

Configuring Access Options on an Infranet Controller User Role (NSM Procedure)

To provide users access to protected resources, you can configure agent and agentless access for a user role.

To configure access options on a user role:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure the user- role access option.
3. Click the **Configuration** tab. In the configuration tree, select **Users > User Roles**. The corresponding workspace appears.
4. Add or open a user role. Click either the **Agent** or **Agentless** tab. Add or modify settings as specified in Table 1.
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 1: User Role Access Configuration Details

Option	Function	Your Action
Agent tab		
Install Agent for this role	Allows the user to install the agent for this role.	Select this option to install the agent for this role.
Install Java Agent for this role	Allows the user to download and install the lightweight Java agent for Macintosh or Linux platforms.	Select this option to install Java agent for this role.

Table 1: User Role Access Configuration Details (continued)

Option	Function	Your Action
Enable Host Enforcer	Enables Host Enforcer on the endpoint and sends Host Enforcer policies to Odyssey Access Client for this role (Windows only).	<p>Select this option to enable the Host Enforcer for this role.</p> <p>NOTE:</p> <ul style="list-style-type: none"> ■ By default, after you enable the Host Enforcer option on a role, Odyssey Access Client denies all traffic on the endpoint except for the following allowed types: traffic to and from the Infranet Controller and Infranet Enforcer, WINS, DNS, IPsec, DHCP, ESP, IKE, outgoing TCP traffic, and some ICMP messages (for example, PING from the endpoint to other devices is allowed). Therefore, it's important that you configure Host Enforcer policies to specify the additional types of traffic you want to allow on each endpoint. For example, you must configure Host Enforcer policies to allow any incoming TCP traffic. See "Configuring Infranet Enforcer Resource Access Policies (NSM Procedure)". ■ To avoid blocking all traffic on endpoints and preventing users from accessing all network and Internet resources, we recommend that you configure Host Enforcer policies to allow the specific types of traffic on endpoints before you enable the Host Enforcer option on a role.
Session start script / Session stop script	Executes the script after the start or stop of the OAC session.	<p>Specify the location of the session start scripts / session stop script you want to run on Windows endpoints after Odyssey Access Client connects or disconnects with the Infranet Controller. You can specify a fully qualified path. Scripts can be accessed locally or remotely by means of file share or other permanently available local network resource. You can also use environment variables, such as %USERNAME% in the script path name. For example:</p> <p style="margin-left: 40px;">\\abc\users\%USERNAME%\myscript.bat</p>
odyssey-settings	Specifies the IC Access and Preconfigured Installer settings	Click the odyssey-settings button. See "Configuring OAC Settings for a User Role (NSM Procedure)".
Agentless tab		

Table 1: User Role Access Configuration Details (continued)

Option	Function	Your Action
Enable Agentless Access for this role	Allows users to use agentless access to access protected resources.	Select this option to allow access to endpoints in addition to using Odyssey Access Client on Windows machines. If you don't select the agentless option, the Infranet Controller allows access to protected resources by means of Odyssey Access Client only. NOTE: To configure agentless access, you must also configure a permit infranet auth policy on the Infranet Enforcer to allow access for agentless endpoint platforms. For configuration instructions, see "Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)".
Disable use of AJAX for heartbeats	Disables use of AJAX for heartbeats.	Select this option to disable use of AJAX for heartbeats.

- Related Topics**
- Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure)
 - Configuring Infranet Controller User Roles (NSM Procedure)
 - Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure)

Published: 2009-08-20