

## Creating Resource Profiles Using Citrix Web Applications for Citrix 4.6

**NOTE:** If end-user selects "Embedded client" from "Client preferences" when accessing Citrix, then the session will not be launched.

The Citrix Web template enables you to easily configure Citrix access using the Juniper Citrix Terminal Services proxy, JSAM, or WSAM (as explained in [Citrix Templates](#)).

To create a resource profile using the Citrix template:

1. Navigate to the **Users > Resource Profiles > Web Applications/Pages** page in the admin console.
2. Click **New Profile**.
3. Select **Citrix Web Interface/JICA** from the **Type** list.
4. Enter a unique name and optionally a description for the Citrix resource profile.
5. In the **Web Interface (NFuse) URL** field, enter the URL of the web server that hosts your ICA files using the format: [protocol://]host[:port]/[path]. 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 IVE can download Citrix Java applets or Citrix cab files. (The IVE uses the specified URL to define the default bookmark for the Citrix resource profile.) You may enter a directory URL or a file URL. For detailed guidelines on how to format Web resources, see [Defining Base URLs](#).
6. Specify which type of Citrix implementation you are using in your environment by selecting one of the following options:
  - **Java ICA Client with Web Interface (NFuse)**—Select this option if you have deployed the Citrix Web Interface for MPS (i.e., NFuse) to deliver Java ICA clients.
  - **Java ICA Client without Web Interface (NFuse)**—Select this option if you have deployed a generic web server to deliver Java ICA clients.
  - **Non-Java ICA Client with Web Interface (NFuse)**—Select this option if you have deployed the Citrix Web Interface for MPS (i.e., NFuse) to use any of the different clients (Java, ActiveX, local). **(Select this option)**
  - **Non-Java ICA Client without Web Interface (NFuse)**—(Read only) If you have deployed a non-Java ICA client without the Citrix Web Interface for MPS (i.e., NFuse), you cannot create a Citrix resource profile through this template. Instead, click the **client application profile** link beneath this option. The link brings you to the **Client Application Profiles** page, where you can create a SAM resource profile. For instructions, see [Specifying Applications and Servers for WSAM to Secure](#).
7. From the **Web Interface (NFuse) version** list, select which Citrix version you are using. (The IVE uses this value to pre-populate the Forms POST SSO values in your single sign-on autopolicy. For more information, see [Specifying Remote SSO Autopolicy Options](#).) **(Select 4.5 from the Version list)**
8. In the **MetaFrame servers** section, specify the Metaframe Servers to which you want to control access and click **Add**. When specifying servers, you can enter wildcards or IP ranges.

The IVE uses the values that you enter to automatically create a corresponding resource policy that enables access to the necessary resources:

- If you choose **Java ICA Client with|without Web Interface** (above), the IVE creates a corresponding Java ACL resource policy that enables Java applets to connect to the specified Metaframe servers.
  - If you choose **Non-Java ICA Client with Web Interface** (above), and then you select **ICA client connects over WSAM|JSAM** (below), the IVE creates a corresponding SAM resource policy that enables users to access the specified Metaframe servers.
  - If you choose **Non-Java ICA Client with Web Interface** (above), and then you select **ICA client connects over CTS** (below), the IVE creates corresponding Terminal Services and Java resource policies that enable users to access the specified Metaframe servers. **(Select this option)**
9. (Java ICA clients only) If you have deployed Citrix using a Java ICA Client, select the **Sign applets with code-signing certificate** checkbox to resign the specified resources using the certificate uploaded through the **System > Configuration > Certificates > Code-signing Certificates** page of the admin console. (For instructions, see [Using Code-signing Certificates.](#))

When you select this option, the IVE 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 IVE uses the specified Web resources to create a list of trusted servers.

10. (Non-Java ICA clients only) If you have deployed Citrix using a non-Java ICA Client with a Web interface, you must use the Juniper Citrix Terminal Services proxy, Secure Application Manager, or Network Connect to secure traffic to your Metaframe servers instead of the Content Intermediation Engine. To secure traffic through Network Connect, see instructions in [Network Connect.](#)

To secure traffic through the Juniper Citrix Terminal Services proxy or the Secure Application Manager, select one of the following options in the **ICA Client Access** section:

- **ICA client connects over CTS Client**—Select this option to secure your Citrix traffic through the IVE Citrix Terminal Services client (if your users are using Active X clients) or Java rewriting engine (if your users are using Java clients). (When you select this option, the IVE automatically enables the **Terminal Services** option on the **Users > User Roles > Select Role > General > Overview** page of the admin console.)

---

**NOTE:** If you select this option, we recommend that you disable Citrix client downloads through the Citrix Web Interface. Otherwise, users could inadvertently start two different windows downloading two versions of the Citrix client simultaneously—one through the IVE (which automatically attempts to download the Citrix client if one is not present on the user’s computer) and one through the Citrix Web Interface.

- 
- **ICA client connects over WSAM**—Select this option to secure traffic using WSAM. (When you select this option, the IVE automatically enables the **Secure Application Manager** option on the **Users > User Roles > Select Role > General > Overview** page of the admin console.)
  - **ICA client connects over JSAM**—Select this option to secure traffic using JSAM. Then, configure the following options:
    - i. **Number of Servers/Applications**—Enter the lesser of the following two numbers: maximum number of Citrix servers in your environment or the maximum number of published applications that a user can open simultaneously. For instance, if your environment contains one server and five published applications, enter “1” in this field. Or, if your environment contains 20 servers and 10 published applications, enter “10” in this field. The maximum value this field accepts is 99.
    - ii. **Citrix Ports**—Specify the ports on which the Metaframe servers listen.

(When you select the **ICA client connects over JSAM** option, the IVE automatically enables the **Secure Application Manager** option on the **Users > User Roles > Select Role > General > Overview** page of the admin console.)

---

**NOTE:** You cannot enable WSAM and JSAM for the same role. Therefore, if you try to create a Citrix resource profile that uses one of these access mechanisms (for instance, JSAM) and another profile associated with role already uses the other access mechanism (for instance, WSAM), the IVE does not enable the new access mechanism (JSAM) for the role. Also note that you can only use WSAM or JSAM to configure access to one Citrix application per user role.

---

11. If you want to allow users to access local resources such as printers and drives through their Citrix Web Interface sessions, select the **Configure access to local resources** checkbox. Then, select from the following options:
    - Select **Connect printers** if you want to enable the user to print information from the terminal server to his local printer.
    - Select **Connect drives** if you want to enable the user to copy information from the terminal server to his local client directories.
    - Select **Connect COM Ports** if you want to enable communication between the terminal server and devices on the user’s serial ports.
- 

**NOTE:**

- To control access to local resources exclusively through your Citrix Metaframe server settings, de-select the **Configure access to local resources**

checkbox. When you select de-select option, the Metaframe server settings take effect. Or, if you want to selectively override Citrix Metaframe server settings for the bookmark, select the **Configure access to local resources** checkbox and then specify the local resources to which you want to enable or disable access. Note that if you enable access to a local resource through the IVE, however, you still must enable access to it through the Metaframe server as well.

- When you enable local resources through the terminal server, each user can only access his own local resources. For instance, user 1 cannot see user 2's local directories.

- 
12. In the **Autopolicy: Web Access Control** section, create a policy that allows or denies users access to the resource specified in the **Web Interface (NFuse) URL** field. (By default, the IVE automatically creates a policy for you that enables access to the resource and all of its sub-directories.) For more detailed instructions, see [Defining a Web Access Control Autopolicy](#).
  13. If you selected one of the Web interface options in above, update the SSO policy created by the Citrix template in the **Autopolicy: Single Sign on** section. (Single sign-on autopolicies configure the IVE to automatically pass IVE data such as usernames and passwords to the Citrix application. The IVE automatically adds the most commonly used values to the single sign-on autopolicy based on the Citrix implementation you choose.)

At minimum, you need to select the **Autopolicy: Single Sign on** checkbox, double-click the **Value** in the **Domain** column, fill in the appropriate domain, and click the check mark on the right side of the column. For more detailed instructions, see [Specifying Remote SSO Autopolicy Options](#). (Enable the single-sign on checkbox)

Once you select Single sign on, In the post headers section there will be a **Cookie** header that gets populated automatically. Edit that **Cookie** header and update the value of the cookie with "**WINGSession=remoteClientDetected=Auto(ica-Local)&icaClientAvailable=True**".

1. Or, if you selected the non-Web interface option, you may optionally create your own single sign-on autopolicy using instructions in [Defining a Single Sign-On Autopolicy](#).
2. Click **Save and Continue**.
3. In the **Roles** tab, select the roles to which the Citrix resource profile applies and click **Add**.

The selected roles inherit the autopolicies and bookmarks created by the Citrix resource profile. If it is not already enabled, the IVE 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 **Users > User Roles > Select Role > Web > Options** page of the admin console for all of the roles you select.

4. Click **Save Changes**.
5. (Optional) In the **Bookmarks** tab, modify the default bookmark created by the IVE and/or create new ones using instructions in [Defining a Web Bookmark](#). (By default, the IVE

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.)