

Configuring OAC Settings for a User Role (NSM Procedure)

Each time the user accesses a resource that is protected by the Infranet Controller, the Odyssey Access Client configuration settings you specify will be used.



NOTE: Except for the login name in the profile, all of the other configuration settings you specify on the Infranet Controller overwrite any existing settings on the endpoint if Odyssey Access Client is already installed when the user accesses the Infranet Controller.

To configure odyssey settings:

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**.
4. Add or open a user role and click the **Agent** tab.
5. Click the **odyssey-settings** button and configure the settings as specified in Table 1 on page 1.

There are two tabs under Odyssey Settings. The first tab, IC Access, allows you to configure authentication and connection settings for the Odyssey Access Client. The second tab, Preconfigured Installer, provides an interface that allows you to upload a preconfigured version of Odyssey Access Client that you can deploy to users when they access a role.

6. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 1: OAC Configuration Details

Option	Function	Your Action
IC Access tab		
Name of Profile and Infranet Controller	Displays the hostname or the Infranet Controller URL.	Select the profile name. <ul style="list-style-type: none">■ Use Infranet Controller's host name—Specifies the name of the profile and the Infranet Controller instance in Odyssey Access Client. If the Infranet Controller does not have a hostname configured, the URL for the Infranet Controller or the redirect URL from a captive portal is used instead.■ Use this name:—Specifies the name of the profile and the Infranet Controller instance in Odyssey Access Client.

Table 1: OAC Configuration Details (continued)

Option	Function	Your Action
Profile name	Specifies the profile name. The field is enabled only if the Use this name option is selected in Name of Profile and Infranet Controller box.	Enter the name for the profile and the Infranet Controller instance in Odyssey Access Client.
Require connection to this Infranet Controller	Requires Odyssey Access Client to always attempt to connect to this Infranet Controller and prevents the user from disconnecting from this Infranet Controller. The user also cannot delete the properties of this Infranet Controller from the Odyssey Access Client configuration.	Select this option to require connection to the Infranet Controller.
Login name	Specifies the settings that you want to configure in the Odyssey Access Client profile.	Select the login name. <ul style="list-style-type: none">■ Use qualified Windows login name (domain name).— Configures the login name with the user's Windows domain name and username in the format domain name\username. Use this option if you are using an Active Directory authentication server that requires a domain name in addition to a username for authentication.■ Use unqualified Windows login name— Configures the login name with the user's Windows user name only. Use this option for authentication servers that require a user name only for authentication.■ Prompt for login name using the following Prompt:— Displays a dialog box for the user to enter a name during the initial Odyssey Access Client installation only. The login name is then configured and the user is not prompted again. You can also configure the text string used for the prompt in the dialog box.
Login prompt to be displayed	Specifies the login prompt to be displayed.	Enter the login prompt if you have selected the Prompt for login name using the following Prompt: in the Login name box.
Permit login using password	Enables password authentication for how you want Odyssey Access Client to obtain the user's credentials to sign into the Infranet Controller.	Select to enable password authentication.

Table 1: OAC Configuration Details (continued)

Option	Function	Your Action
Select password type to use	Specifies the password type to use. This field appears only if you select Permit login using password field.	Select the option for how you want Odyssey Access Client to obtain the user's credentials. <ul style="list-style-type: none"><li data-bbox="958 457 1422 695">■ Use Windows password — Enables Odyssey Access Client to automatically authenticate the user to the Infranet Controller by using the user's Windows password. During the initial Odyssey Access Client installation, the user must enter a password once, but then the Odyssey Access Client automatically uses the Windows password after that.<li data-bbox="958 705 1422 966">■ Prompt for password— Enables Odyssey Access Client to prompt the user to enter a password when the user is authenticated the first time after startup. Odyssey Access Client reuses the user's credentials for the duration of the Windows session. If you choose this option and if you have configured single sign-on, Odyssey Access Client does not prompt the user for the password.

Table 1: OAC Configuration Details (continued)

Option	Function	Your Action
Select protocol for outer authentication	Specifies whether the outer authentication protocol for traffic between Odyssey Access Client and the Infranet Controller are Tunneled TLS (TTLS) or Protected EAP (PEAP).	<p>Select the protocol for outer authentication:</p> <ul style="list-style-type: none"> ■ If you select Use EAP-TTLS as outer authentication protocol and you want to use a client certificate as part of the EAP-TTLS authentication, click the eap-ttls button and select Use the user's certificate and perform inner authentication. This option uses EAP-TTLS certificate-based authentication and tunnels password credentials with inner authentication. Note that the most typical use of EAP-TTLS authentication is without a client certificate. ■ If you select Use EAP-PEAP as outer authentication protocol and you want to use a client certificate as part of the EAP-PEAP authentication, click the eap-peap button and select Inner authentication is required. <p>NOTE:</p> <ul style="list-style-type: none"> ■ Only enable the personal client certificate option for either EAP-TTLS or EAPPEAP to use a client certificate if you also configure a realm or role to require a client certificate on the endpoint. If you enable the personal client certificate option and do not configure the realm or role certificate restriction, you will cause unnecessary restrictions on the use of this Odyssey Access Client profile. ■ If you enable the personal client certificate option, the Infranet Controller automatically selects Permit login using my Certificate and Use automatic certificate selection in the Odyssey Access Client profile.
Anonymous name	Enables users to appear to log in anonymously while passing the user's login name (called the inner identity) through an encrypted tunnel. As a result, the user's credentials are secure from eavesdropping and the user's inner identity is protected.	As a general rule enter anonymous in the Anonymous name box, which is the default value. In some cases, you may need to add additional text. For example, if the outer identity is used to route the user's authentication to the proper server, you may be required to use a format such as anonymous@acme.com . If you leave the Anonymous name box blank, Odyssey Access Client passes the user's login name (inner identity) as the outer identity.

Table 1: OAC Configuration Details (continued)

Option	Function	Your Action
Configure wired adapter	Configures a wired adapter to use for wired access to the Infranet Controller at a later time, if the user is accessing the Infranet Controller through a wireless adapter during Odyssey Access Client installation.	Select the option.
Configure wireless adapter	Specifies the network settings you want to configure in Odyssey Access Client for wireless adapters.	Select the wireless adapter option. The Network name (SSID) option, Association mode option and Encryption method option are enabled only if the wireless adapter option is selected.
Network name (SSID)	Specifies the network name.	Enter the network name, which can use up to 32 alphanumeric characters and is case-sensitive. You must enter the name correctly to connect successfully. For example: <MyCorpNet > .
Association mode	Specifies the association mode you want Odyssey Access Client to use when associating to the access point hardware on your network.	Select the association mode: <ul style="list-style-type: none">■ open—Connects to a network through an access point or switch that implements 802.1X authentication. Select this mode if users are not required to use shared mode or Wi-Fi Protected Access (WPA).■ WPA—Connects to a network through an access point that implements WPA.■ WPA2—Connects to a network through an access point that implements WPA2, the second generation of WPA that satisfies 802.11i.

Table 1: OAC Configuration Details (continued)

Option	Function	Your Action
Encryption method	Specifies the encryption method you want Odyssey Access Client to use. The available choices depend on the association mode you selected.	<p>Select the encryption mode:</p> <ul style="list-style-type: none"> ■ none—Uses 802.1X authentication without WEP keys. This option is available only if you configure access point association in open mode. This is a typical setting to use for wireless hotspots. ■ WEP—Uses WEP keys for data encryption. You can select this option if you selected open mode association. Select WEP encryption if the access points in your network require WEP encryption. Odyssey Access Client automatically generates the WEP keys. ■ AES—Uses the advanced encryption standard protocol. Select AES if the access points in your network require WPA or WPA2 association and are configured for AES data encryption. ■ TKIP—Uses the temporal key integrity protocol. Select TKIP if the access points in your network require WPA or WPA2 association and are configured for TKIP data encryption. <p>NOTE: If you select WEP encryption, the Infranet Controller automatically selects the Keys will be generated automatically for data privacy option in the Odyssey Access Client Network properties for the wireless adapter on Odyssey Access Client.</p>
Preconfigured Installer tab		
Current Preconfiguration file	Specifies the name of the zip containing the preconfigured installer file.	Enter the filename.
Preconfiguration file	Specifies the location containing the preconfigured installer file.	Browse to locate the preconfigured installer file.

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