

## Configuring Citrix Web Applications Resource Profile (NSM Procedure)

The Citrix Web template enables you to easily configure Citrix access using the Juniper Networks Citrix Terminal Services proxy, JSAM, or WSAM.

To configure a Citrix Web application resource profile:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Citrix Web application resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Web**.
3. Click the **New** button and the New dialog box appears.
4. Select **Citrix Web Interface/JICA** from the Type list.
5. Enter a unique name and optionally a description for the Citrix resource profile.
6. Add or modify settings as specified in Table 1.
7. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 1: Citrix Web Application Configuration Details**

Options	Your Action
Web Interface (NFuse) URL	<p>Enter the URL of the Web server that hosts your ICA files.</p> <p>Use the format: <i>[protocol://]host[:port][/path]</i>. For instance, enter the URL of an NFuse server, the Web interface for a Citrix Metaframe Presentation Server, or a Web server from which the device can download Citrix Java applets or Citrix cab files.</p>
Citrix implementation type	<p>Specify which type of Citrix implementation you are using in your environment by selecting one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Java ICA Client with Web Interface (NFuse)</b>—Select this option if you have deployed the Citrix Web Interface for MPS (that is, NFuse) to deliver Java ICA clients.</li> <li>■ <b>Java ICA Client without Web Interface (NFuse)</b>—Select this option if you have deployed a generic Web server to deliver Java ICA clients.</li> <li>■ <b>Non-Java ICA Client with Web Interface (NFuse)</b>—Select this option if you have deployed the Citrix Web Interface for MPS (that is, NFuse) to use any of the different clients (Java, ActiveX, local).</li> <li>■ <b>Non-Java ICA Client without Web Interface (NFuse)</b>—(Read only) If you have deployed a non-Java ICA client without the Citrix Web Interface for MPS (that is, NFuse), you cannot create a Citrix resource profile through this template. Instead, click the <b>Client Application Profile</b> link beneath this option.</li> </ul>
Web Interface (NFuse) version	Select the required Citrix version from the drop-down list.

**Table 1: Citrix Web Application Configuration Details** (continued)

Options	Your Action
MetaFrame servers	<p>Specify the Metaframe presentation servers to which you want to control access.</p> <p>Click <b>Add</b>. When specifying servers, you can enter wildcards or IP ranges.</p> <p>The device uses the values that you enter to automatically create a resource policy that enables access to the necessary resources. They include:</p> <ul style="list-style-type: none"> <li>■ If you select either <b>Java ICA Client with or without Web Interface</b>, the device creates a Java ACL resource policy that enables Java applets to connect to the specified Metaframe servers.</li> <li>■ If you select <b>Non-Java ICA Client with Web Interface</b>, and then you select <b>ICA client connects over WSAM or JSAM</b>, the device creates a corresponding SAM resource policy that enables users to access the specified Metaframe servers.</li> <li>■ If you select <b>Non-Java ICA Client with Web Interface</b>, and then you select <b>ICA client connects over CTS</b>, the device creates corresponding Terminal Services and Java resource policies that enable users to access the specified Metaframe servers.</li> </ul>
Sign applets with uploaded code-signing certificate(s)	<p>Enable this check box to re-sign the specified resources using the certificate uploaded after selecting <b>System &gt; Configuration &gt; Certificates &gt; Code-signing Certificates</b> page.</p> <p><b>NOTE:</b> This option is for Java ICA clients only. Enable this option only if you have deployed Citrix using a Java ICA client.</p> <p>When you select this option, the device uses all of the “allow” values that you enter in the resource profile’s Web access control autopolicy to automatically create a corresponding code-signing resource policy. Within this policy, the device uses the specified Web resources to create a list of trusted servers.</p>
Configure access to local resources	<p>Enable this check box to allow users to access local resources such as printers and drives through their Citrix Web interface sessions. Select one of the following options after enabling this option:</p> <ul style="list-style-type: none"> <li>■ Select <b>Connect printers</b> if you want to enable the user to print information from the terminal server to the local printer.</li> <li>■ Select <b>Connect drives</b> if you want to enable the user to copy information from the terminal server to the local client directories.</li> <li>■ Select <b>Connect COM Ports</b> if you want to enable communication between the terminal server and devices on the user’s serial ports.</li> </ul>
Autopolicy: Web Access Control	<p>Enable this check box to create a policy that allows or denies users access to the resource specified in the Web Interface (NFuse) URL box. By default, the device automatically creates a policy for you that enables access to the resource and all of its subdirectories.</p>
Roles	<p>Select the roles to which the Citrix resource profile applies.</p>



**NOTE:** If you selected one of the Web interface options from the Table 1, then update the SSO policy created by the Citrix template. Select the **Autopolicy: Single Sign-on** check box. (Single sign-on autopolicies configure the device to automatically pass device data such as usernames and passwords to the Citrix application. The device automatically adds the most commonly used values to the single sign-on autopolicy based on the Citrix implementation you choose).

---

The selected roles inherit the autopolicies and bookmarks created by the Citrix resource profile. If it is not already enabled, the device also automatically enables the Web option in the Users > User Roles > Select\_Role > General > Overview page of the admin console and the Allow Java Applets option in the Users > User Roles > Select\_Role > Web > Options page of the NSM UI for all of the roles you select.

In the Bookmarks tab, you can optionally modify the default bookmark created by the device and/or create new ones. (By default, the device creates a bookmark to the Web interface (NFuse) URL defined in the Web Interface (NFuse) URL field and displays it to all users assigned to the role specified in the Roles tab).

**Related Topics**

- Configuring a Citrix Listed Application Resource Profile (NSM Procedure)
- Configuring Custom Web Applications Resource Profile (NSM Procedure)
- Configuring a Citrix Terminal Services (Default ICA) Resource Profile (NSM Procedure)

---

Published: 2009-08-20