

Configuring a JSAM Resource Profile (NSM Procedure)

A JSAM resource profile configures JSAM to secure traffic to a client/server application. When you create a JSAM application resource profile, the JSAM client tunnels network traffic generated by the specified client applications to servers in your internal network.

To create a JSAM 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 JSAM application resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > SAM > Client Applications**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in Table 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Configuring JSAM Resource Profile details

Option	Function	Your Action
Settings tab		
Name	Specifies a name for the resource profile.	Enter the name.
Description	Describes the resource profile.	Enter the description.
Type	Allows you to select either JSAM or WSAM to configure resource profile.	Select JSAM option to configure JSAM resource profile.
Settings tab > JSAM > Custom		
Server Hostname or IP	Specifies the hostname or IP address of the remote server.	Enter the hostname or IP address.
Server Port	Specifies the port on which the remote server listens for client connections.	Enter the port.
Localhost IP	Specifies the IP address of the localhost.	Enter the IP address.
Client Port	Specifies the port on which JSAM should listen for client application connections.	Enter the port.

Table 1: Configuring JSAM Resource Profile details (continued)

Option	Function	Your Action
Create an access control policy allowing SAM access to these servers	Allows access to the list of servers specified in the Server Port column	Select the Create an access control policy allowing SAM access to these servers check box to enable this feature.
Allow JSAM to dynamically select an available port if the specified client port is in use	Allows JSAM to select an available port when the client port you specify is taken. The client application must allow you to specify the port number for the connection to use this option.	Select the Allow JSAM to dynamically select an available port if the specified client port is in use check box to enable this option.
Settings > Lotus Notes > Autopolicy: SAM Access Control > Rules tab		
Name	Specifies the name of the policy.	Enter the name.
Resources	Specifies the application server to which this policy applies.	Enter the application resource name.
Action	Allows or denies user access to the resources.	Select either Allow or Deny from the Action drop-down list.
Settings > Microsoft Outlook/Exchange		
New Application Servers	Specifies the hostname for the MS Exchange server.	Enter the hostname
Create an access control policy allowing SAM access to these servers	Enables user to access the server specified in the previous step, application servers (enabled by default).	Select the Create an access control policy allowing SAM access to these servers check box to enable this option.
Settings tab > NetBIOS File Browsing		
New Application Servers	Specifies the fully qualified hostname for your application servers.	Enter the hostname.
Create an access control policy allowing SAM access to these servers	Allows user access the server specified in the previous step, application servers (enabled by default).	Select the Create an access control policy allowing SAM access to these servers check box to enable this option.
Settings > Roles tab		
Roles Selections	Specifies the roles to which the resource profile applies.	Select the role and, then click Add to move the role from the Non-members to the Members list.

- Related Topics**
- Configuring a Citrix Terminal Services (Custom ICA) Resource Profile (NSM Procedure)
 - Configuring a Citrix Terminal Services (Default ICA) Resource Profile (NSM Procedure)