

Configuring Secure Application Manager on a Secure Access Device User Role (NSM Procedure)

The Secure Application Manager (SAM) option provides secure, application-level remote access to enterprise servers from client applications.

To configure SAM option on the user role:

1. In the 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 Secure Application Manager on a user-role access option.
2. Click the **configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. 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: User Role SAM Configuration Details

Option	Function	Your Action
SAM > JSAM Applications tab		
Name	Displays the application name in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the description.
Type	Specifies the applications for which JSAM secures traffic.	Select one of the following option Custom, Citrix NFuse, Lotus Notes, Microsoft Outlook/Exchange, NetBIOS file browsing from the drop-down list.
Type > Custom		
Server Hostname or IP	Specifies the DNS name of the server or the server IP address.	Enter the DNS name or the IP address.
Server Port	Specifies the port on which the remote server listens for client connections.	Enter the port number.

Table 1: User Role SAM Configuration Details (continued)

Option	Function	Your Action
Localhost IP	Specifies a static address for JSAM to listen on loopback address for client requests to network application servers.	Enter a static loopback address.
Client Port	Specifies the port on which JSAM should listen for client application connections.	Enter the port number.
Allow Secure Application Manager to dynamically select an available port if the specified client port is taken	Allows JSAM to select an available port when the client port you specify is taken.	Select the Allow Secure Application Manager to dynamically select an available port if the specified client port is taken check box to enable this feature.
Type > Citrix NFuse		
Maximum Citrix Sessions	Specifies the maximum number of client sessions.	Enter the number.
New Allowed Citrix Ports	Specifies the ports on which the Metaframe servers listen.	Enter the port number.
Type > Microsoft Outlook/Exchange		
New Application Servers	Specifies the application servers for client application connections.	Enter the server name.
Type > NetBIOS file browsing		
New Application Servers	Specifies the application servers for client application connections.	Enter the server name.
SAM > WSAM Applications tab		
Name	Displays the application name in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the description.
Applications	Specifies the applications for which WSAM secures traffic.	Select one of the following option Citrix , Lotus Notes , Microsoft Outlook/Exchange , NetBIOS file browsing or Custom from the Applications drop-down list.
SAM > WSAM Allowed Servers tab		

Table 1: User Role SAM Configuration Details (continued)

Option	Function	Your Action
Name	Displays the application name in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device end-user home page.	Enter the description.
Server	Allows you to specify the server's hostname (the wild cards '*' or '?' are accepted) or an IP/netmask pair.	Enter the server's hostname.
Ports	Allows you to specify multiple ports for a host as separate entries.	Enter the port numbers.
SAM > WSAM Bypass Applications tab		
Name	Displays the application name in the Client Application Sessions area of the Secure Access device in the end-user home page.	Enter the name of the application.
Description	Displays the description in the Client Application Sessions area of the Secure Access device in the end-user home page.	Enter the description.
Application	Specifies the application for which WSAM client does not secure traffic.	Enter the application name.
Path	Allows you to provide an absolute path to the application.	Enter the path.
SAM tab > Options tab		
Auto-launch Secure Application Manager	Enables the Secure Access device to automatically launch the Secure Application Manager when a user signs in. If you do not select this option, users must manually start the Secure Application Manager from the Client Applications Sessions Area of the Secure Access device end-user home page.	Select the Auto-launch Secure Application Manager check box to enable this feature.

Table 1: User Role SAM Configuration Details (continued)

Option	Function	Your Action
Auto-uninstall Secure Application Manager	Enables the Secure Access device to automatically uninstall the Secure Application Manager after user signs off.	Select the Auto-uninstall Secure Application Manager check box to enable this feature.
Prompt for username and password for intranet sites	Allows the Secure Access device to prompt users to enter their sign-in credentials before connecting to sites on their internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer prompts the user for network sign-in credentials whenever the user wants to access an intranet site.	Select the Prompt for username and password for intranet sites check box to enable this feature.
Auto-upgrade Secure Application Manager	Enables the Secure Access device to automatically download the Secure Application Manager to a client machine when the version of Secure Application Manager on the Secure Access device is newer than the version installed on the client.	Select the Auto-upgrade Secure Application Manager check box to enable this feature.
Session start script	Enables the Secure Access device to run a batch, application, or Win32 service file when the WSAM session starts.	Enter the name and path for the file.
Session end script	Enables the Secure Access device to run a batch, application, or Win32 service file when the WSAM session ends.	Enter the name and path for the file.
User can add applications	Enables user to add applications.	Select the User can add applications check box to enable this feature.
Automatic host-mapping	Allows the Secure Application Manager to edit the Windows PC hosts file and replaces entries of Windows application servers with localhost. These entries are changed back to the original data when a user closes the Secure Application Manager.	Select the Automatic host-mapping check box to enable this feature.

Table 1: User Role SAM Configuration Details (continued)

Option	Function	Your Action
Skip web-proxy registry check	Does not have JSAM check a user's registry for a Web proxy. Some users do not have permissions to look at their registries. If JSAM tries to look at their registries, then users see an error that they do not have permission. This option ensures that users do not see this message.	Select the Skip web-proxy registry check check box to enable this feature.
Auto-close JSAM window on sign-out	Enables JSAM to automatically close when a user signs out of the Secure Access device by clicking Sign Out in the Secure Access device browser window. JSAM continues to run if the user simply closes the browser window.	Select the Auto-close JSAM window on sign-out check box to enable this feature.

- Related Topics**
- Configuring Secure Meeting on a Secure Access Device User Role (NSM Procedure)
 - Configuring Terminal Services on a Secure Access Device User Role (NSM Procedure)
 - Configuring WSAM Resource Profile (NSM Procedure)

Published: 2009-08-20