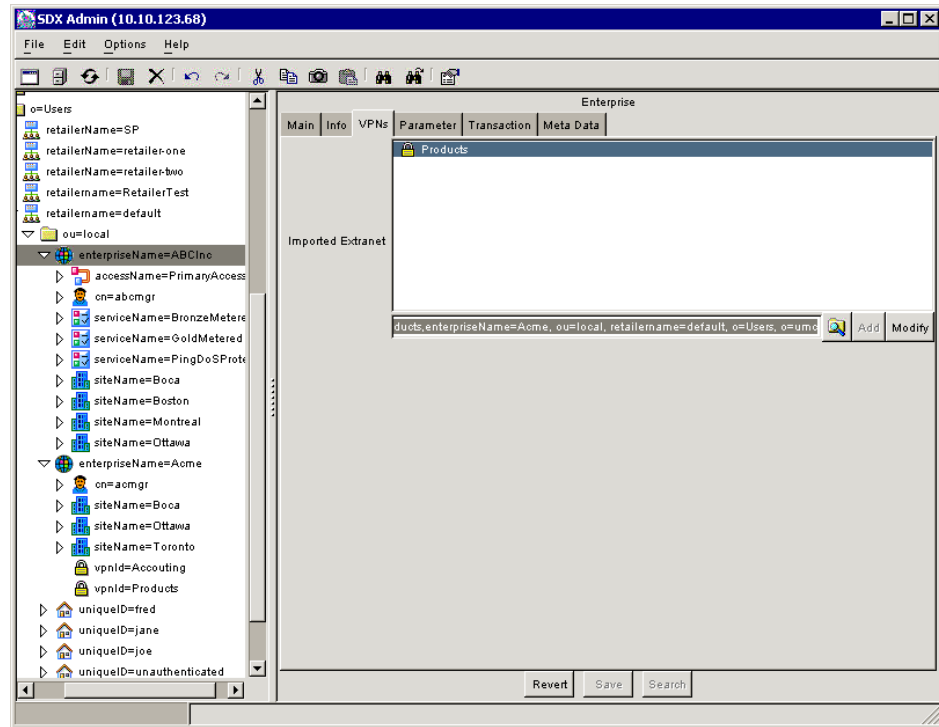
The extranet clients appear in the Extranet Client field of the VPN pane.

6. Click Save in the VPN pane.

7. In the navigation pane, highlight the subscriber for whom you want to import the VPN.

The subscriber's pane appears.

8. Click the VPNs tab for this subscriber.

Figure 8: Enterprise Pane

9. Click the magnifying glass below the Imported Extranet field.

The Select Object dialog box appears and displays a list of subscribers.

10. Navigate to the VPN you want to import.

- To navigate to a subordinate VPN, double-click on a subscriber in the list.
- To navigate to a VPN at a higher level in the directory, use the menu at the top of the Select Object dialog box.
- To select multiple options, shift-click or control-click the subscribers.

11. Click OK.

The VPN appears in the subscriber's pane.

12. Click Add.

The VPN appears in the Extranet Client field of the subscriber's pane.

13. Click Save in the subscriber's pane.

Removing Extranet Clients

IT managers can remove extranet clients through Enterprise Manager Portal (see *SDX Components Guide, Vol. 2, Chapter 9, Managing Services with Enterprise Manager Portal*). Service providers can remove extranet clients to VPNs with an LDAP client or SDX Admin.

Removing Extranet Clients with SDX Admin

To remove an extranet client with SDX Admin:

1. In the navigation pane, click on the subscriber who is the extranet client.
2. Click on the VPN tab for this subscriber.

The subscriber's pane appears (for example, see Figure 8 on page 138).

3. Highlight the VPN in the Imported Extranet field, right-click, and select Delete.
4. Click Save in the subscriber's pane.
5. In the navigation pane, click on the VPN.

The VPN pane (see Figure 7 on page 135) appears.

6. Highlight the extranet client in the Extranet Client field, right-click, and select delete.
7. Click Save in the VPNs pane.

Validating VPN Data in the Directory

When an IT manager cancels the export of a VPN, the Enterprise Manager portal automatically deactivates any active subscriptions to that VPN for the associated extranet client. If an IT manager cancels the export of a VPN at the same time that the extranet client activates a subscription to this VPN, there is a remote possibility that the Enterprise Manager portal will maintain the active subscription.

We recommend that you periodically check for and deactivate these types of invalid subscriptions to prevent this type of invalid subscription. We provide a data integrator, VPN Subscription Deactivator, for this purpose. This data integrator works with the Enterprise Service Portal audit plug-in. For more information on data integrators and VPN Subscription Deactivator, see *SDX Integration Guide, Chapter 9, Data Integration*.

To use this data integrator:

1. Install and configure the Enterprise Service Portal audit plug-in with the Enterprise Manager portal (see *SDX Components Guide, Vol. 2, Chapter 7, Installing and Configuring Enterprise Service Portals*).
2. Install the Data Integration package (see *SDX Software Basics Guide, Chapter 5, Installing the SDX-300 Software*).
3. Run the script `/opt/UMC/datint/etc/vpndatamgt` with the check option, or configure a utility, such as a crontab file, to run this script at a defined time (see *SDX Integration Guide, Chapter 9, Data Integration*).

Deleting VPNs

Service providers can delete VPNs in the directory. To delete VPNs:

1. Delete subscriptions to BoD services associated with the VPN.

Subscriptions to BoD services associated with a particular VPN all contain the substitution

```
bodVpnName=<vpnID>
```

where `<vpnID >` is the DN of the VPN to be deleted.

You can delete subscriptions with the specified substitution through an LDAP client. You can also delete individual subscriptions with SDX Admin (see *Modifying and Deleting Subscribers and Subscriptions* on page 131), although this solution is not practical for large numbers of subscribers. As a third option, you can develop a data integrator to delete the subscriptions (see *SDX Integration Guide, Chapter 9, Data Integration*).

2. Remove all extranet clients (see *Removing Extranet Clients* on page 139).
3. Delete the VPN object from the directory.

For information about deleting entries with SDX Admin, see *SDX Software Basics Guide, Chapter 13, Using SDX Admin*.

If you also want to delete the VPNs from the JUNOS routing platform, delete the routing instances that implement the VPN in the network. For complete information about configuring JUNOS routing platforms, see the JUNOS Internet Software documentation.