

## Configuring Secure Meetings (NSM Procedure)

Unlike other access features, Secure Meeting does not have a resource policy. Instead, you configure system-level settings that apply to all roles for which this feature is enabled. You can:

- Specify session lifetime limits for meetings.
- Enable daylight savings adjustments to scheduled meetings.
- Specify the maximum color depth of meeting presentations.
- Enable automatic email notifications for users who are invited to meetings scheduled through the Secure Access device end user console.
- Define the MySecureMeeting URL.

To configure secure meetings:

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 secure meetings.
2. Click the **Configuration** tab, and select **System > Configuration > Secure Meeting**. The corresponding workspace appears.
3. Add or modify settings as specified in Table 1 on page 1.
4. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modification.

**Table 1: Configuring Secure Meeting Details**

Option	Function	Your Action
Idle Timeout (minutes)	Specifies the number of minutes a meeting session may remain idle before ending.	Enter the time.
Max. Session Length (minutes)	Specifies the number of minutes a meeting session may remain open before ending.	Enter the time.
Enable Upload Logs	Allows non-Secure Access device users to upload meeting logs.	Select <b>Enable Upload Logs</b> to enable this feature.  <b>NOTE:</b> If you select the Upload Logs option, you must also use settings in the <b>System &gt; Log/Monitoring &gt; Client Logs &gt; Settings</b> page of the admin console to enable client-side logging.
Root meeting URL	Allows you to select the meeting URL you want to associate with MySecureMeeting meetings.  <b>NOTE:</b> Meeting URLs are created in the <b>Authentication &gt; Signing In &gt; Sign-In Policies</b> page.	Select the meeting URL.

**Table 1: Configuring Secure Meeting Details** (continued)

Option	Function	Your Action
Meeting name	Specifies the token to append to the meeting URL to uniquely identify this URL.	Select any one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>Username</b>—Appends the user’s Secure Access device username to the meeting URL.</li> <li>■ <b>Sequential room number with prefix</b>—Specifies a string to append to the meeting URL, such as a “meeting”. Numbers will be appended to the string to ensure uniqueness.</li> <li>■ <b>Expression</b>—Appends an expression, such as &lt; <b>userAttr.lname</b> &gt; , to the meeting URL. If the attribute is not valid, username is appended to the meeting URL instead.</li> </ul>
Meeting room number prefix	Allows you to specify a string to append to the meeting URL, such as a “meeting”. Numbers will be appended to the string to ensure uniqueness  For example, <b>meeting_room1</b> , <b>meeting_room2</b> .	Specify a string.
Meeting name expression	Allows you to specify an expression, such as < <b>userAttr.lname</b> > , to the meeting URL. If the attribute is not valid, username is appended to the meeting URL instead.	Specify an expression.
SMTP Server	Allows you to specify the IP address or host name of the SMTP server that can route email traffic from the appliance to the meeting invitees.	Enter the IP address or host name of the SMTP server.
SMTP Login	Allows you to specify a valid login name for the specified SMTP email server (if required by the SMTP server).	Enter a valid login name for the SMTP email server.
SMTP Password (clear text)	Allows you to specify a password for the specified SMTP email server.	Enter the password for the specified SMTP email server.
SMTP Email	Specifies the email address or the address of another administrator that secure meeting uses the specified address as the sender’s email if the email creator does not configure his own email address on the Secure Access device.	Enter the email address or the address of another administrator.
Observe DST schedules of this country	Allows you to specify the country whose daylight savings time rules the Secure Access device should observe. The client uses this setting as a baseline and then adjusts meeting times for individual users as necessary based on browser settings and Secure Access device client-side DST preference settings.	Select a country from the drop down list.

**Table 1: Configuring Secure Meeting Details** (continued)

Option	Function	Your Action
Enable 32-bit (True Color) Presentations	Allows users to present in true color. By default, Secure Meeting presents applications to users using the same color-depth as the presenter's desktop (up to 32-bit color). If you do not select this option and a user presents an application in 32-bit color, however, Secure Meeting changes the image to 16-bit to improve performance.	Select <b>Enable 32-bit (True Color) Presentations</b> to enable this feature.

- Related Topics**
- Configuring Global Security (NSM Procedure)
  - Configuring Sensors (NSM Procedure)

