

Using the API

The API is a set of commands for advanced users who want to automate a Polycom RealPresence Group Series system. You can use the API by connecting a control system or computer RS-232 serial port to a RealPresence Group Series system. You can also use telnet over the LAN to use the API with RealPresence Group Series systems.

Using the API with an RS-232 Interface

If you use an RS-232 interface to send API commands, you must connect and configure the control system or computer and the RealPresence Group Series system for serial communication.

Configuring the RS-232 Interface

If you use the API with a serial connection, make sure that the RS-232 interfaces of the RealPresence Group Series system and your computer are configured appropriately.

To configure the RS-232 settings on your system:

- 1 Go to the web interface and select **Admin Settings > General Settings > Serial Port**.
- 2 Configure the Baud Rate and RS-232 Mode options as follows:

Option	Configure this way on your computer	Configure this way on the RealPresence Group Series system
Baud Rate	Must be the same rate for both devices. Available rates are: • 9600 • 19200 • 38400 • 57600 • 115200	
RS-232 Mode	—	Control

The RS-232 port on the RealPresence Group Series system supports the following modes:

- **Off** Disables the serial port.

Using the API with the Maximum Security Profile Enabled

When configured for the Maximum security profile, API sessions using a LAN Connection (telnet) are not available, and API sessions using an RS-232 port or SSH require you to log on using a valid user ID and password. The system will accept either the local admin account user ID (and associated remote access password) or the local user account user ID (and associated remote access password).

In addition, if Active Directory External Authentication is enabled, then Active Directory account credentials can also be used. In this case, however, the local user account is disabled and so cannot be used. See the *Polycom RealPresence Group Series Administrator Guide* for details on the use of Active Directory External Authentication.

Using the API with a LAN Connection

If you have a computer connected to the LAN, you can send API commands to the RealPresence Group Series system through telnet (port 24) and SSH (port 22).



Note: If your computer is running the Windows 7 operating system, you might need to install the telnet client before starting a telnet session. The telnet client is not installed by default with Microsoft Windows 7 operating systems.

To use the API with a LAN connection:

- 1 On the computer, open a command line interface.
- 2 Start a telnet session using the RealPresence Group Series system IP address and port number that is currently configured for telnet API—for example, `telnet 10.11.12.13 24`.
- 3 Log in, if prompted, using the local admin account's remote access password.

Using the API Controller Code

With their cooperation, Polycom has provided AMX, Crestron, and Extron the complete RealPresence Group Series API for development of their Partner modules. These modules are available and can be obtained from the manufacturer's websites.

Secure API Access

You can access a RealPresence Group Series system using the Secure Shell (SSH) protocol. Secure API access is authenticated for local and Active Directory (AD) accounts.



Note: When a password is empty, SSH will not validate credentials and allow a user to log in. Polycom recommends that you consistently use passwords for secure access.

Enable and Disable Secure API Access

Secure API access using SSH is enabled by default. The `sshenable` API command and **Enable SSH Access** web interface option can be used to enable or disable the feature.

To enable SSH for secure API access, do one of the following:

- In the system web interface, go to **Admin Settings > Security > Global Security > Access** and enable the **Enable SSH Access** setting.
- In an API session, enter `sshenable true`.

To disable SSH for secure API access, do one of the following:

- In the system web interface, select **Admin Settings > Security > Global Security > Access** and disable the **Enable SSH Access** setting.
- In an API session, enter `sshenable false`.



Note: Disabling SSH turns off user authentication. Connections receive an access denied notification only after submitting credentials.

Access the API with SSH

To obtain secure access to the API, you must use an SSH client and connect to the IP address configured for the system on port 22.



Note: The system allows three attempts to enter correct login credentials. The SSH client program closes after the third failed attempt.

To access the API with SSH:

- 1 Enable remote access.
- 2 If necessary, enable external authentication.
- 3 Enable the SSH feature.
- 4 Start an SSH session using the RealPresence Group Series system IP address and port 22.
- 5 When prompted, enter the remote access credentials.

For information on configuring local or AD accounts, refer to the *Polycom RealPresence Group Series Administrator Guide* at support.polycom.com.

Additional API Resources

The following online resources are available for your reference as you use the API.

Technical Support Contact Information

To contact Polycom Technical Support, go to support.polycom.com. This web site provides you with contact information for Polycom technical support. Use this web site when you need help using the API.

System Commands

This chapter describes the API commands for RealPresence Group Series systems.

For an alphabetical list of all the commands, refer to the table of contents for this document. For a list of commands by category, refer to Categorical List of API Commands on page 415.



Note: While every attempt has been made to ensure that the expected results of executing the API commands are accurate and complete, Polycom cannot be responsible for system behaviors and control actions that are not explicitly documented in this publication.

About the API Commands

This section provides details about the descriptions for the API commands.

Definitions

Each API command is defined on one or more reference pages. The definitions are based on terms that are listed in the following table.

Terms	Description
Command Description	Brief statement about the purpose of the command.
Syntax	Format required to execute the command.
Parameter	A list of parameters that are defined for the command.
Description (parameter)	A description of each parameter that is defined for the command.

systemsetting sipusername

Gets or sets the system's SIP name.

Syntax

```
systemsetting sipusername ["name"]  
systemsetting get sipusername
```

Parameter	Description	User Accessible	Additional Restrictions
get	Returns the current setting.		
"name"	Specifies the SIP URI for SIP registration.		

Feedback Examples

- ```
systemsetting sipusername Polycom
returns
systemsetting sipusername Polycom
```
- ```
systemsetting get sipusername  
returns  
systemsetting sipusername Polycom
```

Limitations

None

Comments

None