

## Remote Access and Desktop Connection Management for Hybrid Cloud VDI

**Version 9.1 and 2022  
August 2022**

## Contacting Leostream

Leostream Corporation  
271 Waverley Oaks Rd  
Suite 204  
Waltham, MA 02452  
USA

<http://www.leostream.com>

Telephone: +1 781 890 2019

To submit an enhancement request, email [features@leostream.com](mailto:features@leostream.com).

To request product information or inquire about our future directions, email [sales@leostream.com](mailto:sales@leostream.com).

## Copyright

© Copyright 2002-2022 by Leostream Corporation

This software program and documentation are copyrighted by Leostream. The software described in this document is provided under a license agreement and may be used or copied only under the terms of this agreement. No part of this manual may be copied or reproduced in any form without prior written consent from Leostream.

## Trademarks

The following are trademarks of Leostream Corporation.

Leostream™

The Leostream graphical logo™

The absence of a product name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that product, name, or logo by Leostream.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of The Open Group. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory, Hyper-V, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

## Patents

Leostream software is protected by U.S. Patent 8,417,796.

# Contents

Contents	3
Overview	4
How SSL VPNs work	4
Authentication	4
Networking and Encryption	4
Juniper Networks® SSL VPN Setup	5
Configuring Juniper Networks Roles	6
Building a General Role for Leostream	6
Expanding the Role for Java RDP Clients	7
Expanding the Role to use winlaunchterm.cgi for RDP Connections	8
Expanding Roles to Bypass the Connection Broker Bookmark	9
Defining Role Mappings	10
Configuring Connection Broker Web Resource Profiles in Juniper Networks	12
Assigning the Connection Broker Resource to the Juniper Networks Role	15
Configuring Resource Policies	15
Configuring a Web Rewriting Policy	15
Setting up a Terminal Services Access Control Policy	18
Configuring Single Sign-On to Leostream	19
Configuring Protocol Plans in the Connection Broker	21
Launching Connections using winlaunchterm.cgi and Microsoft RDP	21
Launching Connections using a Java RDP Client	23
Signing the Elusiva Open Source Java RDP Client	26
Cisco® 55xx SSL VPN Setup	27
General Cisco SSL VPN Setup	28
Setting up the Cisco SSL VPN to Work with the Connection Broker	30
Configuring a Connection Broker Bookmark	30
Single Sign-On URL Post	32
Assigning the Bookmark to a Group Policy	33
Assigning Users to a Group Policy	34
Logging in Through the Cisco SSL VPN	34
Using the Cisco Systems VPN Client with Leostream Connect	34
F5® FirePass® SSL VPN Setup	37

## Overview

The Connection Broker is a management layer, not a proxy solution. Therefore, the display protocol does not travel through the Connection Broker. For external access to desktops, the Connection Broker uses your existing hardware-based SSL VPN device, allowing you to provide secure access to traveling users without needing to qualify another SSL VPN solution.

You can also use the Leostream Gateway to tunnel traffic from your user's client to their isolated remote desktop. See the [Leostream Gateway Guide](#) for more information.

## How SSL VPNs work

An SSL VPN performs two functions:

- Authentication
- Encryption of data as it passes over the Internet from the user's computer to the corporate network.

## Authentication

Users typically access an SSL VPN using a Web browser. Their Web browser recognizes the SSL certificate in the SSL VPN server as being valid and containing the correct address. The addition of Leostream to an existing SSL VPN does not change the security model.

The SSL VPN must pass the user's username and password to the Connection Broker in order for the user to have single sign-on to the broker. This information transfer can be problematic if the SSL VPNs authenticates against a stand-alone Radius server, rather than against an LDAP server such as Microsoft Active Directory®. In addition, if the SSL VPN requires only the username and cryptographic key, the SSL VPN cannot pass sufficient information for single sign-on.

The simplest solution is for the SSL VPN to first authenticate against the radius server, and then to authorize against the Connection Broker. The latter step passes the user credentials to the Connection Broker.

## Networking and Encryption

SSL VPNs break the standard model of networking. They take data packets from the corporate network, or the user's computer, and send them across a connection established at the application level. To do so, they act as a form of advanced reverse proxy. In the user's computer, the networking layer thinks it is talking to a device on the local network. At corporate end, the corporate computers also think they are talking to a local device.

The key element of an SSL VPN is a virtual network adapter. The adaptor appears to the operating system as a normal network adapter, but instead sends it to an application. This application could be an SSL VPN application that encrypts the data and sends it across a pipe to another SSL VPN

application that sends it to another virtual network adapter so it reappears.

In the simplest case, the network within the user's computer is *bridged* with the corporate network, but this requires both networks to be within the same subnet. For example, assume the user has an IP address of 172.29.229.151 and the server they are talking to has an IP address of 172.29.229.23. It does allow LAN broadcasts (required by services such as Windows NetBIOS file sharing and network neighborhood browsing).

The other option is *routing*, where the user's computer is on one subnet, with an address of 192.168.2.151, and the corporate network is on another subnet 172.29.229.xxx with a server at 172.29.229.151. This is more efficient because only traffic destined for the remote system passes over the SSL VPN encrypted tunnel, but it requires routes to be setup that link each subnet.

The networking operation is carried out at the end user's computer in one of two ways. The first approach is to install an SSL VPN client after which all the user's applications have access to the remote network.

After the SSL VPN sets up a network connection, the Leostream Connect client can be run on the user's computer or the user can launch connection from the Leostream Web client.

## Juniper Networks® SSL VPN Setup

The Leostream Connection Broker integrates with the Juniper Networks® SSL VPN providing users with secure access to their resources from outside the corporate network. Configuring your Juniper Networks SSL VPN and Connection Broker to work together consists of the following steps.

1. Configure the Juniper Networks SSL VPN administrator interface to include the following:

- a. User Roles to enable access to the Resource Profiles defined for the Leostream Connection Broker.

If your users log in from client devices running different operating systems, such as Windows or Macintosh, you will need different roles for each user.

- b. Web Application Resource Profiles defined for the Leostream Connection Broker. The type of Web Application Resource Profile you create depends on the type of connections your users are establishing.

In these Resource Profiles, you'll set Web Access Control and Single Sign-on auto-policies to allow connection(s) to backend resources and provide single sign-on to the Connection Broker.

2. Build Connection Broker protocol plans for users who connect via the Juniper Networks SSL VPN.



Juniper Networks and Leostream use common terms such as Roles and Policies, but these terms relate to different concepts in the two products.

The following sections describe these steps in more detail. For complete instructions on working with the Juniper Networks Secure Access administrator interface, see the [Administration Guide](#) available from the Juniper Networks Web site.



The Juniper device does not inform the Connection Broker when the user logs out or disconnects from their remote desktop. To invoke actions specified in a user's release plan after logging in via a Juniper SSL VPN, you must install a Leostream Agent on the remote desktop.

## Configuring Juniper Networks Roles

The first step in integrating Leostream and Juniper Networks is to create Juniper Networks Roles and map these Roles to users via the Juniper Networks User Realms. After creating Roles, you create Resource Profiles for your Connection Broker and assign those Resource Profiles to these Roles.

The number of Juniper Networks Roles you need, and their configuration, depends on what viewing clients are used to launch connections and on the number of different viewing clients you need to support. If all users use the same set of viewing clients, you can use one Role. If you have users logging in from client devices running different operating systems, such as Microsoft Windows and Apple Macintosh, and you want to use different viewing clients for each operating system, you need two Roles.

### Building a General Role for Leostream

You create a general Role for your Leostream Connection Broker, as follows.

1. Select the **Users > User Roles > New User Role** menu from the left-side of your Juniper Networks device Central Manager.
2. In the **Name** edit field, provide a descriptive name for this role.
3. Optionally, enter a description for this role in the **Description** edit field, for example:

Roles >  
New Role

Name:

Description:

4. After a user logs into the Juniper Networks device, the default start page typically displays a list of bookmarks for the user's offered Resource Profiles, one of which points to the

Leostream Connection Broker. You can, instead, automatically log the user into the Connection Broker after they log into the Juniper Networks device by over-riding the default start page. To automatically log the user into Leostream, ensure that the **UI Options** check box in the **Options** section is selected if you want to over-ride the default start page associated with all User Roles

5. In the **Access features** section, select the **Web** check box to provide access to your Leostream Connection Broker, as shown in the following figure

**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
- ☐ IKEv2

6. Click **Save Changes** at the bottom of the form to finish creating the new role

To have this role go to the Connection Broker **Sign In** page, instead of displaying a bookmark for the Connection Broker, modified the General UI Options, as described in [Expanding Roles to Bypass the Connection Broker Bookmark](#).

Additional Role configuration may be necessary depending on the type of viewing clients your users launch. The following sections can be combined to build Roles that allow users to launch a variety of client types.

- To configure the Role to allow users to connect to desktop using a Java RDP client, see [Expanding the Role for Java RDP Clients](#)
- To configure the Role to use `winlaunchterm.cgi` to launch Microsoft RDP connections to desktops, see [Expanding the Role to use winlaunchterm.cgi for RDP Connections](#)

### Expanding the Role for Java RDP Clients

Users that log into the Juniper Networks device from client devices running a Linux or Macintosh operating system need to use a Java RDP client to launch connections to desktops. The Juniper Networks `winlaunchterm.cgi` script does not support these operating systems.

To create a Role:

1. Create a Role using the procedure described in [Configuring Juniper Networks Roles](#).
2. Any Resource Policies associated with this role must include a Java Access Control Policy.

After the Role is complete, create a Web Resource Profile for your Connection Broker (see [Configuring Resource Policies](#)).

### Expanding the Role to use winlaunchterm.cgi for RDP Connections

For users logging in from a Windows client, you can build a Role that uses the `winlaunchterm` command to launch RDP connections. To create the Role:

1. Create a Role using the general procedure described in [Configuring Juniper Networks Roles](#).
2. In this Role, click on the **General** tab.
3. In the **General** tab, click on the **Overview** tab.
4. In the **Access features** section, select the **Terminal Services** check box. Your role now has two check boxes selected, as shown in the following figure

**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
  - ☐ Java versionNote: On Windows Mobile, WSAM functionality is delivered via Junos Pulse
- ☐ Telnet/SSH
- ☒ **Terminal Services**
- ☐ Virtual Desktops
- ☐ Meetings
- ☐ Email Client
- ☐ Network Connect
  - ☒ Network Connect
  - ☐ Junos Pulse
- ☐ IKEv2

5. Click **Save Changes** at the bottom of the form.
6. Within this role, go to the **Terminal Services** tab.
7. In the **Terminal Services** tab, go to the **Options** tab.
8. Select the **User can add sessions** option, as shown in the following figure.



The screenshot shows a web interface for configuring Citrix client delivery methods. The 'Options' section at the bottom contains two checkboxes: 'User can add sessions' (checked) and 'Enable Remote Desktop Launcher' (unchecked). A red arrow points to the 'User can add sessions' checkbox.

9. Click **Save Changes**.

10. In order to use `winlaunchterm.cgi` to establish RDP connections, you must create the following Resource Policies and assign them to this Role.

- [Web Rewriting Policy](#) – If you do not create a Web Rewriting Policy, clicking on the **Connect** link for a desktop after logging into Leostream produces no results.
- [Terminal Services Access Control Policy](#) – If you do not create a Terminal Services Access Control Policy, clicking **Connect** link for a desktop after logging into Leostream launches the RDP connection to the desktop, but the connection fails.

This role is appropriate for any client device that launches RDP connections using the Juniper Networks `winlaunchterm` command, called from a Leostream protocol plan or directly by the Juniper Networks device.

After the Role is complete, create a Web Resource Profile for your Connection Broker. See [Configuring Resource Policies](#) for more information.

### Expanding Roles to Bypass the Connection Broker Bookmark

If your users log into the Juniper Networks device to access only the Leostream Connection Broker, you can configure their Juniper Networks Role to skip the Bookmarks page and, instead, directly log the user into Leostream.

To configure a Role to log directly into the Connection Broker:

1. From the Central Manager menus, select the **Users > User Roles**.
2. From the list of Roles, click the name of the role that will log users into Leostream.

3. In this role's **General** tab, click on the **UI Options** tab.
4. Scroll down to the **Start page** section.
5. Select the **Custom page** option.
6. In the **Start page URL**, enter the URL to your Connection Broker, including the port number, as shown, for example, in the following figure.

7. Select the **Also allow access to directories below this url** option.
8. Click **Save Changes**.

## Defining Role Mappings

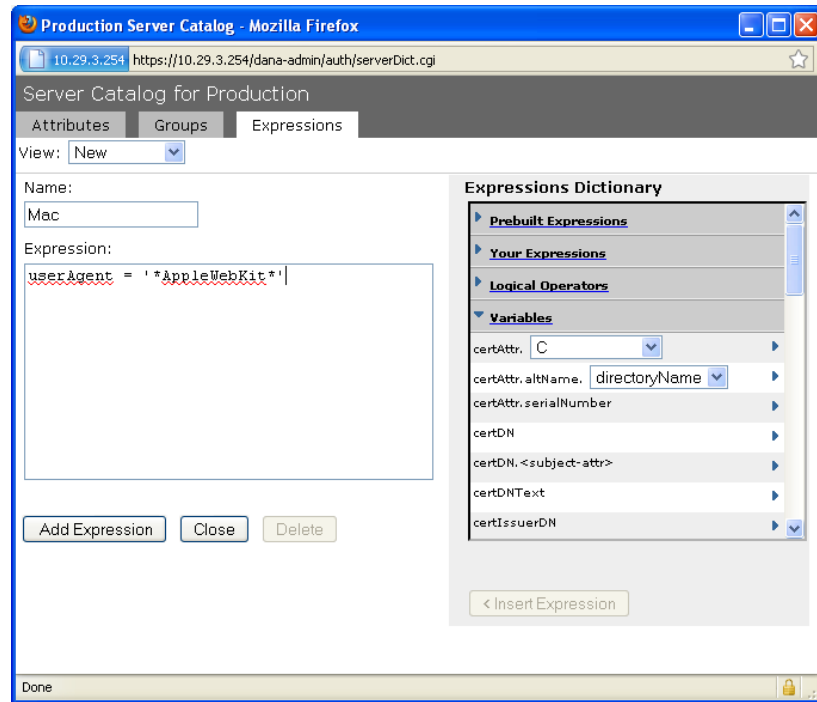
Use Role Mappings within your User Realms to assign the correct Role to users, based on the type of client they use. For example, the following procedure creates a rule that assigns a user logging in using a Safari Web browser to the `Leostream - Mac` role.

1. Select the **User Realms > Users > Role Mapping** menu from the left-side of your Juniper Networks device Central Manager.
2. Click **New Rule**.
3. From the **Rule based on** drop-down menu, select **Custom Expressions**. Custom Expressions allow you to define rules that filter users based on their Web browser type.
4. Click **Update** next to the **Rule based on** drop-down menu.
5. In the **Name** edit field, provide a unique name for this Role Mapping Rule, for example, `Leostream - Mac`.
6. If you do not already have a custom expression that filters by Web browser type, click **Expressions** in the **Rule: If user has any of these custom expressions...** section. Otherwise, skip to step 7.
  - a. In the **Expressions** tab of the **Server Catalog for Production** dialog that opens, enter a name for the new custom expression in the **Name** edit field.

- b. In the **Expressions** edit field, enter the following string to distinguish Safari Web browsers. To distinguish other types of Web browsers, modify your custom expression, accordingly.

```
userAgent = '*AppleWebKit'
```

For example:



- c. Click **Add Expression**.
- d. Click **Close** to return to the form for creating the new Rule.
- From the **Available Expressions** list, select your custom expression.
  - Click **Add->** next to the **Available Expressions** list.
  - From the **Available Roles** list in the **...then assign these roles** section, select the role to associated with this expression. In this example, because the custom expression is filtering on the Safari Web browser, the **Leostream - Mac** Role is selected.
  - Click **Add->**.
  - If a user assigned to a role by this rule should not be assigned to any other role, select the **Stop processing rules when this rule matches** option.

## 12. Click **Save Changes**.

The rules in the Role Mapping table are processed from top-down. If you have multiple Rules for users logging into Leostream, place the most restrictive Rule first, followed by roles with decreasing restrictions.

For example, in the following figure, the first rule assigns the `Leostream - Mac` role based on the custom expression created in the previous procedure. Users logging in from a Safari Web browser satisfy this Rule. All other users fall through the first Rule and satisfy the second Rule, thereby being assigned to the `Leostream - Windows` Role.

**Users**

General Authentication Policy **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete ↑ ↓ Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/> 1.	<code>matches_expression "Mac"</code>	→ <code>Leostream - Mac</code>	Leostream - Mac	✓
<input type="checkbox"/> 2.	<code>username is ""</code>	→ <code>Leostream - Windows</code>	Leostream - Windows	✓

## Configuring Connection Broker Web Resource Profiles in Juniper Networks

Leostream integrates with Juniper Networks via Web Resource Profiles. The following procedure creates a Resource Profile that can be used for the following connection types:

- Standard Microsoft RDP client connections created by the Juniper Networks `winlaunchterm` script. This option uses the **Juniper SSL VPN** section of the Leostream Connection Broker protocol plan.
- Java RDP client connections created by a URL defined in the Connection Broker. This option uses the **External Viewer** section of the Leostream Connection Broker protocol plan.

To create a Custom Resource Profile for Leostream:

1. Select the **Users > Resource Profiles > Web** menu from the left-side of your Juniper Networks device Central Manager.
2. Click **New Profile**.
3. From the **Type** list, select **Custom**.
4. Enter a name into the **Name** edit field.
5. Optionally enter a description into the **Description** edit field.

6. Enter your Connection Broker URL into the **Base URL** edit field. Ensure that you include the port number, for example:

```
https://broker_address.mycompany.com:443
```

7. Ensure that the auto-policy for Web Access Control is enabled. Your form appears similar to the following figure.

Web Application Resource Profiles >  
New Web Application Resource Profile

Type: \* Custom

Name: \* Leostream - Custom

Description:

Base URL: \* https://172.29.229.211:443

Autopolicies: Autopolicies are resource policies that correspond to you must enter a fully qualified domain name in your

[Show ALL autopolicy types >>](#)

☒ **Autopolicy: Web Access Control**

Use this autopolicy to control access to web servers and URLs.

[Delete](#) [↑](#) [↓](#)

Resource	Action	
<div></div>	<span>Allow</span>	<a href="#">Add</a>
<input type="checkbox"/> https://172.29.229.211:443/*	Allow	

Examples:  
http://\*.domain.com/public/\*  
https://www.domain.com:443/

8. If you plan to use Java RDP clients for connections, turn on the auto-policy for Java Access Control, as follows.

- a. Click the **Show ALL autopolicy types >>** button
- b. Check the **Autopolicy: Java Access Control** option. The section expands, as shown in the following figure.

☒ **Autopolicy: Java Access Control**

Use this autopolicy to specify the servers and ports to which java applets connect. You may also use this autopolicy to enable re-signing using code-signing certificates.

[Delete](#) [↑](#) [↓](#)

Resource	Action	
<div></div>	<span>Allow socket access</span>	<a href="#">Add</a>
<input type="checkbox"/> 172.29.229.211:443	Allow socket access	

☒ Sign applets with uploaded [code-signing certificate\(s\)](#)

- c. In the edit field below the **Resource** table header, enter the following text.

```
*:3389
```

If you establish RDP connections on a non-standard RDP port, change 3389 to your specific port number.

- d. Leave the default selection of **Allow socket access** in the **Action** drop-down menu.
- e. Click **Add**.
- f. By default, the Juniper Networks device resigns Java applets using a self-signed certificate. To have the Juniper Networks device resign the Java applet with an uploaded certificate, select the **Sign applets with uploaded code-signing certificates**. Consult the Juniper Networks documentation for more information on uploading and using code-signing certificates.

The Java access control policy should appear similar to the following figure.



9. If you want the Juniper Networks device to pass the user's credentials to the Connection Broker, providing single sign-on from the Juniper Networks device to the Connection Broker and the user's resources, enable the **Single Sign-on** auto-policy. See [Configuring Single Sign-On to Leostream](#) for instructions.
10. Click **Save and Continue**.
11. To assign Roles to this Resource Profile:
- In the **Roles** tab that opens, select the **Role** to which this Resource Profile applies. Ensure that the Role is configured correctly based on what type of RDP connection is being established.
  - Click **Add->**.
  - Click **Save Changes**.

The Juniper Networks device automatically generates a bookmark for the Resource Profile that

points to the Leostream Connection Broker **Sign In** page. You can opt to not display this bookmark to the Leostream user and, instead, automatically open the **Sign In** page after the user logs into the Juniper Networks device. See [Expanding Roles to Bypass the Connection Broker Bookmark](#) for instructions.

Users assigned to this type of Resource Profile should have Connection Broker policies that use protocol plans set to either the **Juniper SSL VPN** or **External Viewer** option. See [Configuring Protocol Plans in the Connection Broker](#) for information on configuring Connection Broker protocol plans.

## Assigning the Connection Broker Resource to the Juniper Networks Role

After you create and save Resource Profiles, you can add or modify the Roles associated with those Resource Profiles using the **Roles** tab. To access and use the **Roles** Tab.

1. Select the **Users > Resource Profiles > Web** menu from the left-side of your Juniper Networks device Central Manager.
2. Click on the name of the Resource Profile in the list.
3. Go to the **Roles** tab.
4. To add a Role:
  - a. Select your Connection Broker role in the **Available Roles** list.
  - b. Click **Add ->**.
5. To remove a Role:
  - a. Select your Connection Broker role in the **Selected Roles** list.
  - b. Click **Remove**.
6. Click **Save Changes**.

## Configuring Resource Policies

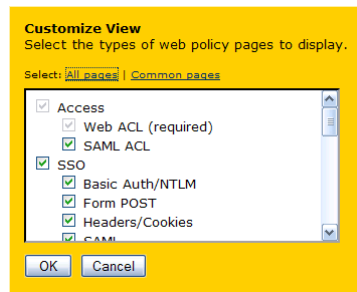
### Configuring a Web Rewriting Policy

By default, the SSL VPN dynamically rewrites the Connection Broker URL. To avoid this, create a Selective Rewrite Web Resource Policy that instructs the Juniper Networks Secure Access device to not rewrite the Connection Broker URL, as follows.

1. Select the **Users > Resource Policies > Web** menu from the left-side of your Juniper

Networks device Central Manager.

2. If the **Rewriting** tab is not displayed on the **Web Access Policies** page, click the **Customize** button located to the right of the tabs. In the **Customize View** dialog that opens, shown in the following figure:
  1. Click the **All pages** link.
  2. Click **OK**. You should notice a number of tabs appear on the form.



3. Click the **Rewriting** tab.
4. Click the **Selective Rewriting** tab.
5. Click **New Policy**.
6. Create a new Selective Rewrite policy, as follows:
  1. Enter a name for the policy in the **Name** edit field, for example, **Don't-Rewrite-Leostream-CB-Response**.
  2. In the **Resources** list, enter the hostname or IP address for your SSL VPN outside the firewall. This is *not* the Connection Broker IP address; it is the external URL of the Juniper Networks device that the users connect to.  
  
For example:      `https://sslvpn.yourcompany.com/*`
  3. In the **Roles** section, select your Leostream Role from the **Available roles** list.
  4. Click **Add->** to move the Role into the **Selected roles** list.
  5. In the **Actions** section, select **Don't rewrite content, Redirect to target web server**.
  6. Click **Save Changes**. Your configuration should look similar to the following figure.



Web Rewriting Policies >

## Dont-Rewrite-Leostream-CB-Response

General Detailed Rules [Customize...](#)

\* Name:  Required: Label to reference this policy.

Description:

**Resources**

Specify the resources for which this policy applies, one per line. In order for your resource comparisons to work effectively, you must enter a fully qualified domain name in your resource.

\* Resources:  Examples:  
http://\*.domain.com/public/\*  
https://www.domain.com:443/\*  
10.10.10.10/255.255.255.0:80,443/public/\*  
10.10.10.10/24:8000-9000/\*

**Roles**

☐ Policy applies to ALL roles  
☒ Policy applies to SELECTED roles  
☐ Policy applies to all roles OTHER THAN those selected below

Available roles:

Add -> Remove

Selected roles:

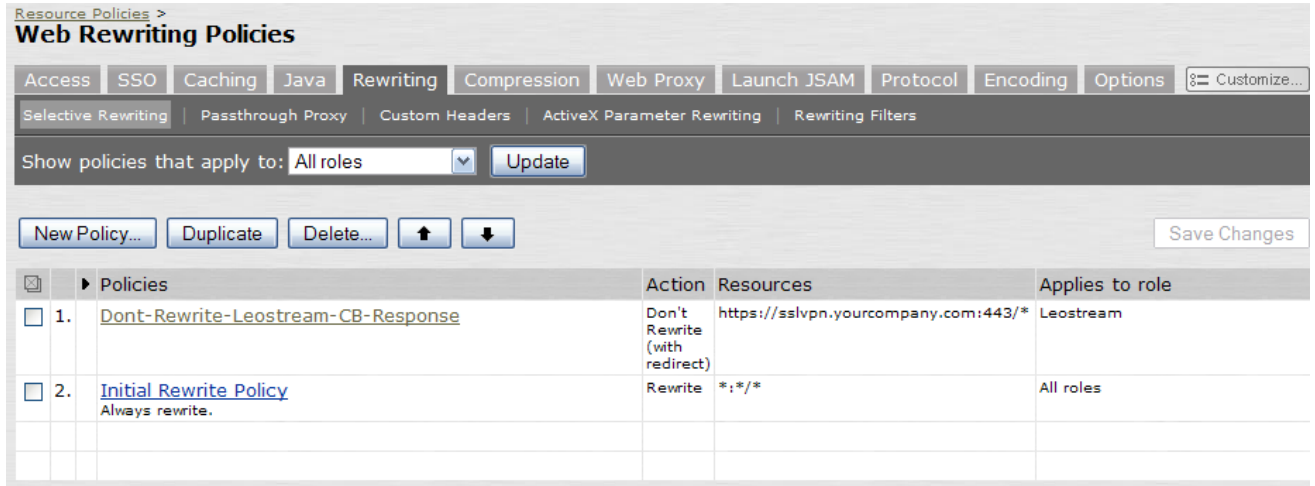
**Action**

☐ Rewrite content (auto-detect content type)  
☐ Rewrite content as...

☒ Don't rewrite content: Redirect to target web server  
☐ Don't rewrite content: Do not redirect to target web server  
☐ Use Detailed Rules (see [Detailed Rules](#) page)

**Save changes?**

The Juniper Networks device applies Resource Policies from top to bottom. After creating the new Rewriting Policy, ensure that you move it above the default Initial Rewrite Policy, as shown in the following figure.



### Setting up a Terminal Services Access Control Policy

By default, the SSL VPN blocks access to Remote Desktop/Terminal Server (3389/tcp). If you initiate an RDP connection using the `winlaunchterm` command, you must define a Terminal Services Access Control Policy, as follows.

1. Select the **Users > Resource Policies > Terminal Services > Access Control** menu from the left-side of your Juniper Networks device Central Manager.
2. Click **New Policy**.
3. Enter a name for the policy in the **Name** edit field.
4. Optionally provide a description for the new Resource Policy in the **Description** field.
5. In the **Resources** section, enter the following text to allow access to port 3389.  
  
\*:3389
6. In the **Roles** section, select your Leostream Role from the **Available roles** list.
7. Click **Add->** to move the Role into the **Selected roles** list.
8. In the **Action** section, select **Allow access**.
9. Click **Save Changes**.

Your configuration should look similar to the following figure.

Terminal Services Policies >  
**Leostream TS ACL**

General Detailed Rules

\* Name:  Required: Label to reference this policy.

Description:

**Resources**

Specify the resources for which this policy applies, one per line.

\* Resources:  Examples:  
<USER>.domain.com:22,23  
exchange\*.domain.com:\*  
10.10.10.10/255.255.255.0:80,443,8080  
10.10.10.10/24:8000-9000

**Roles**

☐ Policy applies to ALL roles  
☒ Policy applies to SELECTED roles  
☐ Policy applies to all roles OTHER THAN those selected below

Available roles:

Add -> Remove

Selected roles:

**Action**

☒ Allow access  
☐ Deny access  
☐ Use Detailed Rules (see [Detailed Rules](#) page)

Save changes?

## Configuring Single Sign-On to Leostream

Optionally, you can enable an advanced policy to forward the user's credentials to the Leostream Connection Broker. With single sign-on enabled, the user is automatically logged into the Connection Broker and their offered resources.

To enable single sign-on:

1. Select the **Resource Profiles > Web** menu from the left-side of your Juniper Networks device Central Manager
2. Click on the name of the Web Application Resource Profile to edit.

3. Click the **Show ALL autopolicy types >>>** button.
4. Select **Autopolicy: Single Sign-on** option.
5. Select the radio button for **Remote SSO**.
6. Select the **POST the following data** option.
7. In the **Resource** edit field, enter the URL for your Connection Broker.
8. In the **Post URL** edit field, enter the URL to your Connection Broker Sign in page, for example:  
  

```
https://leostream-cb.yourcompany.com:443/index.pl
```
9. Ensure that the **Deny direct logon for this resource** and **Allow multiple POSTs to this resource** options are not selected.
10. In the table of post parameters, enter the following information:

Label	Name	Value	User modifiable?
user	user	<USERNAME>	Not modifiable
password	password	<PASSWORD>	Not modifiable
__save	__save	Sign In	Not modifiable
__DATA_FIELDS	__DATA_FIELDS	password,user	Not modifiable
__FORM_SUBMIT	__FORM_SUBMIT	1	Not modifiable



Please note the single ('\_') and double ('\_\_') underscores used in the example, and that the value for <USERNAME> and <PASSWORD> must include the less than and greater than signs. All fields are case sensitive.

The Leostream Connection Broker Web Resource Profile form looks similar to the following figure.

☒ **Autopolicy: Single Sign-on**

Use this autopolicy to automatically pass user credentials to the Web application.

☐ Disable SSO  
☐ Basic Auth  
☐ NTLM  
☐ Kerberos  
☐ Constrained Delegation  
☒ Remote SSO

☒ POST the following data

Resource : \*

Post URL: \*

☐ Deny direct login for this resource  
☐ Allow multiple POSTs to this resource

Label	Name	Value	User modifiable?
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Not modifiable
<input checked="" type="checkbox"/>	user	<USERNAME>	Not modifiable
<input checked="" type="checkbox"/>	password	<PASSWORD>	Not modifiable
<input checked="" type="checkbox"/>	__save	Sign In	Not modifiable
<input checked="" type="checkbox"/>	_DATA_FIELDS	password,user	Not modifiable
<input checked="" type="checkbox"/>	_FORM_SUBMIT	1	Not modifiable

☐ Send the following data as request headers

Resource : \*

Header name	Value
<input type="text"/>	<input type="text"/>

11. Click **Save Changes**.



You can use the **Send the following data as request headers** to pass additional information about the client to the Connection Broker. The information appears in the HTTP head string, which you can view if you edit the client in the Connection Broker. You can use the HTTP header string to create client locations, for example.

## Configuring Protocol Plans in the Connection Broker

The following sections describe how to create Connection Broker protocol plans to use in conjunction with a Juniper Networks device. After you create the protocol plan, associated it with pools in the policies assigned to your users that log in remotely.

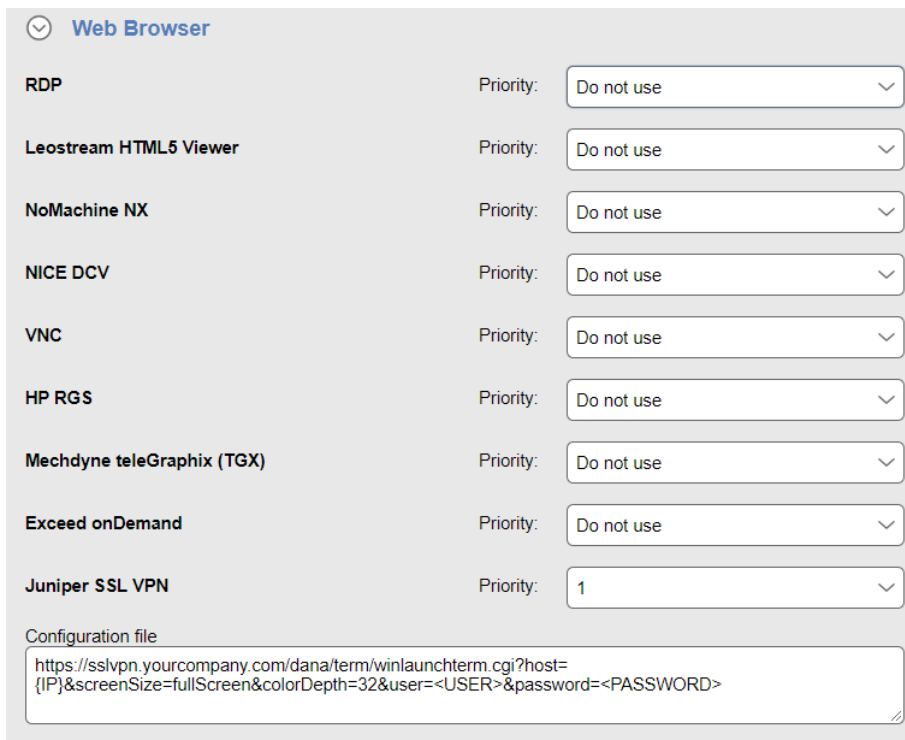
### Launching Connections using winlaunchterm.cgi and Microsoft RDP

You can configure a Connection Broker protocol plan that sends a Terminal Services request to the Juniper Networks device. Use this protocol plan with Juniper Network Web Resource Profile configured to use `winlaunchterm.cgi` (see [Creating Custom Resource Profiles for Microsoft RDP and Java RDP Connections](#)).

The following procedure configures a protocol plan that uses the `winlaunchterm.cgi` command to launch the Microsoft RDP client.

1. Open the **Edit Protocol Plan** page for the protocol plan to assign to the desktops for users who log in through the SSL VPN.

2. Select **1** from the **Priority** drop-down menu for **Juniper SSL VPN** in the **Web Browser** section, as shown in the following figure.
3. Select **Do not use** from the **Priority** drop-down menu for all other protocols in the **Web Browser** section, as shown in the following figure.



**Web Browser**

RDP	Priority: Do not use
Leostream HTML5 Viewer	Priority: Do not use
NoMachine NX	Priority: Do not use
NICE DCV	Priority: Do not use
VNC	Priority: Do not use
HP RGS	Priority: Do not use
Mechdyne teleGraphix (TGX)	Priority: Do not use
Exceed onDemand	Priority: Do not use
<b>Juniper SSL VPN</b>	Priority: <b>1</b>

Configuration file

```
https://sslvpn.yourcompany.com/dana/term/winlaunchterm.cgi?host={IP}&screenSize=fullScreen&colorDepth=32&user={DOMAIN}\<USER>&password=<PASSWORD>
```

4. Enter the URL in the **Configuration file** edit field, for example:

```
https://sslvpn.yourcompany.com
/dana/term/winlaunchterm.cgi?host={IP}&screenSize=fullScreen&colorDepth=
32&user={DOMAIN}\<USER>&password=<PASSWORD>
```

Where *sslvpn.yourcompany.com* is the external address of your Juniper IVE.

In this URL:

- Parameters are case sensitive
- You can combine using ampersand characters (&)
- You can set variables using Connection Broker or Juniper dynamic tags.

The Connection Broker replaces the { IP } dynamic tag with the hostname or IP address of the user's remote desktop. The Juniper device replaces the <USER> and <PASSWORD> dynamic tag with the user's credentials.

You can include the following additional options in the URL:

- `screensize (screenSize=fullScreen, screenSize=800x600, screenSize=1024x768, screenSize=1280x1024)`
- `connectDrives (connectDrives=Yes, connectDrives=No)`
- `connectPrinters (connectPrinters=Yes, connectPrinters=No)`

### Launching Connections using a Java RDP Client

You can use the **External Viewer** option in Connection Broker protocol plans to launch desktop connections using a third-party Java RDP client. Use this protocol plan with Juniper Network Web Resource Profiles that contain the necessary Java Access Control Policy.

The following list includes examples of third-party Java RDP clients.

- Elusiva Open Source [Java Remote Desktop Protocol](#) client



You must manually sign the Elusiva Java RDP client before you can use it within your Connection Broker. See [Signing the Elusiva Open Source Java RDP Client](#) for instructions.

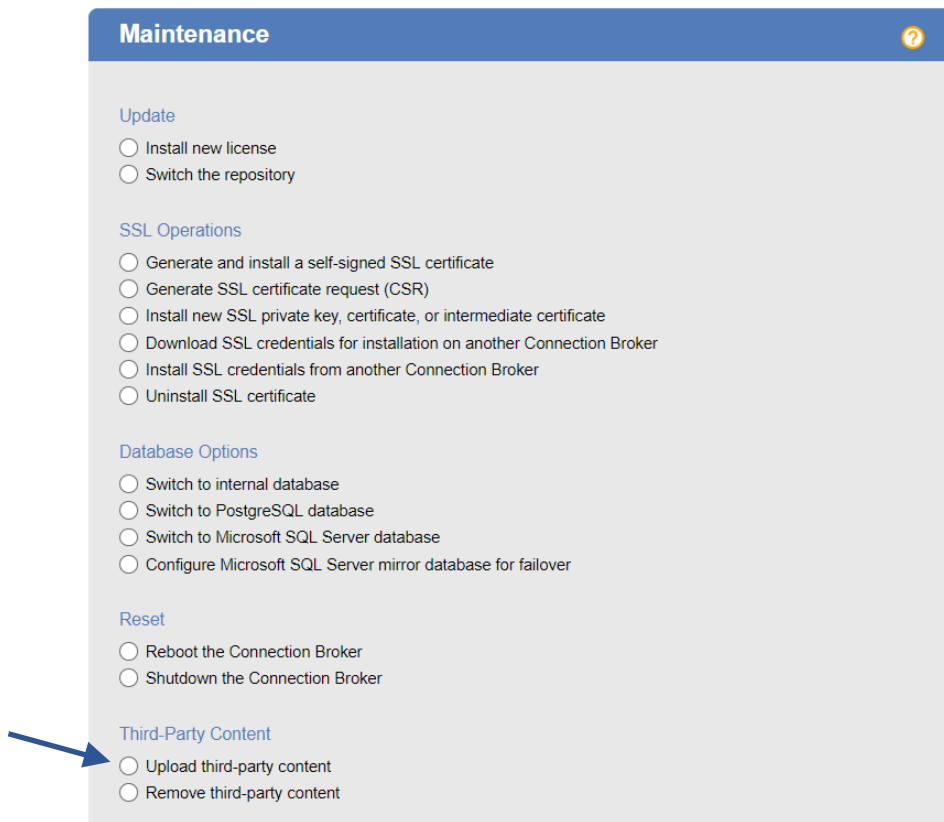
- HOB Inc., [HOBLink JWT](#) Java client



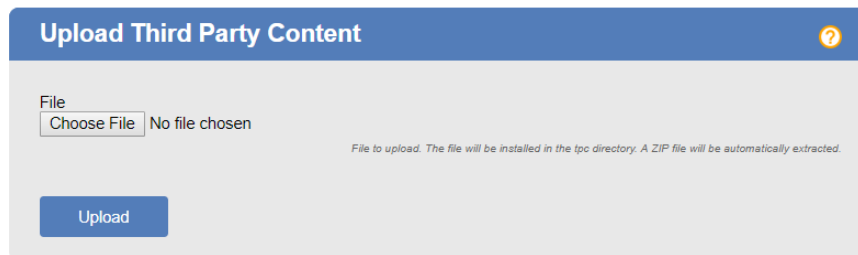
Version 7.0 of the Juniper IVE includes a Hob RDP Java applet, which is launched using a bookmark created for a Terminal Service Resource Profile. Currently, Juniper Networks bookmarks cannot be launched programmatically. Therefore, you cannot use the integrated Hob RDP Java applet in your Leostream environment.

To launch a Java RDP client from the Connection Broker, you must upload the client into the Connection Broker and use the **External viewer** option in the protocol plan, as follows.

1. Download the Java client you plan to use and store it in a location that is accessible to all the Connection Broker's in your cluster.
2. In your Connection Broker, go to the > **System > Maintenance** page.
3. Select the **Upload third party content** option, as shown in the following figure.



- Click **Next**. The following page opens.



- Enter the full path to the Java client you downloaded in step one.



If using the Elusiva Java RDP client, ensure that you sign the client before uploading it into the Connection Broker (see [Signing the Elusiva Open Source Java RDP Client](#)).

- Click **Install**. The file is uploaded into your Connection Broker's Web servers `/tpc` directory. For example, the full file name is:

```
https://cb-address/tpc/filename
```

Where `cb-address` is your Connection Broker hostname or IP address and `filename` is the name of your Java RDP client file.



7. If you have a cluster of Connection Brokers, repeat steps 2 through 6 for each Connection Broker in the cluster.
8. On the **> Configuration > Protocol Plans** page, open the **Edit Protocol Plan** page for the protocol plan to assign to the desktops for users who log in through the SSL VPN.
9. Select **1** from the **Priority** drop-down menu for **External viewer** in the **Web Browser** section.
10. In the **Configuration file** edit field, enter HTML code that launches the Java RDP client. For example, for Elusiva Java RDP, enter the following text.

```
<html>
<head>
  <title>Connection Broker Title</title>
</head>
<body>
  <applet name='rdp' code='com.elusiva.rdp.applet.RdpApplet'
    archive='JavaRDP14-1.1.jar' codebase='tpc' width='30%'
    height='30%'>
    <param name='server' value='{IP}'>
    <param name='port' value='3389'>
    <param name='username' value='{USER}'>
    <param name='password' value='{PLAIN_PASSWORD}'>
    <param name='domain' value='{AUTH_DOMAIN}'>
  </applet>
</body>
</html>
```

For the HobLink JWT client, enter the following text.

```
<HTML>
<HEAD>
  <meta http-equiv="Content-Type" content="text/html">
  <TITLE>Leostream Connection Broker</TITLE>
  <STYLE type="text/css">
    p,h1,h2,h3,h4
    { font-family:Verdana,Arial,sans-serif; }
  </STYLE>
</HEAD>
<BODY background="lib/back.gif">
  <APPLET CODE="hob.hltc.JHLTCap01.class" MAYSCRIPT WIDTH=1
  HEIGHT=1 ARCHIVE="lib/jwtwebJ2.jar,lib/jmf.jar"
  CODEBASE="tpc/HobSoft" ALIGN="baseline">
    <PARAM name="PROFILE" value="PROFILE_NAME">
    <PARAM name="USERID" value="{USER}">
    <PARAM name="PASSWORD" value="{PLAIN_PASSWORD}">
    <PARAM name="DOMAIN" value="{AUTH_DOMAIN}">
    <PARAM name="IPADDRESS" value="{IP}">
    <PARAM name="AUTOCON" value="yes">
    <PARAM name="java_arguments" value="-Dsun.java2d.noddraw=true">
  </APPLET>
</center>
</BODY>
</HTML>
```

In the HobLink JWT client example, the parameter *PROFILE\_NAME* is the name of the HobLink profile file that you uploaded into the Connection Broker. In the previous example, it resides in the HobLink installation directory indicated by the *codebase* ,i.e., *tpc/HobSoft*.

In both of the previous examples, the *codebase* parameter indicates the directory within the Connection Broker virtual appliance where the applet code exists. If you uploaded the client using the **Upload third party content** option, the code is found in the *tpc* directory. If you uploaded the client into the virtual appliance using another method, ensure that you modify the code base appropriately.

11. Ensure that no other protocol in the **Web Browser** section has a **Priority** set to 1.
12. Click **Save** to save the protocol plan.
13. Use this protocol plan in the policies that are assigned to users logging in through the Juniper Networks device.

## Signing the Elusiva Open Source Java RDP Client

You can configure the Juniper SSL VPN device to re-sign Java applets that the device intermediates. In order for the device to re-sign the applet, however, the applet must be signed when it is originally handed to the device.

To sign the Java applet with a self-signed certificate:

1. On a machine that includes a Java 2 SDK, invoke the following `keytool` command to create a self-signed certificate for the Java RDP client. Run this command on a single line.

```
keytool -genkey -keyalg RSA -keysize 1024 -validity 365 -keystore mystore
-storepass ab453r -alias mycert
```

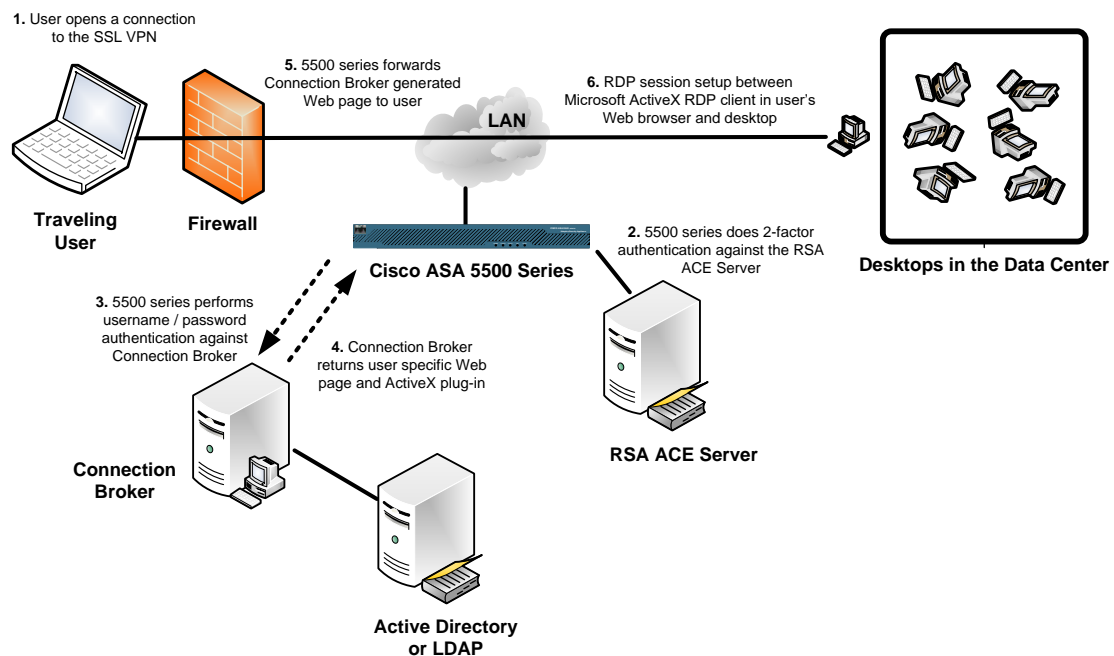
2. When prompted, provide the necessary information to create the certificate.
3. After the certificate is created, invoke the following command to sign the Java RDP client.

```
jarsigner -keystore mystore -storepass ab453r JavaRDP14-1.1.jar mycert
```

If you prefer, you can sign the Java applet with a certificate generated by a certificate authority, such as Verisign. Refer to the [Elusiva Web site](#) for more information.

## Cisco® 55xx SSL VPN Setup

The Leostream Connection Broker integrates with [Cisco ASA 5500 Series](#) clientless (Web) SSL VPN devices. Using a clientless Cisco SSL VPN, you can provide end-users with secure Web-based access to their desktops in the datacenter, as depicted in the following figure.



Configuring your Cisco SSL VPN and Connection Broker to work together consists of the following steps.

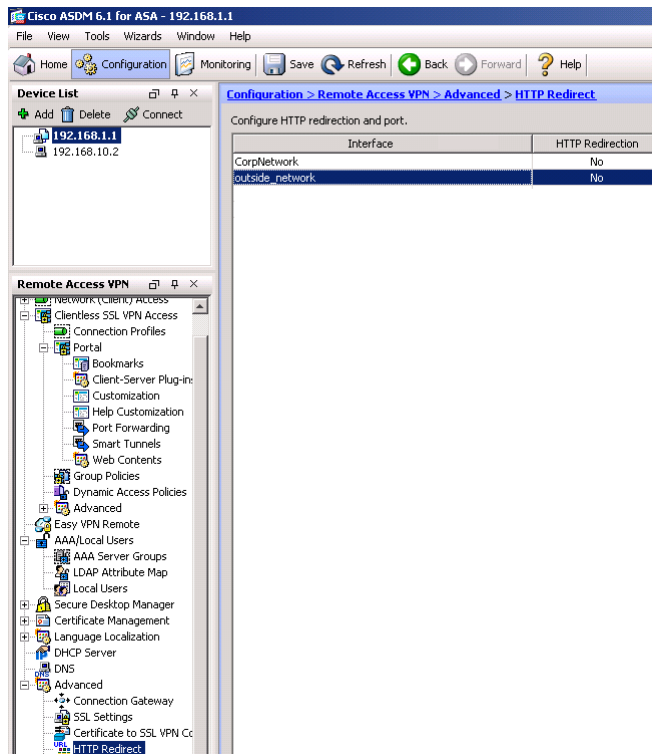
1. Use the Cisco SSL VPN ASDM interface to configure the following:
  - A bookmark for the Connection Broker
  - A policy that applies the bookmark to a group of users
2. Setup the Connection Broker protocol plan to launch an RDP session when accessed through the Cisco SSL VPN.

The following sections describe these steps in more detail. For complete instructions on working with the Cisco SSL VPN ASDM interface, see the [ASDM User Guide](#) available from the Cisco Web site.

## General Cisco SSL VPN Setup

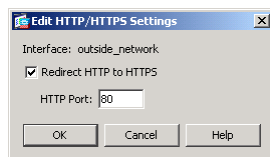
Before you begin integrating your Cisco SSL VPN with your Connection Broker, ensure that you have done the following.

- Install software version 8.0 or higher on the Cisco ASA device.
- Install ASDM version 6.1. The following examples use version ASDM version 6.1.
- Ensure that your inside and outside network connections are properly configured. For example, in the following figure the SSL VPN has an IP address of 192.168.1.1, and has two configured networks. The inside network is named `CorpNetwork`, and the outside network is named `outside_network`.

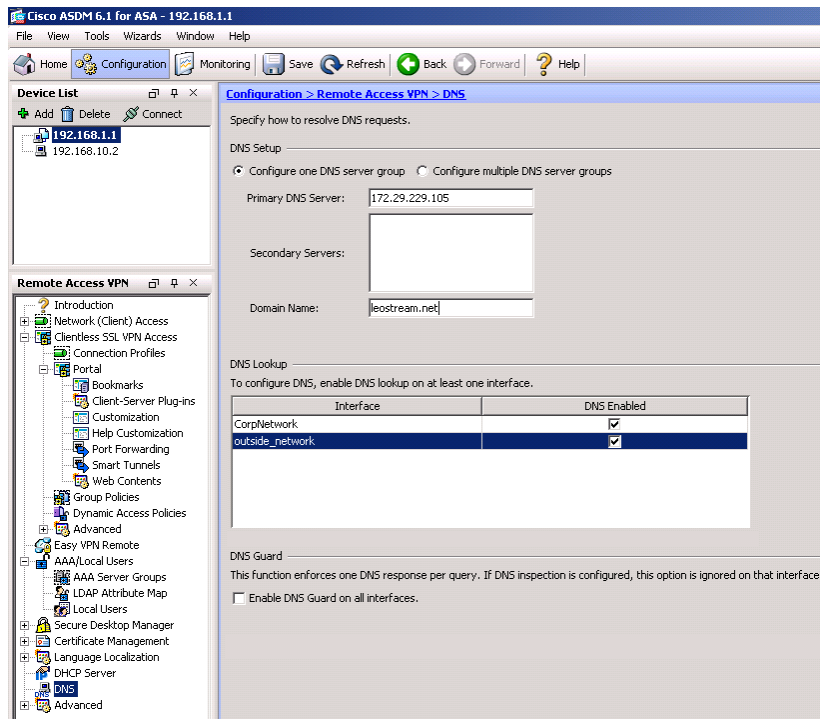


- You can optionally turn on HTTP redirection for the outside network, to allow users to reach the SSL VPN URL using either HTTP or HTTPS. To enable HTTP redirection:

1. Open the **Advanced** node in the **Remote Access VPN** tree.
2. Select **HTTP Redirect**, as shown in the previous figure.
3. Double-click on the entry for your outside network, labeled `outside_network` in the previous figure. The following dialog opens.



4. Check **Redirect HTTP to HTTPS** to turn on redirection.
  5. Enter the **HTTP port** number.
  6. Click **OK**.
- Configure your DNS server on both the inside and outside network, as shown in the following figure.



If the outside network is not aware of your DNS, you may see name resolution errors when users try to connect to their desktops on the internal network.

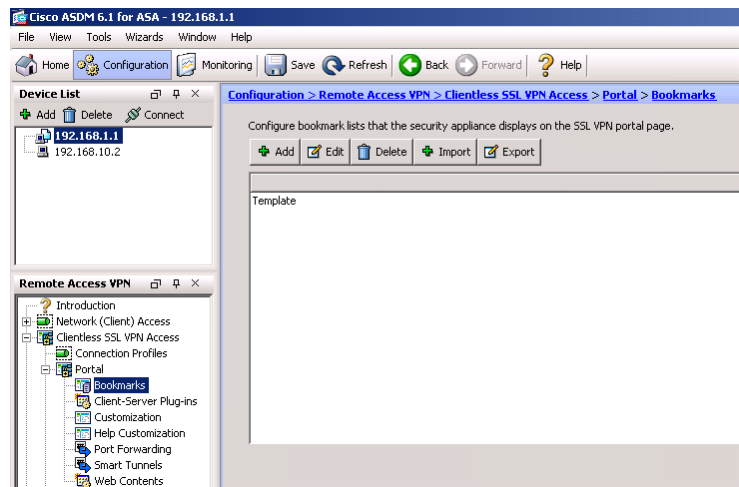
You can set up the Cisco SSL VPN using the ASDM Web interface, the command line, or some combination of both. If you are using the command line interface, see the [Cisco Security Appliance Command Reference](#) for information on the available commands. Note that certain commands can be run only in a certain mode. See the “Using the Command Line Interface” section of the previously reference guide for more information.

The remainder of this section describes how to use the ASDM Web interface to configure your SSL VPN to work with the Connection Broker.

## Setting up the Cisco SSL VPN to Work with the Connection Broker

### Configuring a Connection Broker Bookmark

To create a bookmark for your Connection Broker, navigate to the **Clientless SSL VPN Access > Portal > Bookmarks** node in the **Remote Access VPN** tree, shown in the following figure.



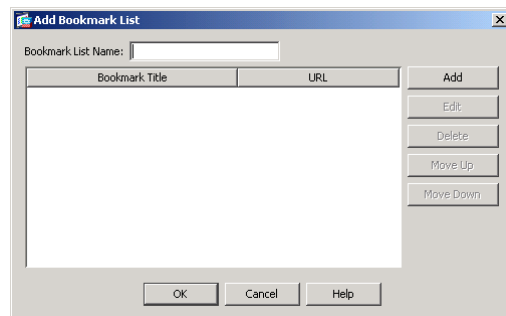
Either add a new bookmark list, or add the Connection Broker bookmark to an existing list.

To edit an existing bookmark list:

1. Select the bookmark list.
2. Click **Edit**.

To create a new bookmark list:

1. Click **Add**. The **Add Bookmark List** dialog, shown in the following figure, opens.



2. In the **Bookmark List Name** edit field, enter a name for this bookmark list, for example `ConnectionBroker`.

Add a bookmark to the new or existing bookmark list, as follows.

1. Click **Add**. The **Add Bookmark** dialog, shown in the following figure, opens.

**Add Bookmark**

Bookmark Title:

URL:  http ://

Optional Settings

Subtitle:

Thumbnail:  -- None --

☐ Enable Smart Tunnel option

☐ Allow the users to bookmark the link

**Advanced Options**

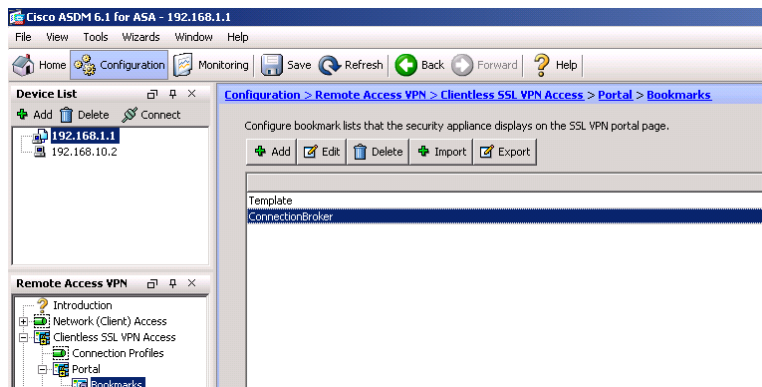
URL Method: ☒ Get ☐ Post

Post Parameters

Name	Value

2. Enter a name for the bookmark into the **Bookmark Title** edit field.
3. Select `https` from the **URL** drop-down menu.
4. Enter your Connection Broker hostname or IP address into the **URL** edit field.
5. The remaining fields can be left at their default values, including selecting the **Get** option for the **URL Method** advanced option. Click **OK** on the **Add Bookmark** page.
6. Click **OK** on the **Bookmark List** dialog.

The new or updated Connection Broker bookmark list appears in the **Clientless SSL VPN Access > Portal > Bookmarks** node, as shown in the following figure.



## Single Sign-On URL Post

Cisco ASA 5500 Series SSL VPN devices support forms-based authentication pass-through. You can



use a **Post** URL method with the appropriate parameters to achieve single sign-on through the Connection Broker bookmark.

To perform single sign-on, the Connection Broker requires a form post with the following format:

```
http://cb.yourcompany.com/index.pl?user=userName&password=pwd&_DATA_FIELDS=
password%2Cuser&_FORM_SUBMIT=1
```

Where:

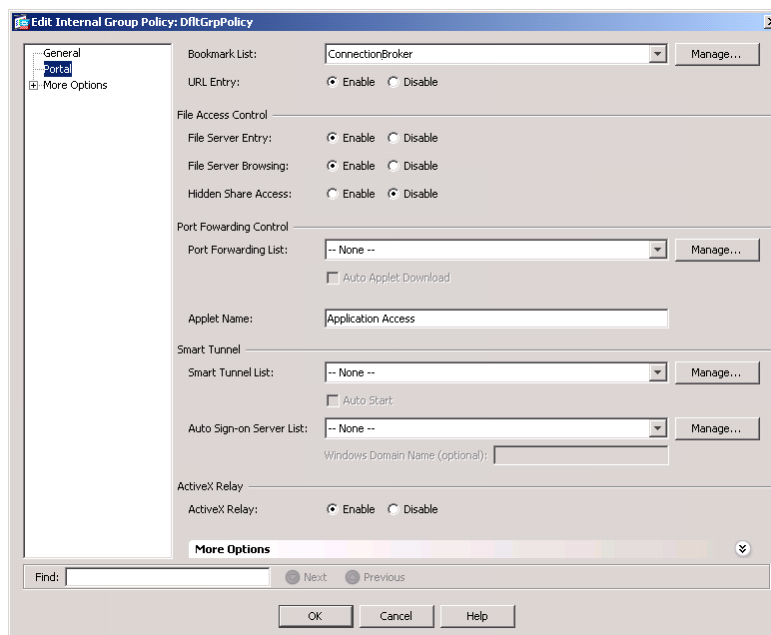
- *cb.yourcompany.com* is your Connection Broker address
- *userName* is the name of the user to log in
- *pwd* is the user's password

Look at the list of [Clientless SSL VPN Macro Substitutions](#) for a list of available parameters to pass through the user name and password.

### Assigning the Bookmark to a Group Policy

To create a group policy with access to your Connection Broker bookmark, navigate to the **Clientless SSL VPN Access > Group Policies** node in the **Remote Access VPN** tree.

Create a new policy, or edit an existing policy, and ensure that the **Bookmark List** assigned to that policy contains your Connection Broker bookmark. For example, in the following figure, the default group policy selects the `ConnectionBroker` bookmark list created in the previous section.



Connection Broker bookmarks do not require port forwarding or smart tunnelling.

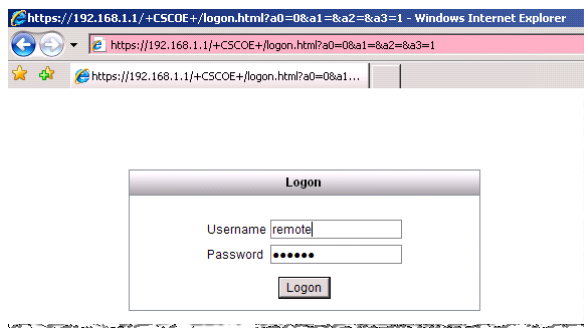
## Assigning Users to a Group Policy

You can define users locally in the SSL VPN device, or set up an LDAP attribute map to use existing Microsoft Active Directory authentication servers. In either case, ensure that your users are correctly assigned to the group policy that contains your Connection Broker bookmark.

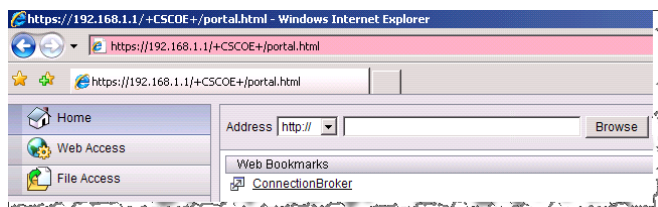
## Logging in Through the Cisco SSL VPN

To log in through the Cisco SSL VPN, point your Web browser to the URL of the clientless SSL VPN appliance.

The **Logon** page opens, for example:



When you click **Logon**, the Cisco SSL VPN passes your username and security token to an RSA server for authentication. If the authentication is successful, your bookmarks page opens, for example:



Click on your Connection Broker bookmark to open the Connection Broker **Sign In** page. This Web page is similar to the normal Connection Broker **Sign In** page, with the addition of the Cisco toolbar, shown on the left.

Log into the Connection Broker and, if necessary, select the desktop you want to launch.

You can return to your bookmarks page by clicking the **Home** button in the Cisco toolbar.

## Using the Cisco Systems VPN Client with Leostream Connect

The Windows version of Leostream Connect can automatically establish a secure tunnel using the Cisco Systems VPN Client, providing seamless and secure single sign-on for end users. Leostream Connect uses `vpngui.exe` to launch the tunnel and then automatically connects the user to their remote desktop using the protocol defined in the **Leostream Connect and Thin Clients Writing to Leostream API** section of the protocol plan.

To enable this feature, check the **Use Cisco VPN client to establish secure tunnel for connections** option at the bottom of the **Leostream Connect and Thin Clients Writing to Leostream API** section of the protocol plan, shown in the following figure.

**Cisco VPN client**

☒ Use Cisco VPN client to establish secure tunnel for connections  
Establish tunnel prior to desktop connection; tear down when connection closes

Profile

[Empty text area for profile configuration]

When the Cisco option is selected, as shown in the previous figure, the **Profiles** edit field appears. Enter a valid profile (the contents of a PCF-file) in the **Profiles** edit field, for example:

```
[main]
Description=Authentication to your domain
Host=enter-cisco-vpn-ip
AuthType=1
GroupName=dev
GroupPwd=
enc_GroupPwd=enter-password
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPPhonebook=
ISPCommand=
Username=enter-username
SaveUserPassword=0
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=0
BackupServer=
EnableMSLogon=1
MSLogonType=0
EnableNat=1
TunnelingMode=0
TcpTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=
SendCertChain=0
PeerTimeout=90
EnableLocalLAN=0
```

After you define your protocol plan, assign it to the pools of desktops used in each policy. When the protocol plan enables login through the Cisco VPN Client, Leostream Connect assumes the VPN client is available.

The user cannot connect to their desktops if the client device does not have an installed Cisco VPN Client. Therefore, you must create separate protocol plans for users that will log in from clients that may or may not have an installed Cisco VPN Client. Use these two protocol plans in different policies and assign the policies to the user based on the user's location.

For example, in the following figure, the user is assigned the `Remote Policy` when they log in from home, but is assigned the `Office Policy` when they log in at the office. The policy `Remote Policy` uses a protocol plan that enables the Cisco VPN Client feature while the policy `Office Policy` disables Cisco VPN Client logins.

**Edit Assignments for Authentication Server "Leostream"**

Domain name  
**leostream.net**

---

**Assigning User Role and Policy**  
In this section you can set up rules to assign Users to Roles and Policies based on their group membership. Optionally use the Order column to re-order the rows.

Order	Group		Client Location		User Role		User Policy
1	Development	+	In Office	→	Domain User	&	Office Policy
2	Development	+	At Home	→	Domain User	&	Remote Policy

For information on creating locations, see Creating Locations in Chapter 13 of the [Connection Broker Administrator's Guide](#). For information on assigning policies to users, see Chapter 14: Assigning User Roles and Policies.

## F5® FirePass® SSL VPN Setup

The F5® FirePass® SSL VPN supports HTTP form-based authentication, as shown in the following figure.

The screenshot shows the 'Users : Authentication' configuration page. At the top, there's a 'For the group:' dropdown set to 'Default'. Below it is the 'Authentication Scheme' section, which states 'Your current authentication scheme is: HTTP form-based authentication.' The configuration fields are as follows:

- Start URL:** `http://172.29.229.122/index.pl`
- Form action:** `http://172.29.229.122/index.pl`
- Form parameter for user name:** `user`
- Form parameter for password:** `password`
- Hidden form parameters and values:** A text area containing:
 

```
_FORM_SUBMIT=1
_DATA_FIELDS=password,user
```

Below the text area, a note states: 'Format is name=value. Each line should contain only one name/value pair. Example: TARGET=http://myhost.com/index.htm SMLOCALE=US-EN'
- Number of redirects to follow:** A numeric input field.
- Successful logon detection:** Three radio button options:
  - ☐ By resulting redirect URL (with a URL input field)
  - ☐ By specific string in result body (with a 'Specific string' input field)
  - ☒ By presence of specific cookie (with a 'Cookie name' input field containing 'uid')

At the bottom, there are 'Save', 'Test', 'User name', and 'Password' fields.

To configure:

1. Enter the Connection Broker address in the **Start URL** and **Form Action** fields
2. Enter **user** as the **Form parameter for user name**
3. Enter **password** as the **Form parameter for password**
4. In the **Hidden form parameters and values** enter:

```
_FORM_SUBMIT=1
_DATA_FIELDS=password,user
```

5. In the **Successful logon detection**, select **By presence of a specific cookie**, and enter a **Cookie name** of **uid**.

You can test the login using the **User name** and **Password** fields at the bottom of the page.