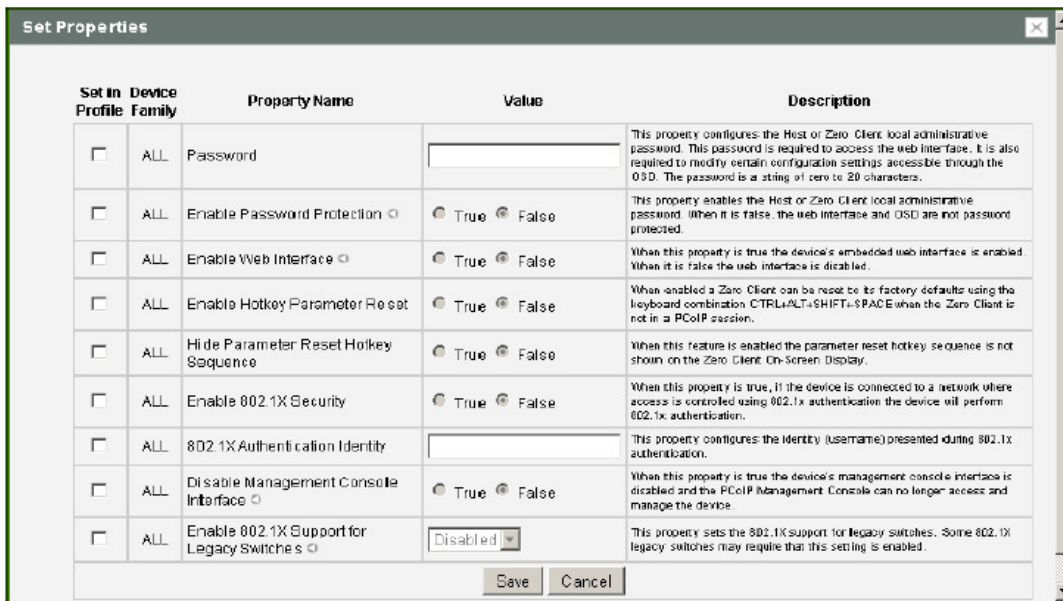


Configuring Security

Security Settings

The settings on this page let you configure a profile with the security parameters to use for hosts and clients.

1. Expand the Security Configuration category
2. Click Edit Properties
3. Select Password and enter a desired password
4. Select Enable Password Protection and set the value to True
5. Select Enable Web Interface and set the value to True



Set In Profile	Device Family	Property Name	Value	Description
<input type="checkbox"/>	ALL	Password	<input type="text"/>	This property configures the Host or Zero Client local administrative password. This password is required to access the web interface. It is also required to modify certain configuration settings accessible through the OSD. The password is a string of zero to 20 characters.
<input type="checkbox"/>	ALL	Enable Password Protection <input type="checkbox"/>	<input checked="" type="radio"/> True <input type="radio"/> False	This property enables the Host or Zero Client local administrative password. When it is false, the web interface and OSD are not password protected.
<input type="checkbox"/>	ALL	Enable Web Interface <input type="checkbox"/>	<input checked="" type="radio"/> True <input type="radio"/> False	When this property is true the device's embedded web interface is enabled. When it is false the web interface is disabled.
<input type="checkbox"/>	ALL	Enable Hotkey Parameter Reset	<input checked="" type="radio"/> True <input type="radio"/> False	When enabled a Zero Client can be reset to its factory defaults using the keyboard combination CTRL+ALT+SHIFT+SPACE when the Zero Client is not in a PCoIP session.
<input type="checkbox"/>	ALL	Hide Parameter Reset Hotkey Sequence	<input checked="" type="radio"/> True <input type="radio"/> False	When this feature is enabled the parameter reset hotkey sequence is not shown on the Zero Client On-Screen Display.
<input type="checkbox"/>	ALL	Enable 802.1X Security	<input checked="" type="radio"/> True <input type="radio"/> False	When this property is true, if the device is connected to a network where access is controlled using 802.1x authentication the device will perform 802.1x authentication.
<input type="checkbox"/>	ALL	802.1X Authentication Identity	<input type="text"/>	This property configures the Identity (username) presented during 802.1x authentication.
<input type="checkbox"/>	ALL	Disable Management Console Interface <input type="checkbox"/>	<input checked="" type="radio"/> True <input type="radio"/> False	When this property is true the device's management console interface is disabled and the PCoIP Management Console can no longer access and manage the device.
<input type="checkbox"/>	ALL	Enable 802.1X Support for Legacy Switches <input type="checkbox"/>	Disabled	This property sets the 802.1X support for legacy switches. Some 802.1X legacy switches may require that this setting is enabled.

Save Cancel

Figure 4-72: MC Security Configuration

Table 4-68: MC Security Configuration Parameters

Parameter	Description
Password	Enter the password for the host or client Administrative Web Interface (AWI). This password is also required to modify certain configuration settings accessible through the client On Screen Display (OSD). This field accepts a string of zero to 20 characters.
Enable Password Protection	When enabled, the host or client AWI password is required. When disabled, the AWI and OSD are not password protected.
Enable Web Interface	When enabled, the host or client can be accessed and managed using the AWI is enabled. When disabled, the device cannot be accessed or managed using the AWI.
Enable Hotkey Parameter Reset	When enabled, the client can be reset to its factory defaults using the keyboard combination Ctrl+Alt+Shift+Space when the client is not in a PCoIP session.
Hide Parameter Reset Hotkey Sequence	When enabled, the reset hotkey sequence is not shown on the client OSD.
Enable 802.1X Security	When enabled, the device will perform 802.1x authentication if it is connected to a network where access is controlled using 802.1x authentication.
802.1X Authentication Identity	Configure the username to present for 802.1x authentication.

OSD Security Settings

The following administrative access security settings for OSD (On-Screen Display) are located on the access page (accessed from the Options> Configuration> Access menu)

- Disable Management Console Interface
- Disable Administrative Web Interface
- Force Password change on next login