

Configuring WSAM Resource Profile (NSM Procedure)

You can create two types of WSAM resource profiles:

- **WSAM application resource profiles**—These resource profiles configure WSAM to secure traffic to a client/server application. When you create a WSAM application resource profile, the WSAM client intercepts requests from the specified client applications to servers in your internal network.
- **WSAM destination network resource profiles**—These resource profiles configure WSAM to secure traffic to a server. When you create a WSAM destination network resource profile, the WSAM client intercepts requests from processes running on the client that are connecting to the specified internal hosts.

To configure a WSAM 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 user roles.
2. Click the **Configuration tree** tab, and select **Users > Resource Profiles > SAM > Client Applications**. The corresponding workspace appears.
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: Configuring WSAM 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 WSAM.	Select the WSAM option to configure a WSAM resource profile.

Table 1: Configuring WSAM Resource Profile Details (continued)

Option	Function	Your Action
Domain Authentication	Allows integrated Windows applications, such as file sharing, Outlook, and so on to authenticate to the domain controller when the client machine is part of a domain.	Select Domain Authentication to enable this feature. NOTE: Before using this option, you must: <ul style="list-style-type: none"> ■ Specify domain controllers in the WSAM Destination list so that LDAP and Kerberos traffic can be proxied and sent to the device. ■ Configure a WSAM access control list (ACL) policy to allow access to all domain controllers.
Settings tab > Autopolicy:SAM Access Control tab		
Name	Specifies the name of a policy that allows or denies users access to the resource specified in the Base URL box.	Enter the name.
Resource	Specifies the resource name.	Enter the resource name.
Action	Enables you to allow or deny the users access to the server that hosts the specified application.	Select either Allow or Deny from the Action drop-down list.
Settings tab > Settings tab		
Application	Specifies the application from which WSAM intermediates traffic.	Select one of the following options: <ul style="list-style-type: none"> ■ Custom—You must manually enter your custom application’s executable file name (such as telnet.exe). Additionally, you may specify this file’s path and MD5 hash of the executable file (although it is not required that you specify the exact path to the executable). If you enter an MD5 hash value, WSAM verifies that the checksum value of the executable matches this value. If the values do not match, WSAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the IVE. ■ Citrix NFuse—WSAM intermediates traffic from Citrix applications. ■ Lotus Notes—WSAM intermediates traffic from the Lotus Notes fat client application. ■ Microsoft Outlook/Exchange—WSAM intermediates traffic from the Microsoft Outlook exchange application. ■ NetBIOS file browsing—WSAM intercepts NetBIOS name lookups in the TDI drivers on port 137.

Table 1: Configuring WSAM Resource Profile Details (continued)

Option	Function	Your Action
Settings > Roles tab		
Role Selections	Allows you to specify the roles to which the resource profile applies.	Select the role, and click Add .

To configure WSAM destination network 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 WSAM destination network resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > SAM > WSAM Destinations**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings as specified in Table 2.
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 2: Configuring WSAM Destination 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.
Allowed WSAM Servers > Network Destination	Specifies which servers you want to secure using WSAM.	Enter a hostname or IP/netmask pairs. You may include a port.
Create an access control policy	Allows access to the server specified in the Network Destination box (enabled by default).	Select the Create an access control policy check box to enable this option.
Settings > Roles tab		
Role Selections	Specifies the roles to which the resource profile applies.	Select the role, and then click Add .

- Related Topics**
- Configuring a File Rewriting Resource Policy (NSM Procedure)
 - Configuring a JSAM Resource Profile (NSM Procedure)