Symantec™ Managed PKI®

Integration Guide for Juniper® SA VPN

Symantec™ Managed PKI® Integration Guide for Juniper® SA VPN

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated July 8, 2013

Legal Notice

THE DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. “Commercial Computer Software and Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec® product.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Integrating Managed PKI Certificates with Juniper® VPN

The enterprise workplace has moved beyond the walls of the organization into a global, mobile environment. To maintain productivity, your end users need to access company resources using a mobile platform. However, you need to be able to trust the end users accessing your systems, and the mobile device they use, no matter if you have provided their devices or if they are using their own mobile devices.

Symantec Managed PKI's digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from a few to thousands of devices, and its in-the-cloud solution provides quick deployment and easy management while also offering Symantec's industry leading security that is unmatched by in-house PKI solutions.

Symantec's Managed PKI issues certificates that can be used to authenticate users for secure communications with company resources, such as VPNs and web sites.

This document describes how to integrate Managed PKI 8.7 or higher certificates with the Juniper® Secure Access (SA) VPN to authenticate users to protected resources, and to secure communications between them.

Partner Information

These procedures have been tested on the following platforms:

Table 1-1 Partner Information

Partner Name	Juniper® Networks
Product Name	Juniper® Secure Access (SA) Series VPN
Version and Platform	SA 2000 Junos OS Release 7.1 and Junos Pulse 4.2.1

How the Juniper VPN Works

The following diagram describes how the Managed PKI certificates integrate with Juniper SA Series VPN to provide secure authentication.

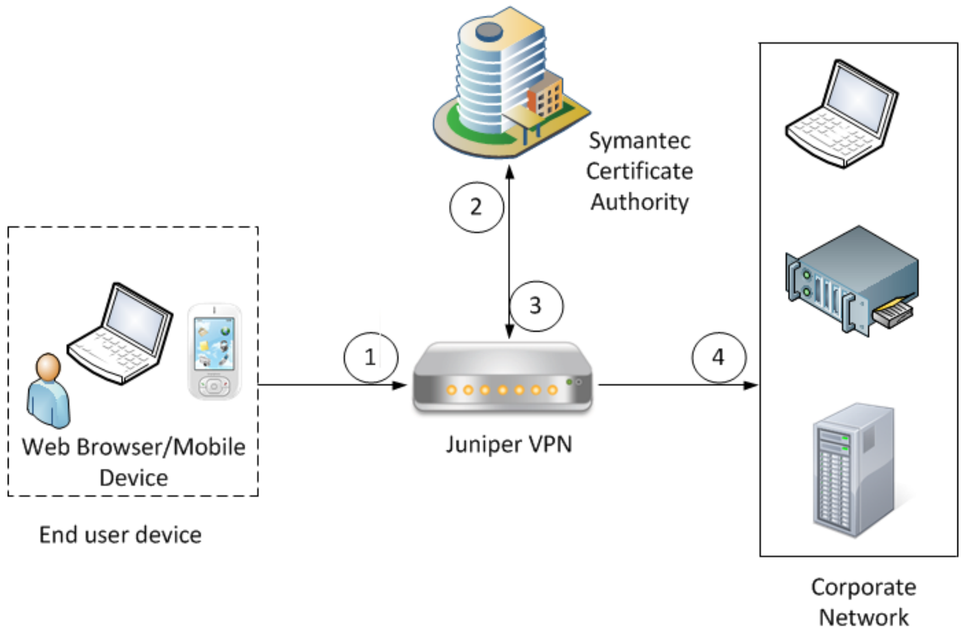


Figure 1-1 Authenticating Juniper VPN with a Managed PKI certificate

1. The end-user device accesses the corporate network through the Juniper VPN.
2. Depending upon how the VPN is configured, it attempts to obtain the status of the certificate:
   - If Online Certificate Status Protocol (OCSP) is configured, the VPN communicates to the Symantec CA to obtain the real-time status of the certificate.
   - If Certificate Revocation List (CRL) is configured, the VPN communicates to the Symantec CA to obtain the status of the certificate based on the most recent certificate revocation list. CRLs are updated on a regular basis.
3. When the Juniper VPN receives the certificate status, it authenticates the end-user's certificate based on the CAs it has been configured to trust.
4. Based on this authentication, the end user device is allowed access to the corporate network, and the Juniper VPN secures communication with the corporate network.

Integration Workflow

The following diagram describes the general steps required to set up the Symantec Managed PKI account and integrate Managed PKI certificates with Juniper VPN.

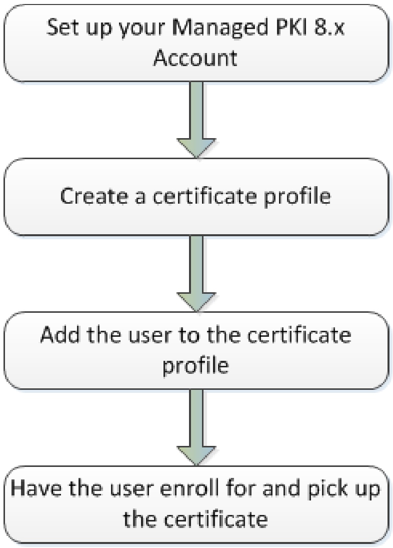

Set up your Managed PKI 8.x Account
Create a certificate profile
Add the user to the certificate profile
Have the user enroll for and pick up the certificate

Figure 1-2 Managed PKI Integration Workflow

Task 1. Set up your Managed PKI 8.x account

Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

You will need to complete and return the following documents. As needed, your Symantec representative will assist you with obtaining and completing these forms.

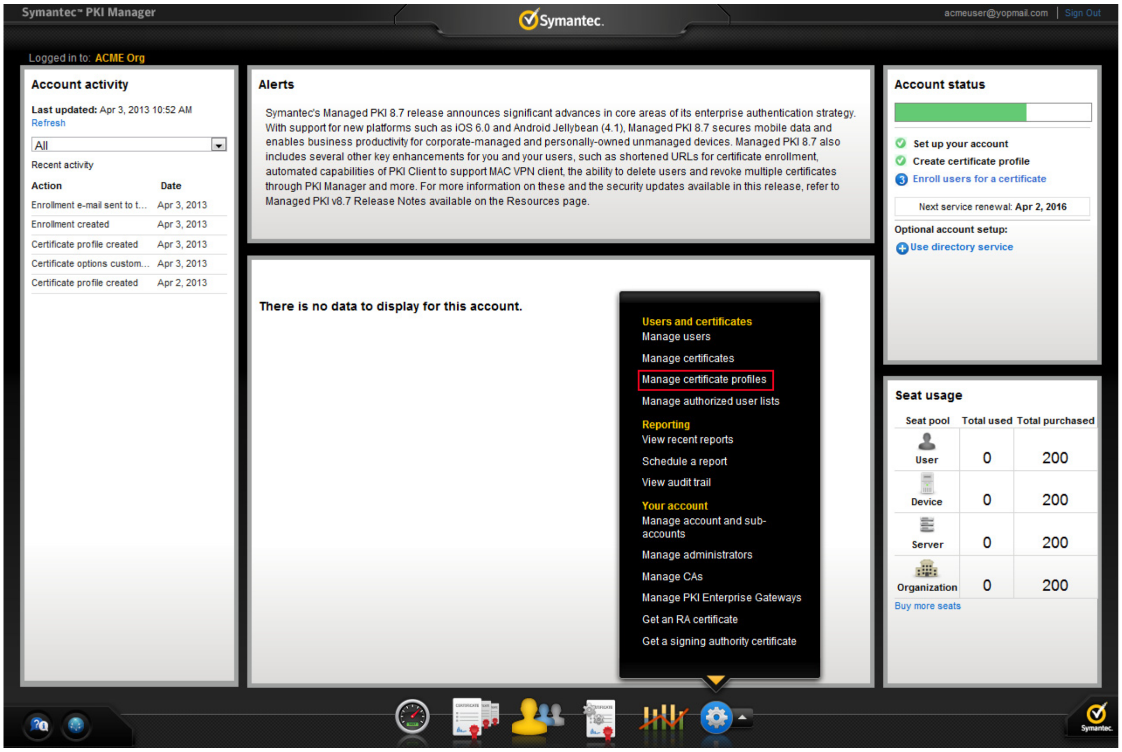
- Master Service Agreement
- Issuing Authority Naming Application (also known as the CA Naming Document)
- Symantec Services Order Form
- Purchase Order, credit card, or reference number

You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. For more information on configuring Managed PKI, refer to PKI Manager and its online help.

Task 2. Create a certificate profile

To obtain a certificate for the router, you first create the certificate profile that will define the certificates you will issue to your end users. Complete the following steps to create your Managed PKI Client Authentication certificate profile:

1. Log into Managed PKI's PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.
2. On PKI Manager, click **Manage certificate profiles** or select **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.



Logged in to: ACME Org

Account activity

Last updated: Apr 3, 2013 10:52 AM
Refresh

All

Recent activity

Action	Date
Enrollment e-mail sent to t...	Apr 3, 2013
Enrollment created	Apr 3, 2013
Certificate profile created	Apr 3, 2013
Certificate options custom...	Apr 3, 2013
Certificate profile created	Apr 2, 2013

Alerts

Symantec's Managed PKI 8.7 release announces significant advances in core areas of its enterprise authentication strategy. With support for new platforms such as iOS 6.0 and Android Jellybean (4.1), Managed PKI 8.7 secures mobile data and enables business productivity for corporate-managed and personally-owned unmanaged devices. Managed PKI 8.7 also includes several other key enhancements for you and your users, such as shortened URLs for certificate enrollment, automated capabilities of PKI Client to support MAC VPN client, the ability to delete users and revoke multiple certificates through PKI Manager and more. For more information on these and the security updates available in this release, refer to Managed PKI v8.7 Release Notes available on the Resources page.

There is no data to display for this account.

Account status

✓ Set up your account
✓ Create certificate profile
3 Enroll users for a certificate

Next service renewal: **Apr 2, 2016**

Optional account setup:
Use directory service

Seat usage

Seat pool	Total used	Total purchased
User	0	200
Device	0	200
Server	0	200
Organization	0	200

Buy more seats

Figure 1-3 Manage Certificate Profile

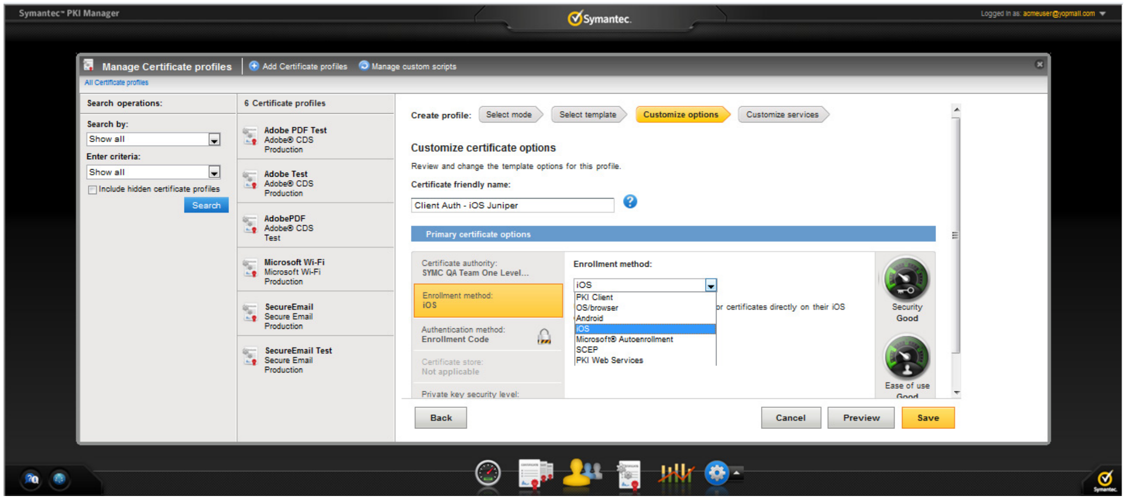
3 Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The Create profile page appears.

4 Select whether these certificates will be issued in Test mode or Production Mode, and click **Continue**. The Create profile page appears.

5 Select **Client Authentication** as the certificate template and click **Continue**. The Customize certificate options page appears.

6 Set the certificate options that suits your needs, but the following configurations are required:

- Enter a profile name.



Customize certificate options

Review and change the template options for this profile.

Certificate friendly name: Client Auth - iOS Juniper

Certificate authority: SYMC QA Team One Level...

Enrollment method: iOS

Authentication method: Enrollment Code

Certificate store: Not applicable

Private key security level:

Enrollment method: iOS

...r certificates directly on their iOS

Figure 1-4 Client Authentication Certificate options

- Select the appropriate Enrollment method from the following:
  - Select **iOS** if your user will enroll for certificates using iOS devices.
  - Select **OS/browser** if your user will enroll for certificates using desktop or laptop.
  - Select **PKI Client** if your user will enroll for certificates using PKI Client.

Click **Advanced options** to view certificate options and define any additional attributes you may need.

7 Click **Save**.

On the confirmation page, you can view the attribute used for the seat ID, a mandatory attribute that authenticates the user for third party configurations or during the enrollment process. This is typically the user's email address.

You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

8 For certificate profiles using the iOS Enrollment method only, click **Edit** from **Provide certificate instructions** under Manage this profile. Table 1-2 describes the values that you can enter to configure VPN settings for this profile:

Table 1-2 VPN Settings for iOS Enrollment Method

Field Name	Value
Connection Type	Juniper (VPN)
Connection name	Enter a unique name as a connection name.
Server Host/IP	The Fully Qualified Domain Name of the VPN. For example, https://vpn.<company>.com
Account	Enter a valid server name that hosts the Juniper VPN.
Realm	This value must match the realm name you will use for user authentication on the VPN. Refer to "Creating User Realm for User Authentication" on page 10 for details.
Role	This value must match the role name you will use for user authentication on the VPN. Refer to "Configuring User Roles on the VPN device" on page 11 for details.
Enable VPN On Demand	Select this option for networks that use certificate-based authentication.

Task 3. Add the user to the certificate profile

You must add the user to the certificate profile in PKI Manager before the user can enroll for and pick up a certificate.

1 In PKI Manager, click **Manage users**, or select **Manage users** from the Tasks menu on the bottom navigation bar.

2 Click **Add Users** from the top of the resulting Manage users page.

3 Enter the seat ID (typically the end user's email address) and click **Continue**.

- Enroll for a single user by entering end user's email address.
- Enroll for multiple users at one time by uploading a comma-separated value (csv) file with your user data. You can skip step 4 if you are enrolling multiple users using a .csv file.

4 Enter the First Name, Last Name, and select the **I want to enroll this user for a certificate** check box and click **Continue**.

5 Select the certificate profile you created in Task 2, "Create a certificate profile" on page 3 and click **Continue**.

6 Enter the **Other Name (UPN)**, **Email**, and select the **Have the system send the enrollment email to the user** check box (optional) and click **Continue**.

The enrollment link is displayed to the administrator along with the enrollment code required for authentication. Symantec recommends that you send the enrollment code separately from the enrollment link, and that you do not send the enrollment code by email.

Note: The enrollment link will not be displayed if you have selected **Have the system send the enrollment email to the user** in step 6.

Task 4. Have the user enroll for and pick up the certificate

Once added to the certificate profile, the user must enroll for and pick up the certificate. The following are the steps for picking up certificates for different enrollment methods.

Table 1-3 Steps for picking up certificates

Enrollment Method	How Certificates are Picked Up
iOS	1 Download the **Junos Pulse** application from the App Store^{SM}. 2 Open a browser on the iOS device. 3 Paste the enrollment link from the enrollment email into the browser. 4 Enter the User Id and enrollment code (provided by the administrator) and tap **Continue**. The Identity Confirmed page appears. 5 Tap **Continue**. The Install Profile page appears. 6 Tap **Install**, then tap **Install Now** from the pop-up window. 7 Enter your device passcode and click **Done**. 8 To verify the configuration settings, click **Configuration**.

Table 1-3 Steps for picking up certificates

Enrollment Method	How Certificates are Picked Up
OS/browser	**Supported Browsers:** ■ For Windows XP or Windows 7 - Internet Explorer or Firefox ■ For Apple OS X - Safari or Firefox Refer the Managed PKI documentation for the exact version numbers. 1 Click the enrollment link in the email or paste it into your browser. 2 Enter the email address used for enrollment and click **Continue**. 3 Enter the enrollment code provided by the administrator or received in an email and click **Continue**. This step authenticates the end user to ensure the correct user is picking the certificate. 4 Click **Continue**. 5 Click **Install certificate** to install the certificate.
PKI Client	**If PKI Client is not already installed on the user's machine, the user will be prompted to install it during enrollment.** 1 Click the enrollment link in the email or paste it into your browser. 2 Enter the email address used for enrollment and click **Continue**. 3 Enter the enrollment code provided by the administrator or received in an email and click **Continue**. This step authenticates the end user to ensure the correct user is picking the certificate. 4 Click **Continue**. 5 Click **Install Certificate**. 6 Enter the PIN for the certificate store (PKI Client) when prompted and click **OK**.

Renewing Certificates

You must renew the certificate before it expires (typically a year after initially enrolling for it). The following are the steps for renewing certificates for different enrollment methods.

Table 1-4 Steps for renewing certificates

Enrollment Method	How Certificates are Renewed
iOS	If renewal notifications are enabled, the user receives an email containing a renewal link at some period before the certificate expires. Clicking the link prompts the user to select a credential to authenticate the renewal. The user is then taken to the PKI Certificate Services page and the renewed certificate is installed.
OS/browser	If renewal notifications are enabled, the user receives an email containing a renewal link at some period before the certificate expires. Clicking the link takes the user to the PKI Certificate Services page for certificate renewal, where the user follows a renewal process similar to the enrollment process.
PKI Client	PKI Client prompts the user to renew for certificates that are PIN-protected. For certificates that are not PIN-protected, PKI Client performs the renewal and installs the new certificate transparently.

Configuring Juniper SA VPN

This chapter discusses how to configure the Juniper SA VPN to use Managed PKI certificates for authentication. For more information, refer to the Juniper SA VPN documentation for details.

You must complete the following procedures to complete the configuration of Juniper VPN:

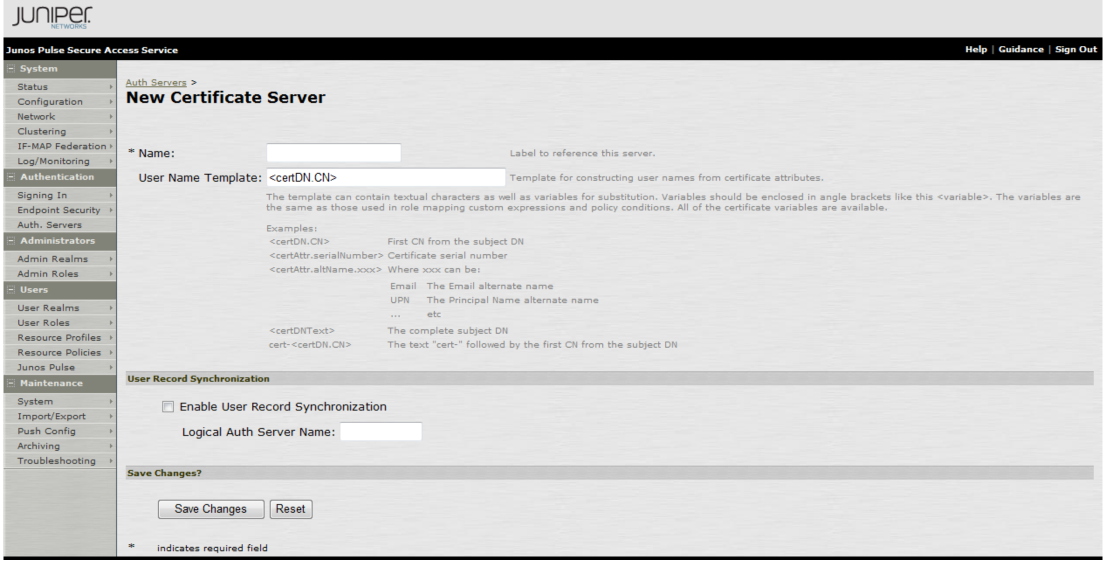
- "Accessing Juniper VPN" on page 9
- "Configuring the Authentication Server" on page 9
- "Creating User Realm for User Authentication" on page 10
- "Configuring User Roles on the VPN device" on page 11
- "Configure the User Realm for User Authentication" on page 11
- "Configuring Sign-In Page for the Network Connect Client" on page 12
- "Configure Sign-In Policies for the Network Connect Client" on page 13

Accessing Juniper VPN

1. Click the Juniper VPN admin URL.
2. Enter the user name and password.
3. Click **Submit**. The Junos Pulse Secure Access Service page is displayed.

Task 1. Configuring the Authentication Server

1. Click **Authentication** → **Auth Servers**. The Authentication Servers page appears.
2. In the **New** drop-down list, set the server type to **Certificate Server**, and click **New Server**. The New Certificate Server page appears.



Auth Servers >

New Certificate Server

* Name: Label to reference this server.

User Name Template: <certDN.CN> Template for constructing user names from certificate attributes.

The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. The variables are the same as those used in role mapping custom expressions and policy conditions. All of the certificate variables are available.

Examples:

<certDN.CN>	First CN from the subject DN
<certAttr.serialNumber>	Certificate serial number
<certAttr.altName.xxx>	Where xxx can be: Email The Email alternate name UPN The Principal Name alternate name ... etc
<certDNText>	The complete subject DN
cert-<certDN.CN>	The text "cert-" followed by the first CN from the subject DN

User Record Synchronization

☐ Enable User Record Synchronization

Logical Auth Server Name:

Save Changes?

* indicates required field

Figure 2-1 New Certificate Server page

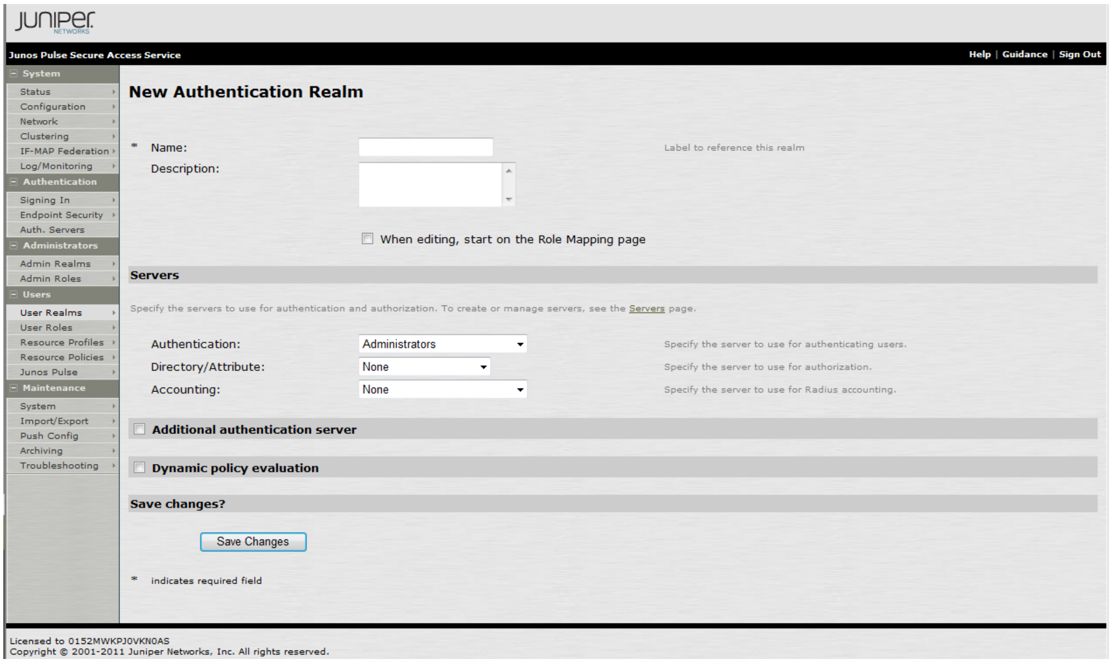
3 Enter a unique name in the **Name** field.

4 Enter `certDN.CN` in the **User Name Template** field.

5 Click **Save Changes**.

Task 2. Creating User Realm for User Authentication

1 Click **Users** → **User Realms** → **New User Realm**. The New Authentication Realm page appears.



New Authentication Realm

* Name: Label to reference this realm

Description:

☐ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication:	Administrators	Specify the server to use for authenticating users.
Directory/Attribute:	None	Specify the server to use for authorization.
Accounting:	None	Specify the server to use for Radius accounting.

☐ Additional authentication server

☐ Dynamic policy evaluation

Save changes?

* indicates required field

Licensed to 0152MWKPJ0VKN0AS

Copyright © 2001-2011 Juniper Networks, Inc. All rights reserved.

Figure 2-2 New Authentication Realm page

2 Enter a unique value in the **Name** field.

3 Enter a description for the name in the **Description** field.

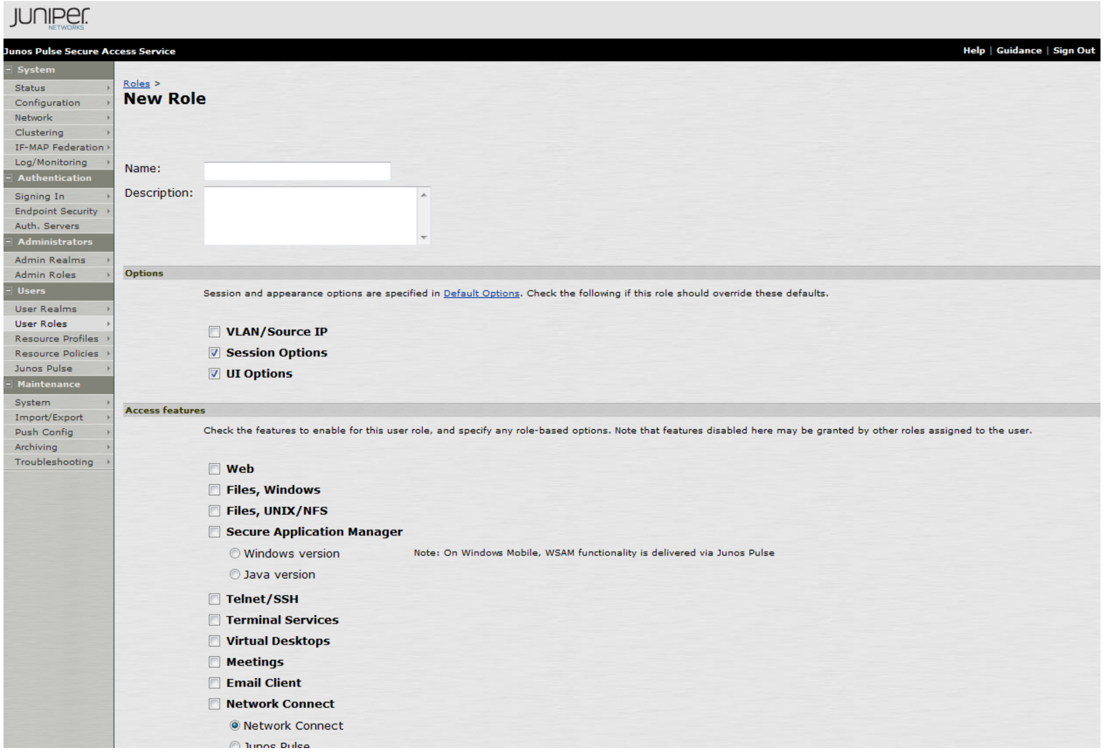
4 In the **Authentication** drop-down list, select the server you created in "Configuring the Authentication Server" on page 9.

Use the default configuration settings for other fields.

5 Click **Save Changes**.

Task 3. Configuring User Roles on the VPN device

1 Click **Users → User Roles → New User Role**. The New Role page appears.



Name:

Description:

Options

Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.

□ VLAN/Source IP
☑ Session Options
☑ UI Options

Access features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

□ Web
□ Files, Windows
□ Files, UNIX/NFS
□ Secure Application Manager
○ Windows version   Note: On Windows Mobile, WSAM functionality is delivered via Junos Pulse
○ Java version
□ Telnet/SSH
□ Terminal Services
□ Virtual Desktops
□ Meetings
□ Email Client
□ Network Connect
● Network Connect
○ Junos Pulse

Figure 2-3 New Role page

2 Enter a unique name in the **Name** field.

3 Enter a description for the name in the **Description** field.

4 Select the appropriate options and access features for the role you are creating. You must select at least one access feature for a role. Refer to the Juniper SA VPN documentation for details.

5 Click **Save Changes**.

Task 4. Configure the User Realm for User Authentication

1 Click **Users → User Realms → New User Realm**. The New Authentication Realm page appears. You can select an existing user realm or create a new user realm. For information on creating user realm, see "Creating User Realm for User Authentication" on page 10.

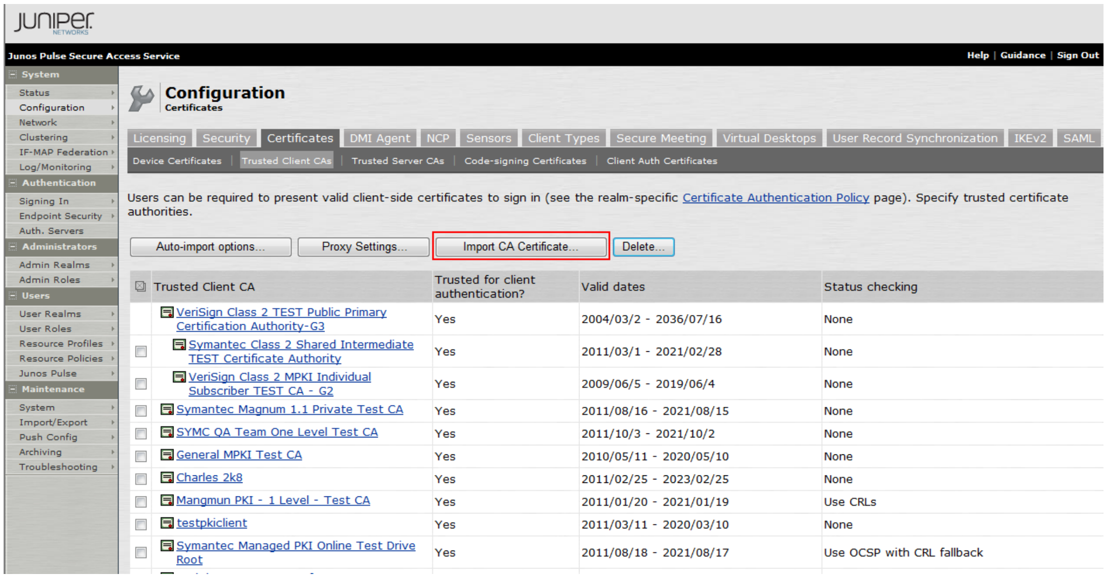
2 Click the **Authentication Policy** tab.

a Click the **Certificate** link.

b Click the **Only allow users with a client-side certificate signed by Trusted Client CAs to sign in** option.

c Click the **Trusted Client CA** link. The Configuration page appears.

d Click **Import CA Certificate** on the Configuration page.


JUNIPer NETWORKS
Junos Pulse Secure Access Service
Help | Guidance | Sign Out
System
Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Configuration
Certificates
Licensing | Security | Certificates | DMI Agent | NCP | Sensors | Client Types | Secure Meeting | Virtual Desktops | User Record Synchronization | IKEv2 | SAML
Device Certificates | Trusted Client CAs | Trusted Server CAs | Code-signing Certificates | Client Auth Certificates
Auto-import options... | Proxy Settings... | Import CA Certificate... | Delete...

Users can be required to present valid client-side certificates to sign in (see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

☐	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
	VeriSign Class 2 TEST Public Primary Certification Authority-G3	Yes	2004/03/2 - 2036/07/16	None
☐	Symantec Class 2 Shared Intermediate TEST Certificate Authority	Yes	2011/03/1 - 2021/02/28	None
☐	VeriSign Class 2 MPKI Individual Subscriber TEST CA - G2	Yes	2009/06/5 - 2019/06/4	None
☐	Symantec Magnum 1.1 Private Test CA	Yes	2011/08/16 - 2021/08/15	None
☐	SYMC QA Team One Level Test CA	Yes	2011/10/3 - 2021/10/2	None
☐	General MPKI Test CA	Yes	2010/05/11 - 2020/05/10	None
☐	Charles 2k8	Yes	2011/02/25 - 2023/02/25	None
☐	Mangmun PKI - 1 Level - Test CA	Yes	2011/01/20 - 2021/01/19	Use CRLs
☐	testpkiclient	Yes	2011/03/11 - 2020/03/10	None
☐	Symantec Managed PKI Online Test Drive Root	Yes	2011/08/18 - 2021/08/17	Use OCSP with CRL fallback

Figure 2-4 Import CA Certificate

e Click **Browse** to import the root and the intermediate CA certificates of the end user certificates downloaded from PKI Manager. These certificates must be installed on the VPN machine so that VPN can trust the users' certificate.

f Click **Import Certificate**.

g Choose **Client certificate status checking**.

h Click **Save Changes**.

3 Click the **Role Mapping** tab to allow end user to sign-in to VPN and get the required access.

a Click **New Rule**.

b Select a rule based on the user name.

c Enter the rule name in the **Name** field.

d Provide a rule for the user name.

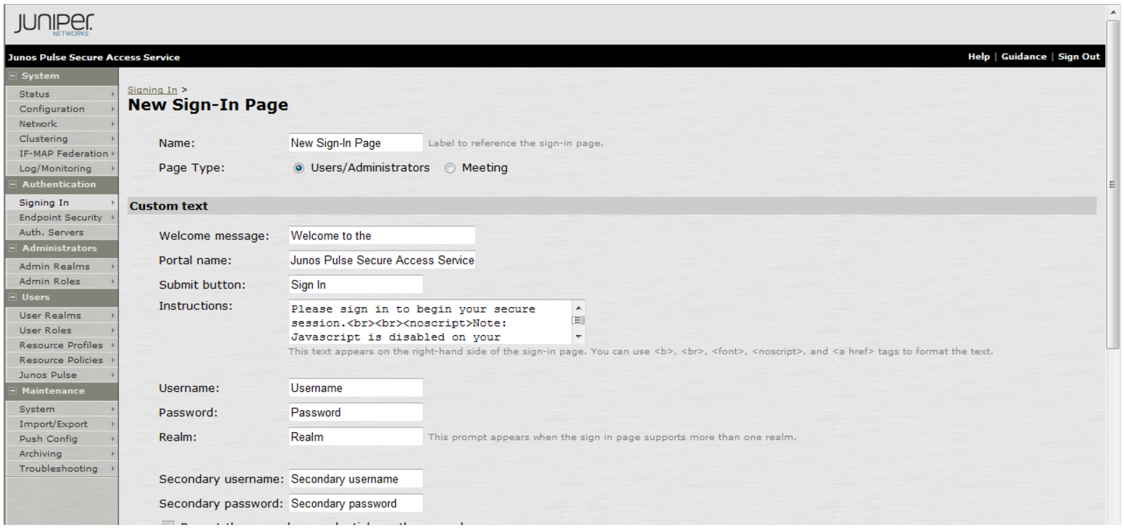
e Assign the role created in "Configuring User Roles on the VPN device" on page 11.

f Click **Save Changes**.

Task 5. Configuring Sign-In Page for the Network Connect Client

1 Click **Authentication** → **Signing In** → **Sign-In Pages**. The Signing In page appears.

2 Click **New Page**. The New Sign-In Page appears.



New Sign-In Page

Name: New Sign-In Page — Label to reference the sign-in page.

Page Type: ● Users/Administrators ○ Meeting

Custom text

Welcome message: Welcome to the

Portal name: Junos Pulse Secure Access Service

Submit button: Sign In

Instructions:

```
Please sign in to begin your secure
session.<br><br><noscript>Note:
Javascript is disabled on your
```

This text appears on the right-hand side of the sign-in page. You can use <b>, <br>, <font>, <noscript>, and <a href> tags to format the text.

Username: Username

Password: Password

Realm: Realm — This prompt appears when the sign in page supports more than one realm.

Secondary username: Secondary username

Secondary password: Secondary password

Figure 2-5 New Sign-in page

3 Enter a name in the **Name** field and update the relevant fields.

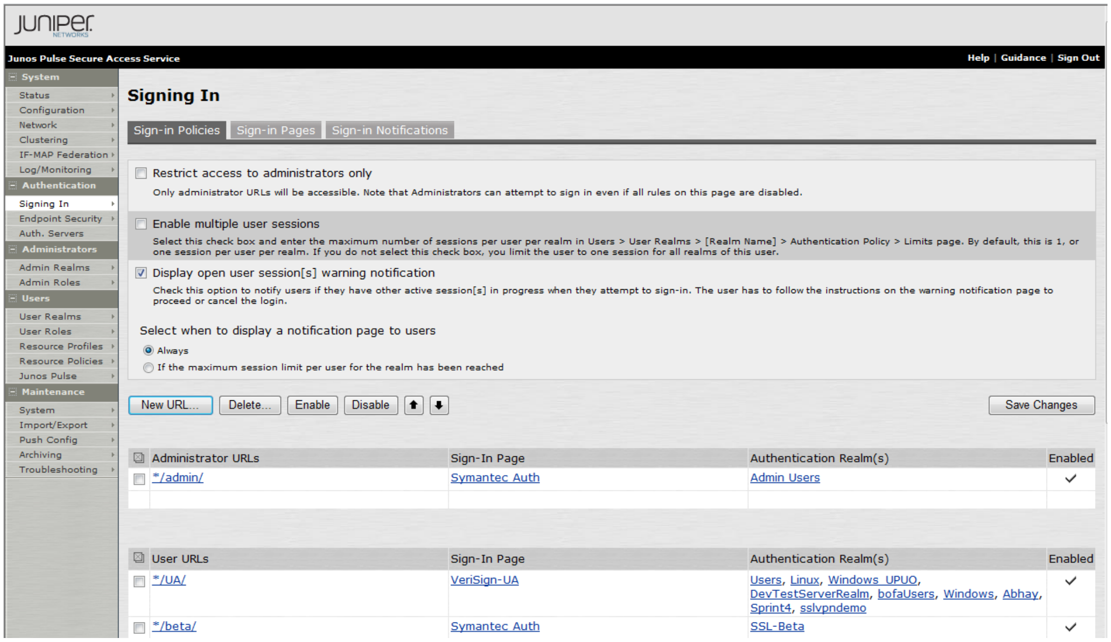
4 Click **Save Changes**.

Task 6. Configure Sign-In Policies for the Network Connect Client

This is standard configuration step in VPN to map between Realm and Sign-in policies. This mandatory configuration is required for successful sign-in.

1 Click **Authentication** → **Signing In** → **Sign-In Policies**. The Signing In page appears.

2 Select the user URLs created in "Configure the User Realm for User Authentication" on page 11, where you want to add the Realm and configure it as needed.



Signing In

☐ Restrict access to administrators only

Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.

☐ Enable multiple user sessions

Select this check box and enter the maximum number of sessions per user per realm in Users > User Realms > [Realm Name] > Authentication Policy > Limits page. By default, this is 1, or one session per user per realm. If you do not select this check box, you limit the user to one session for all realms of this user.

☑ Display open user session[s] warning notification

Check this option to notify users if they have other active session[s] in progress when they attempt to sign-in. The user has to follow the instructions on the warning notification page to proceed or cancel the login.

Select when to display a notification page to users

● Always

○ If the maximum session limit per user for the realm has been reached

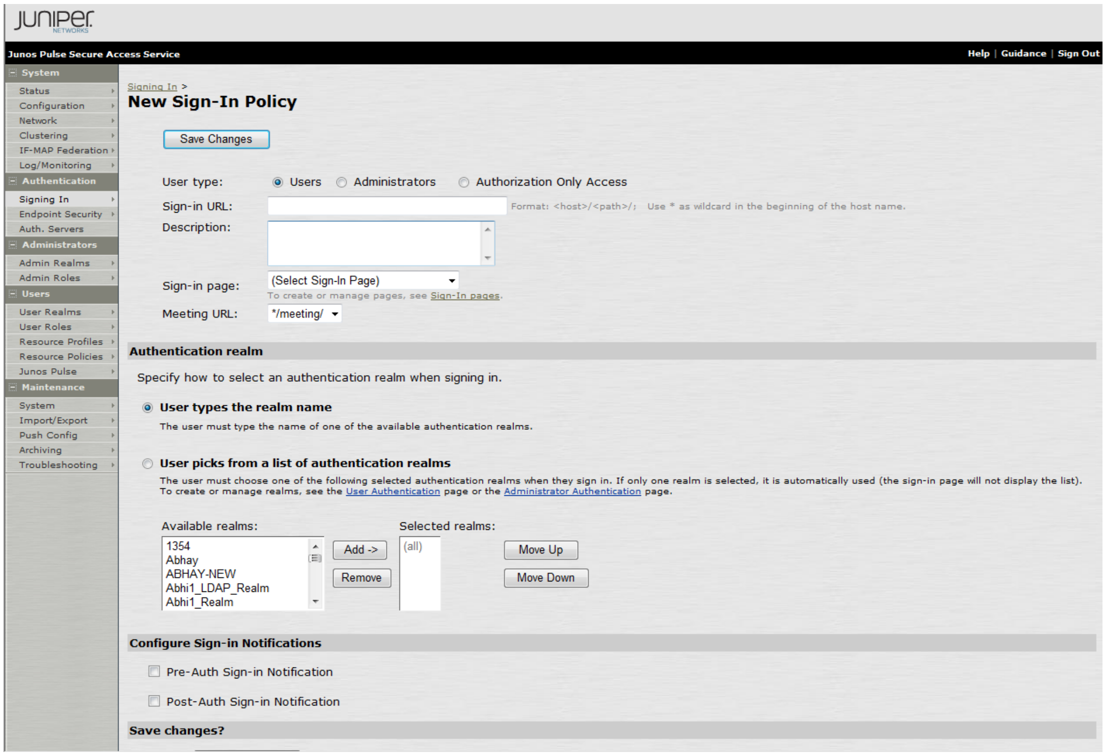
☐	Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
☐	*/admin/	Symantec Auth	Admin Users	✓

☐	User URLs	Sign-In Page	Authentication Realm(s)	Enabled
☐	*/UA/	VeriSign-UA	Users, Linux, Windows_UPUO, DevTestServerRealm, bofaUsers, Windows, Abhay, Sprint4, sslvpndemo	✓
☐	*/beta/	Symantec Auth	SSL-Beta	✓

Figure 2-6 Signing In Policy page

3 Set the page created in the previous step as the Sign-in page from the **Sign-in page** drop-down list.

4 To create a new Sign-in Policy, click **New URL**. The New Sign-In Policy page appears.



Signing In >

New Sign-In Policy

User type: ● Users ○ Administrators ○ Authorization Only Access

Sign-in URL: Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: (Select Sign-In Page)

To create or manage pages, see Sign-In pages.

Meeting URL: */meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

● **User types the realm name**

The user must type the name of one of the available authentication realms.

○ **User picks from a list of authentication realms**

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the User Authentication page or the Administrator Authentication page.

Available realms:
1354
Abhay
ABHAY-NEW
Abhi1_LDAP_Realm
Abhi1_Realm

Selected realms:
(all)

Configure Sign-in Notifications

☐ Pre-Auth Sign-in Notification

☐ Post-Auth Sign-in Notification

Save changes?

Figure 2-7 New Sign-In Policy page

5 Enter the Sign-in URL.

6 Select the **Sign-in page** that you created in the previous step and select the appropriate **Authentication realm** options.

7 Click **Save Changes**.

Specify CDP Options

You can enable and periodically download Certificate Revocation Lists (CRLs) from the CRL Distribution Points (CDPs) to verify the ongoing validity of client-side certificates. For instructions to verify client-side certificates, refer to Juniper documentation available at https://www.juniper.net/techpubs/en_US/sa/topics/task/operational/secure-access-certificates-distribution-points-specifying.html.

Connecting to VPN

The following are various scenarios through which an end user can connect their devices to the Juniper VPN to securely access company resources.

Connecting an iOS device to VPN

1 Open the **Junos Pulse Application** on the iOS device.

2 Tap **Connect**. The status is displayed as connected and VPN is **On**.

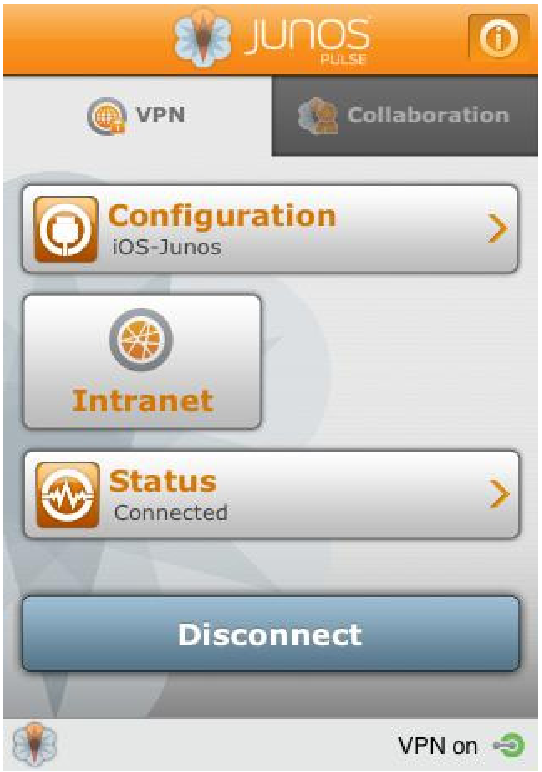
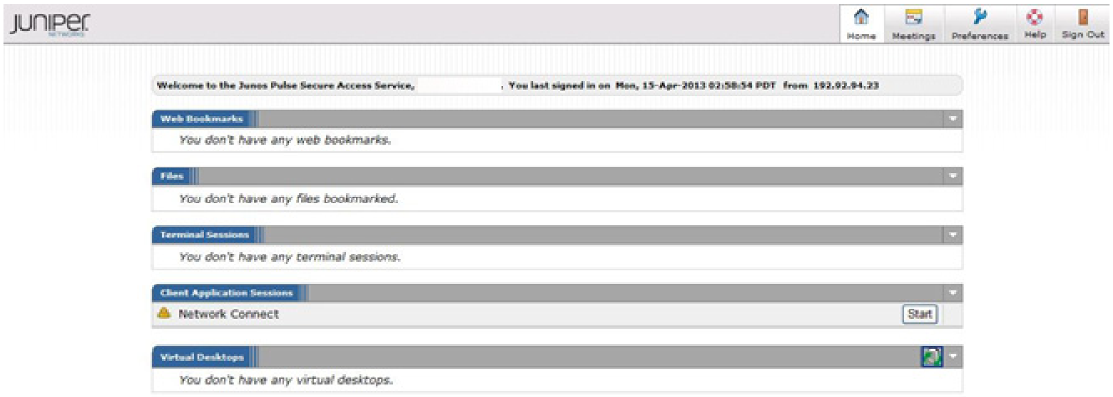


Figure 2-8 Junos Pulse Application

Connecting Desktop/Laptop to VPN

1. Open the browser where the certificate is installed.
2. Access the VPN URL.
3. Select the certificate and click **OK**.
4. Select the Client Application Session and click **Start**.



Welcome to the Junos Pulse Secure Access Service, . You last signed in on Mon, 15-Apr-2013 02:58:54 PDT from 192.92.94.23

You don't have any web bookmarks.

You don't have any files bookmarked.

You don't have any terminal sessions.

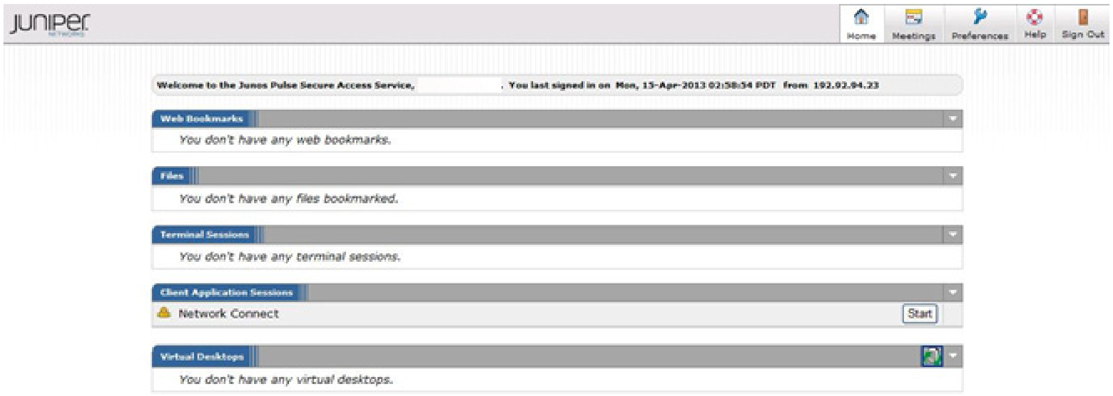
Network Connect

You don't have any virtual desktops.

Figure 2-9 Junos Pulse Secure Access Service for Desktop/Laptop

Connecting Desktop/Laptop to VPN (PKI Client)

1. Open the browser where the certificate is installed.
2. Access the VPN URL.
3. Select the certificate and click **OK**.
4. Enter the PIN for PKI Client when prompted, and click **OK**.
5. Select the Client Application Session and click **Start**.



Welcome to the Junos Pulse Secure Access Service, . You last signed in on Mon, 15-Apr-2013 02:58:54 PDT from 192.92.94.23

You don't have any web bookmarks.

You don't have any files bookmarked.

You don't have any terminal sessions.

Network Connect

You don't have any virtual desktops.

Figure 2-10 Junos Pulse Secure Access Service for PKI Client