ADMINISTRATOR AND
INTEGRATOR GUIDE

1.0.0 | November 2016 | 3725-84023-001A

# Polycom® ISDN Gateway

Copyright© 2016, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

**Trademarks** Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.

All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

**End User License Agreement** By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

**Patent Information** The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

**Open Source Software Used in this Product** This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

**Disclaimer** While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

**Limitation of Liability** Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

**Customer Feedback** We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

**Polycom Support** Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

# Contents

**Before You Begin . . . . . 17**
Audience, Purpose, and Required Skills . . . . . 17
Get Help . . . . . 17
Polycom and Partner Resources . . . . . 17
The Polycom Community . . . . . 17

**Getting Started with the Polycom® ISDN Gateway™ . . . . . 18**

**Setup and Initial Configuration . . . . . 19**
Setting Up Your System Hardware . . . . . 19
Position the Polycom ISDN Gateway . . . . . 19
Connecting to the LAN . . . . . 19
Powering On . . . . . 19
Power-On Self Test (POST) . . . . . 20
Indicator Lights . . . . . 20
Assigning an IP Address to the Polycom ISDN Gateway . . . . . 21
Change the Default IP Address . . . . . 22
Assign an IP Address Using RS 232 . . . . . 22
Setup Wizard . . . . . 22

**Manage the Polycom ISDN Gateway Remotely . . . . . 24**
Polycom ISDN Gateway Web Interface . . . . . 24
Access the Web Interface . . . . . 24
Configure the System Name . . . . . 24
Manage System Profiles . . . . . 25
Store a Profile . . . . . 25
Upload a Profile . . . . . 25
Configuring SNMP . . . . . 25
Download MIBs . . . . . 26
Configure SNMP Management . . . . . 26

**Network Settings . . . . . 28**
LAN Status Lights . . . . . 28
Configuring LAN Properties . . . . . 28
Configure IP Address (IPv4) Settings . . . . . 29

Configure IP Address (IPv6) Settings . . . . . 29
Configure LAN Options Settings . . . . . 30
Configure DNS Servers . . . . . 32
Configuring H.323 Settings . . . . . 32
Configure H.323 Settings . . . . . 33
Configure Polycom ISDN Gateway to Use a Gatekeeper . . . . . 33
Configure Network Quality Settings . . . . . 34
Configuring NAT or Firewall Settings . . . . . 36
Configure NAT or Firewall Traversal . . . . . 36
Enable the H.460 NAT Firewall Traversal . . . . . 37
Configure Contact Information . . . . . 37
Configure Location Settings . . . . . 38
Connect Polycom ISDN Gateway to ISDN or Other Networks . . . . . 38
Indicator Lights for BRI, PRI and V.35 . . . . . 45
ISDN and Other Network Interface Settings . . . . . 46
Configure the BRI Network Interface . . . . . 46
Configure the PRI Network Interface . . . . . 47
Configure the Serial V.35/RS-449/RS-530 Network Interface . . . . . 49
Dial Plan Settings . . . . . 50
Prerequisites for the Dial Plan Configuration . . . . . 50
Configure the BRI Dial Plan . . . . . 51
Configure the PRI Dial Plan . . . . . 51
Configure the V.35 Dial Plan . . . . . 51

**Security . . . . . 53**
Security Options and Passwords . . . . . 53
Configure Security Profiles . . . . . 53
Manage System Access . . . . . 54
Login and Credentials . . . . . 55
Configure Remote Access . . . . . 56
Detect Intrusions . . . . . 57
Setting Up Local Accounts . . . . . 57
Configure Password Policies . . . . . 57
Account Lockout . . . . . 58
View Connections to Your System in a Sessions List . . . . . 59
Enable a Whitelist . . . . . 59
Add IP Addresses . . . . . 60
IP Address Format . . . . . 60
IPv4 Address Formats . . . . . 60
IPv6 Address Formats . . . . . 60

Configure Port Lockout . . . . . 61
View the Remote Sessions List . . . . . 61
Certificates and Revocation . . . . . 62
Certificate Validation Settings . . . . . 62
Configure Certificate Usage . . . . . 63
CSRs and Certificate Types . . . . . 63
Create Certificate Signing Requests (CSRs) . . . . . 63
Create a CSR . . . . . 64
Add a Signed Certificate . . . . . 65
View a Signed Certificate . . . . . 66
Certificate Revocation Settings . . . . . 66
Add Certificates and CRLs . . . . . 66
Remove Certificates and CRLs . . . . . 67
Use the OCSP Revocation Method for Certificates . . . . . 67
Delete Certificates and CRLs . . . . . 68
Configure Security Banners . . . . . 68

**Dialing . . . . . 70**
Dialing from a Video Endpoint . . . . . 70

**Polycom ISDN Gateway Software Updates . . . . . 71**
Polycom ISDN Gateway Software Updates . . . . . 71
Update System Software from a Web Server . . . . . 71
Manually Update Software . . . . . 71
Automatically Apply Software Updates . . . . . 72
Update System Software from a USB Storage Device . . . . . 72
Update System Software manually . . . . . 73

**Using the API . . . . . 74**
Using the API with an RS-232 Interface . . . . . 74
Configure the RS-232 Interface . . . . . 74
Start an API Session using an RS-232 Interface . . . . . 75
Using the API with Maximum Security Profile Enabled . . . . . 75
Use the API with a LAN Connection . . . . . 75
Secure API Access . . . . . 76
Enable Secure API Access . . . . . 76
Disable Secure API Access . . . . . 76
Access the API with SSH . . . . . 76
System Commands . . . . . 77
About the API Commands . . . . . 77

Definitions . . . 77
Syntax Conventions . . . 77
Availability of Commands . . . 78
Command Response Syntax . . . 78
Commands that restart the Polycom ISDN Gateway . . . 78
Additional Tips . . . 79
areacode . . . 79
Syntax . . . 79
Feedback Examples . . . 79
Comments . . . 80
bri1enable, bri2enable, bri3enable, bri4enable . . . 80
Syntax . . . 80
Feedback Examples . . . 80
briallenable . . . 80
Syntax . . . 81
Feedback Examples . . . 81
Comments . . . 81
calldetailreport . . . 81
Syntax . . . 81
Feedback Examples . . . 82
Comments . . . 82
callstats . . . 82
Syntax . . . 82
Feedback Examples . . . 82
calldetail . . . 82
Syntax . . . 83
Feedback Examples . . . 83
country . . . 83
Syntax . . . 83
Feedback Examples . . . 83
cts . . . 84
Syntax . . . 84
Feedback Examples . . . 84
Comments . . . 84
daylightsavings . . . 84
Syntax . . . 84
Feedback Examples . . . 85
dcd . . . 85
Syntax . . . 85
Feedback Examples . . . 85

Comments . . . . . 86
dcdfilter . . . . . 86
Syntax . . . . . 86
Feedback Examples . . . . . 86
Comments . . . . . 86
defaultgateway . . . . . 86
Syntax . . . . . 86
Feedback Examples . . . . . 87
Comments . . . . . 87
destunreachabletx . . . . . 87
Syntax . . . . . 87
Feedback Examples . . . . . 88
Comments . . . . . 88
dhcp . . . . . 88
Syntax . . . . . 88
Feedback Examples . . . . . 88
Comments . . . . . 88
dialchannels . . . . . 89
Syntax . . . . . 89
Feedback Examples . . . . . 89
diffservaudio, diffservfecc, diffservvideo . . . . . 89
Syntax . . . . . 89
Feedback Examples . . . . . 90
Comments . . . . . 90
dns . . . . . 90
Syntax . . . . . 90
Feedback Examples . . . . . 90
Comments . . . . . 90
dsr . . . . . 91
Syntax . . . . . 91
Feedback Examples . . . . . 91
Comments . . . . . 91
dsranswer . . . . . 91
Syntax . . . . . 91
Feedback Examples . . . . . 92
dtr . . . . . 92
Syntax . . . . . 92
Feedback Examples . . . . . 92
Comments . . . . . 93
e164ext . . . . . 93

Syntax . . . 93
Feedback Examples . . . 93
Comments . . . 93
enablefirewalltraversal . . . 93
Syntax . . . 93
Feedback Examples . . . 94
enablersvp . . . 94
Syntax . . . 94
Feedback Examples . . . 94
Comments . . . 95
enablesnmp . . . 95
Syntax . . . 95
Feedback Examples . . . 95
Comments . . . 95
gatekeeperip . . . 95
Syntax . . . 95
Feedback Examples . . . 96
getconfiguredipaddress . . . 96
Syntax . . . 96
Feedback Examples . . . 96
Comments . . . 96
h323name . . . 97
Syntax . . . 97
Feedback Examples . . . 97
hostname . . . 97
Syntax . . . 97
Feedback Examples . . . 98
Comments . . . 98
ipaddress . . . 98
Syntax . . . 99
Feedback Examples . . . 99
Comments . . . 99
ipprecaudio, ipprecfecc, ipprecvideo . . . 99
Syntax . . . 99
Feedback Examples . . . 100
Comments . . . 100
ipv6addrmode . . . 100
Syntax . . . 100
Feedback Examples . . . 100
Comments . . . 101

ipv6globaladdress . . . . . 101
Syntax . . . . . 101
Feedback Examples . . . . . 101
Comments . . . . . 101
ipv6defaultgateway . . . . . 101
Syntax . . . . . 101
Feedback Examples . . . . . 102
Comments . . . . . 102
ipv6linklocal . . . . . 102
Syntax . . . . . 102
Feedback Examples . . . . . 102
Comments . . . . . 103
ipv6sitelocal . . . . . 103
Syntax . . . . . 103
Feedback Examples . . . . . 103
Comments . . . . . 103
ipstat . . . . . 103
Syntax . . . . . 103
Feedback Examples . . . . . 104
isdncountrycode . . . . . 104
Syntax . . . . . 104
Feedback Examples . . . . . 104
Comments . . . . . 105
isdndialingprefix . . . . . 105
Syntax . . . . . 105
Feedback Examples . . . . . 105
isdninterface . . . . . 105
Syntax . . . . . 105
Feedback Examples . . . . . 106
Comments . . . . . 106
isdnnum . . . . . 106
Syntax . . . . . 106
Feedback Examples . . . . . 107
Comments . . . . . 107
isdnswitch . . . . . 107
Syntax . . . . . 107
Feedback Examples . . . . . 108
Comments . . . . . 108
lanport . . . . . 108
Syntax . . . . . 108

Feedback Examples . . . 109
Comments . . . 109
mtumode . . . 109
Syntax . . . 110
Feedback Examples . . . 110
mtusize . . . 110
Syntax . . . 110
Feedback Examples . . . 111
natconfig . . . 111
Syntax . . . 111
Feedback Examples . . . 112
ntpmode . . . 112
Syntax . . . 112
Feedback Examples . . . 112
ntpsecondaryserver . . . 113
Syntax . . . 113
Feedback Examples . . . 113
Comments . . . 113
See Also . . . 114
ntpserver . . . 114
Syntax . . . 114
Feedback Examples . . . 114
Comments . . . 114
pricallbycall . . . 114
Syntax . . . 114
Feedback Examples . . . 115
Comments . . . 115
prichannel . . . 115
Syntax . . . 115
Feedback Examples . . . 116
Important PRI Channel Information . . . 116
pridialchannels . . . 117
Syntax . . . 117
Feedback Examples . . . 117
Comments . . . 117
prilinetype . . . 117
Syntax . . . 117
Feedback Examples . . . 118
isdnintlprefix . . . 118
Syntax . . . 118

Feedback Examples . . . . . 118
Comments . . . . . 118
isdnoutsideline . . . . . 118
Syntax . . . . . 119
Feedback Examples . . . . . 119
Comments . . . . . 119
priswitch . . . . . 119
Syntax . . . . . 119
Feedback Examples . . . . . 120
Comments . . . . . 120
reboot . . . . . 120
Syntax . . . . . 120
Feedback Examples . . . . . 120
Comments . . . . . 121
resetsystem . . . . . 121
Syntax . . . . . 121
Feedback Examples . . . . . 121
rs232 mode . . . . . 121
Syntax . . . . . 121
Feedback Examples . . . . . 122
rs366dialing . . . . . 122
Syntax . . . . . 122
Feedback Examples . . . . . 122
Comments . . . . . 122
rt . . . . . 122
Syntax . . . . . 123
Feedback Examples . . . . . 123
Comments . . . . . 123
rts . . . . . 123
Syntax . . . . . 123
Feedback Examples . . . . . 124
Comments . . . . . 124
serialnum . . . . . 124
Syntax . . . . . 124
Feedback Examples . . . . . 124
servervalidatepeercert . . . . . 124
Syntax . . . . . 124
Feedback Examples . . . . . 125
Comments . . . . . 125
clientvalidatepeercert . . . . . 125

Syntax . . . 125
Feedback Examples . . . 125
Comments . . . 125
setpassword . . . 125
Syntax . . . 126
Feedback Examples . . . 126
Comments . . . 126
snmpadmin . . . 126
Syntax . . . 126
Feedback Examples . . . 127
Comments . . . 127
snmpcommunity . . . 127
Syntax . . . 127
Feedback Examples . . . 128
Comments . . . 128
snmplocation . . . 128
Syntax . . . 128
Feedback Examples . . . 128
Comments . . . 129
snmpsystemdescription . . . 129
Syntax . . . 129
Feedback Examples . . . 129
Comments . . . 129
snmpengineid . . . 129
Syntax . . . 129
Feedback examples . . . 130
Comments . . . 130
snmpconsoleip . . . 130
Syntax . . . 131
Feedback examples . . . 131
Comments . . . 131
snmptrapversion . . . 131
Syntax . . . 131
Feedback examples . . . 132
Comments . . . 132
st . . . 132
Syntax . . . 132
Feedback Examples . . . 132
Comments . . . 133
subnetmask . . . 133

Syntax . . . 133
Feedback Examples . . . 133
Comments . . . 133
systemname . . . 133
Syntax . . . 133
Feedback Examples . . . 134
Comments . . . 134
systemsetting telnetenabled . . . 134
Syntax . . . 134
Feedback Examples . . . 134
Comments . . . 135
systemsetting sshenabled . . . 135
Syntax . . . 135
Feedback Examples . . . 135
Comments . . . 135
systemsetting webenabled . . . 135
Syntax . . . 135
Feedback Examples . . . 136
tcpports . . . 136
Syntax . . . 136
Feedback Examples . . . 136
Comments . . . 136
typeofservice . . . 137
Syntax . . . 137
Feedback Examples . . . 137
udpports . . . 137
Syntax . . . 137
Feedback Examples . . . 138
Comments . . . 138
updatefactory . . . 138
Syntax . . . 138
Feedback Examples . . . 138
Comments . . . 138
usefixedports . . . 138
Syntax . . . 138
Feedback Examples . . . 139
usegatekeeper . . . 139
Syntax . . . 139
Feedback Examples . . . 139
v35broadcastmode . . . 140

Syntax . . . . . 140
Feedback Examples . . . . . 140
v35num . . . . . 140
Syntax . . . . . 140
Feedback Examples . . . . . 141
Comments . . . . . 141
v35portsused . . . . . 141
Syntax . . . . . 141
Feedback Examples . . . . . 142
v35prefix . . . . . 142
Syntax . . . . . 142
Feedback Examples . . . . . 143
See Also . . . . . 143
v35profile . . . . . 143
Syntax . . . . . 143
Feedback Examples . . . . . 143
v35suffix . . . . . 144
Syntax . . . . . 144
Feedback Examples . . . . . 144
See Also . . . . . 144
wanipaddress . . . . . 145
Syntax . . . . . 145
Feedback Examples . . . . . 145
Comments . . . . . 145
whitelistenabled . . . . . 145
Syntax . . . . . 145
Feedback Examples . . . . . 146
Comments . . . . . 146
whoami . . . . . 146
Syntax . . . . . 146
Feedback Examples . . . . . 147
Comments . . . . . 147

**Troubleshooting . . . . . 148**
General Troubleshooting . . . . . 148
Unable to perform the software update . . . . . 148
Unable to establish an IP connection . . . . . 148
Unable to Dial a Call Using the Polycom ISDN Gateway . . . . . 149
System Information, Status and Diagnostics Information . . . . . 149
Access the Status Screen . . . . . 149

System Logging . . . . . 150
Configure System Log Management . . . . . 150
Configure System Log Level and Remote Logging . . . . . 151
Download System Log Files . . . . . 152
Download Call Detail Report (CDR) . . . . . 153
Information in the CDR . . . . . 153
Reset the Polycom ISDN Gateway . . . . . 154
Perform a Factory Restore . . . . . 154
Update Factory Image by USB . . . . . 155
Polycom Technical Support . . . . . 155
Locate the System Serial Number . . . . . 155
Locate the Software Version . . . . . 156
Find Your System IP Address . . . . . 156
Locate the H.323 Extension Settings . . . . . 156
Locate the LAN Status . . . . . 156
Locate Diagnostics . . . . . 156
Knowledge Base . . . . . 156
Polycom Solution Support . . . . . 156

**Appendix A: Network Cables . . . . . 157**
CAT 5e LAN Cable . . . . . 157
ISDN Cable . . . . . 158
PRI Pin Assignments . . . . . 158
V.35/RS-449/RS-530 Serial Adapter . . . . . 160
V.35 NIC Cable . . . . . 163
V.35 and RS-366 Serial Cable . . . . . 164
RS-449 and RS-366 Serial Cable . . . . . 167
RS-530 with RS-366 Serial Cable . . . . . 169
Serial Cables . . . . . 171
Straight-Through Cable . . . . . 171
Recommendations for Use . . . . . 171
Null Modem Adapter . . . . . 173
Crossover cable . . . . . 174

**Appendix B: Port Usage . . . . . 175**
Connections to the Polycom ISDN Gateway . . . . . 175

**Appendix C: Back Panel View . . . . . 177**

**Appendix D: Security Profile Settings . . . . . 179**
Maximum Security Profile Default Settings . . . . . 179

High Security Profile Default Settings . . . . . 183
Medium Security Profile Default Settings . . . . . 187
Low Security Profile Default Settings . . . . . 191

# Before You Begin

The *Polycom ISDN Gateway Administrator and Integrator Guide* is for administrators who need to configure and manage the Polycom® ISDN Gateway device.

Please read the related Polycom documentation before you setup and configure the Polycom ISDN Gateway. The following documents are available from support.polycom.com.

- Setup sheet for your hardware
- Release notes
- *Polycom ISDN Gateway Regulatory Notices*, which describes safety and legal considerations for using the Polycom ISDN Gateway device

## Audience, Purpose, and Required Skills

The primary audience for this guide is administrators who need to set up and configure the Polycom ISDN Gateway. This guide provides concepts and general guidance to the system administrator. Polycom expects the administrator to be a mid-grade IT professional who is experienced in system administration.

## Get Help

For more information about installing, configuring, and administering Polycom products, refer to **Documents and Downloads** at support.polycom.com.

For support or service, please contact your Polycom distributor or go to Polycom Support at: support.polycom.com.

### Polycom and Partner Resources

To find all Polycom partner solutions, see Strategic Global Partner Solutions.

### The Polycom Community

The Polycom Community gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

# Getting Started with the Polycom® ISDN Gateway™

With the Polycom® ISDN Gateway™, you can use your Polycom® RealPresence® Group system to make secure video calls over ISDN networks. You can connect with customers, partners, or others inside or outside your organization over ISDN while benefiting from improved video, audio and content experiences with RealPresence Group Series systems.

The Polycom ISDN Gateway connects to your H.320 network, while creating a secure IP connection to the RealPresence Group system. This allows you to keep your RealPresence Group system connected to the IP network, avoiding bringing the H.320 connection right to the video system. Plus, it can be used by up to four RealPresence Group systems as a shared resource. The Polycom ISDN Gateway converts H.320 to H.323 transparently to users, so they can meet over video securely without worry about network protocols or other connectivity details.

The Polycom ISDN Gateway device offers PRI support for calls up to 1920 kbps, which provides full 1080p HD video and content during video calls.

The device can connect H.320 calls in several different ways, including PRI, Quad BRI and V.35. Power over Ethernet support simplifies wiring and cabling, and a detailed web-based administrator portal is available to configure the system, update software, and more. Polycom ISDN Gateway benefits include:

- Unified gateway for multiple protocols, including ISDN PRI, QBRI, and V.35
- Supports up to four calls over a maximum of 8B (BRI) channels
- Supports up to eight calls (video plus audio combined) over a maximum of 23B (T1) / 30B (E1) channels at up to 1080p30 resolution
- Can be used with a single RealPresence Group system, or as a shared resource for up to four systems
- Provides an option to securely connect to B2B and B2C environments using the H.320 protocol for video conferencing
- Converts the H.320 protocol to H.323 protocol and establishes a secure IP connection between the Polycom ISDN Gateway and the RealPresence Group Series systems

# Setup and Initial Configuration

You must set up your device hardware and configure the system software. Refer to the following topics about setup and configuration:

- Setting Up Your System Hardware
- Connecting to the LAN
- Powering On
- Indicator Lights
- Assigning an IP Address to the Polycom ISDN Gateway
- Setup Wizard

## Setting Up Your System Hardware

This manual provides information to supplement the setup sheets provided with your device and its optional components. For more information, refer to the *Polycom ISDN Gateway Setup Sheet* included in the product box, or go to support.polycom.com to download the PDF.

### Position the Polycom ISDN Gateway

The Polycom ISDN Gateway is designed to be placed on a tabletop or in an equipment rack.

#### To position the Polycom ISDN Gateway:

» Do one of the following:

  » To place the device on a table or shelf, attach the self-adhesive feet.

  » To rack mount the device, use mounting hardware to secure the predrilled chassis to the rack.

## Connecting to the LAN

» You must connect the Polycom ISDN Gateway to a LAN (Local Area Network) using LAN ports to access the web interface.

## Powering On

To power on the Polycom ISDN Gateway, you must connect using one of the following methods:

- Directly to the POE port without using a power injector to the LAN port of the unit

- Directly to the non-POE port using a power injector to the LAN port of the unit

For details on these connections, refer to the *Polycom ISDN Gateway Setup Sheet* included in the product box, or go to support.polycom.com to download the PDF.

## Power-On Self Test (POST)

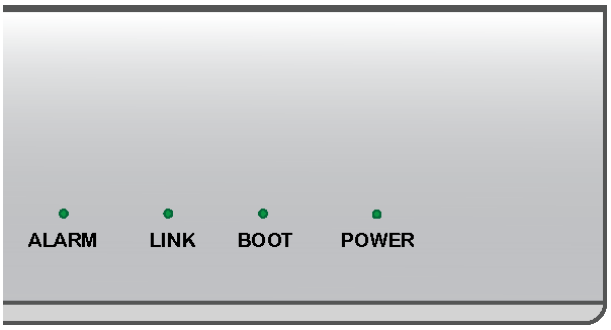
The Polycom ISDN Gateway automatically performs system health checks every time the system starts. If a test fails, the boot LED turns red. Check the system logs by connecting the system to a computer using a serial cable. If any system tests fail, Polycom recommends that you contact Technical Support before using your Polycom ISDN Gateway.

# Indicator Lights

The front of the Polycom ISDN Gateway has the following indicator lights:

- Alarm
- Link
- Boot
- Power

The following figure shows the indicator lights on the front of the Polycom ISDN Gateway.



The indicator lights provide the following information about the device status.

**Alarm**

| Indicator Light | System Status |
|---|---|
| Green light | No alarms |
| Amber light | Minor alarm |
| Red light | Major alarm |

**Link**

| Indicator Light | System Status |
|---|---|
| Green light | Indicates that one ISDN interface and one Ethernet LAN is up. |
| Red light | Indicates that all of the ISDN and/or Ethernet LAN is down. |

**Boot**

| Indicator Light | System Status |
|---|---|
| Off | Boot loader has not started |
| Red light blinking at fast rate | Boot loader has started |
| Red light blinking at slow rate | Kernel has started |
| Green light blinking at slow rate | Copying software package |
| Green light blinking at fast rate | Flashing software package |

**Power**

| Indicator Light | System Status |
|---|---|
| Off | System is powered off |
| Green light | System is powered on |

**Note:** If **Boot**, **Link** and **Alarm** LED are red, this implies that the device is about to reboot.

# Assigning an IP Address to the Polycom ISDN Gateway

Before the Polycom ISDN Gateway can be deployed for use, an administrator must assign an IP address. The IP address is used to display the device's web interface and to access the setup wizard during initial setup.

## Change the Default IP Address

The default IP address of the Polycom ISDN Gateway is 192.168.1.1. You need to configure the Polycom ISDN Gateway using the setup wizard.

### To assign an IP address to the Polycom ISDN Gateway:

1. Configure your computer with a 192.168.1.2 static IP address.
2. Connect the Polycom ISDN Gateway to the computer and open 192.168.1.1 in a web browser.
3. The Out-of-Box configuration wizard will be displayed. Follow the wizard to configure the Polycom ISDN Gateway.

## Assign an IP Address Using RS 232

You can assign an IP address to the Polycom ISDN Gateway using a RS 232 connection.

### To assign an IP address using RS 232:

1. Connect the RS 232 cable to the Polycom ISDN Gateway and a computer.
2. Configure the IP address through the command line interface using the following commands.
   - `ipaddress set <ip-address>`
   - `subnetmask set <subnetmask>`
   - `defaultgateway set <gatewayip>`

**Note:** The API command `defaultgateway` is optional.

## Setup Wizard

The setup wizard walks administrators through the initial setup steps to access the administrative settings in the web interface. The setup wizard is also called the out-of-box (OOB) wizard. When you access the web interface of Polycom ISDN Gateway for the first time, the setup wizard leads you through the minimum configuration steps that are required to setup your device. After the setup is complete, the Polycom ISDN Gateway restarts and the web interface appears.

**Note:** To launch the setup wizard after initial setup, you must factory reset the ISDN Gateway device.

Using the setup wizard, an administrator can configure the following accounts:

- **Admin**: Provides administrators with full access to the Polycom ISDN Gateway. There is no provision to add new or disable/delete existing user accounts. However, the administrator can update the passwords for the existing user accounts. The administrator can also change the configuration settings of the device based on business requirements.
- **Auditor**: Provides read-only access to the auditor accounts. The default password is `auditor`. The admin can change the password at any point of time.

- **User**: Provides restricted rights to user accounts pertaining to the diagnostics only. The default password is `user`. The admin can change the password at any point of time

An administrator can also set an Admin ID and password, which limits user access to the Admin Settings. The default user ID for Admin account is always `admin` and the default admin password is the 14-digit system serial number located on the back of the Polycom ISDN Gateway.

To run the setup wizard or view the configuration screens, do the following:

- Enter the `ipaddress set` command to assign the IP address to the Polycom ISDN Gateway. And then open the IP address assigned to the Polycom ISDN Gateway in a web browser to open the **Setup Wizard**.

After the setup wizard launches, navigate the screens and perform the required steps to configure the Polycom ISDN Gateway.

# Manage the Polycom ISDN Gateway Remotely

You can configure, manage, and monitor the Polycom ISDN Gateway from a computer using the web interface. You can also use SNMP or the API commands.

- The Polycom ISDN Gateway web interface requires only a web browser.
- SNMP requires network management software on your network management station.
- For more information about the API commands, refer to System Commands.

For information about managing the Polycom ISDN Gateway, refer to the following topics:

- Polycom ISDN Gateway Web Interface
- Manage System Profiles

## Polycom ISDN Gateway Web Interface

You can configure, manage, and monitor Polycom ISDN Gateway from a computer using the system web interface.

### Access the Web Interface

To access the Polycom ISDN Gateway web interface, you must configure your browser to allow cookies. For supported browser versions, refer to the *Polycom ISDN Gateway Release Notes*.

#### To access the system using the web interface:

1. In the address bar of your web browser, enter the Polycom ISDN Gateway device's IP address, for example, https://10.11.12.13
2. In the **Login** screen, enter the Admin ID as the user name (default is `admin`), and enter the system serial number as the **Admin Password**.

### Configure the System Name

The system name appears on the **System details** screen. The Polycom ISDN Gateway supports the English language font. Other languages might not display correctly.

**Note**: The first character of a system name must be a letter or a number. Polycom supports double-byte characters for the system name.

### To configure a system name:

1. In the web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **System Name**.
2. In the **System Name** field, enter a name and click **Save**.

# Manage System Profiles

Administrators managing systems that support multiple applications can change system settings using profiles. From the web interface, you can store a Polycom ISDN Gateway profile on a computer as a `.profile` file. There is no restriction in saving the number of profiles. Passwords are not included when you store a profile. The **System behaviors** setting is included in a profile.

**Note**: Polycom recommends only using profiles as the way to back up system settings. Attempting to edit a stored profile or upload a stored profile from one system to a different system can result in instability or unexpected results.

## Store a Profile

You can store a profile using the web interface.

### To store a profile:

1. In the web interface, go to **Utilities > Services > Profile Center**.
2. Click **Download** next to **Current Settings Profile** to download the profile file from the system.
3. Save the file to a location on your computer.

## Upload a Profile

You can upload a profile using the web interface.

### To upload a profile:

1. In the web interface, go to **Utilities > Services > Profile Center**.
2. Next to **Upload Settings Profile**, click **Browse** and then find the profile `.profile` file on your computer.
3. Click **Open** to upload the `.profile` file to your system.

## Configuring SNMP

The Polycom ISDN Gateway supports SNMP (Simple Network Management Protocol) versions 1, 2c, and 3. The Polycom ISDN Gateway sends SNMP reports that indicate the following conditions:

- SNMP alarms for each alert conditions will be received on appropriately configured MIB browser.
- A system powers on.
- Administrator logon is successful or unsuccessful.

## Download MIBs

The MIBs (Management Information Base) are available for download from the web interface.

### To download a Polycom MIB:

1. In the web interface, go to **Admin Settings > Servers > SNMP**.
2. Click **Download MIB**.

## Configure SNMP Management

SNMP management console application resolves SNMP traps and displays human readable text descriptions for those traps. You must install Polycom MIBs on the computer you intend to use as your network management station.

### To configure the Polycom ISDN Gateway for SNMP Management:

1. In the web interface, go to **Admin Settings > Servers > SNMP**.
2. Configure these settings on the SNMP screen, then click **Save**.

| Setting | Description |
|---|---|
| **Enable SNMP** | Allows administrators to manage the system remotely using SNMP |
| **Version1** | Enables the use of the SNMPv1 protocol |
| **Version2c** | Enables the use of the SNMPv2c protocol |
| **Version3** | Enables the use of the SNMPv3 protocol<br>You must select this setting to use the subsequent settings that apply only to SNMPv3. |
| **Read-Only Community** | Specifies the SNMP management community in which you want to enable this system. The default community is `public`.<br>**Note**: Polycom does not support SNMP write operations for configuration and provisioning; the read-only community string is used for both read operations and outgoing SNMP traps. |
| **Contact Name** | Specifies the name of the person responsible for remote management of the system |
| **Location Name** | Specifies the location of the system |
| **System Description** | Specifies the type of video conferencing device |
| **User Name** | Specifies the SNMPv3 User Security Model (USM) account name that is used for SNMPv3 message transactions. The maximum length is 64 characters. |
| **Authentication Algorithm** | Specifies the type of SNMPv3 authentication algorithm used:<br>• SHA<br>• MD5 |
| **Authentication Password** | Specifies the SNMPv3 authentication password. The maximum length is 48 characters. |

| Setting | Description |
|---|---|
| **Privacy Algorithm** | Specifies the type of SNMPv3 cryptography privacy algorithm used:<br>• CFB-AES128<br>• BC-DES |
| **Privacy Password** | Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters. |
| **Engine ID** | Specifies the unique ID of the SNMPv3 engine. This setting might be needed for matching the configuration of an SNMP console application. The Engine ID is automatically generated, but you can create your own ID, as long as it is between 10 and 32 hexadecimal digits. Each group of two hex digits can be separated by a colon character (:) to form a full 8-bit value. A single hex digit delimited on each side with a colon is equivalent to the same hex digit with a leading zero (therefore***:*** is equivalent to***:0f:***).<br>The ID cannot be all zeros or all Fs. |
| **Listening Port** | Specifies the port number SNMP uses to listen for messages. The default listening port is `161`. |
| **Transport Protocol** | Specifies the transport protocol used:<br>• TCP<br>• UDP |
| **Destination Address1**<br>**Destination Address2**<br>**Destination Address3** | Specifies the IP addresses of the computers you intend to use as your network management station and to which SNMP traps are sent.<br>Each address row has four settings:<br>• IP Address (accepts IPv4 and IPv6 addresses, host names, and FQDNs)<br>• Message Type (Trap, Inform)<br>• SNMP protocol version (v1, v2c, v3)<br>• Port (the default is `162`)<br>Disabling the checkbox next to the **Port** setting disables the corresponding Destination Address. |

# Network Settings

Before you begin configuring the network options, you must ensure that your network is ready for video conferencing. Refer to the following topics about preparing your network:

- LAN Status Lights
- Configuring LAN Properties
- Configure LAN Options Settings
- Configuring H.323 Settings

To help determine if your network can support video conferencing, Polycom offers contract high-definition readiness services. For more information, contact your Polycom distributor.

Before you configure the Polycom ISDN Gateway network settings using the system web interface, ensure that you are using a supported browsers with cookies enabled. For a list of supported browsers, refer to the *Polycom ISDN Gateway Release Notes*.

## LAN Status Lights

Each LAN port on the Polycom ISDN Gateway has two lights to indicate connection status and traffic. The following table provides information about the indicator lights and the corresponding system status.

| Indicator Light | System Status |
|---|---|
| Green light is on | Link connection is up |
| Green light is off | Link connection is down |
| Blinking Yellow light | Activity on the link |
| Yellow light is off | No activity |

## Configuring LAN Properties

You can configure the following LAN property settings:

- IPv4 Settings
- IPv6 Settings
- LAN Options
- DNS Servers

## Configure IP Address (IPv4) Settings

You can configure the IPv4 settings for the Polycom ISDN Gateway web interface.

### To configure IPv4 settings:

1. In the web interface, go to **Admin Settings** > **Network** > **LAN Properties**.
2. In the IPv4 section, configure the following IP Address (IPv4) settings.

| Setting | Description |
|---|---|
| **IP Address (IPv4)** | Specifies how the system obtains an IP address. Select one of the following:<br>• **Obtain IP address automatically:** If the Polycom ISDN Gateway gets an IP address from the DHCP server on the LAN<br>• **Enter IP address manually:** If the IP address is not assigned automatically<br>**Note:** Changing this setting causes the system to restart |
| **Your IP Address is** | Displays the IP address automatically assigned to the Polycom ISDN Gateway.<br>If you have selected **Enter IP Address Manually**, enter the IP address here.<br>**Note:** Changing this setting causes the system to restart. |
| **Subnet Mask** | Displays the subnet mask currently assigned to the Polycom ISDN Gateway.<br>If the Polycom ISDN Gateway does not automatically obtain a subnet mask, enter the subnet mask.<br>**Note:** Changing this setting causes the system to restart. |
| **Default Gateway (IPv4)** | Displays the gateway currently assigned to the Polycom ISDN Gateway.<br>If the Polycom ISDN Gateway does not automatically obtain a gateway IP address, enter a gateway IP address.<br>**Note:** Changing this setting causes the system to restart. |

## Configure IP Address (IPv6) Settings

You can configure the IPv6 settings for the Polycom ISDN Gateway in the web interface.

### To configure IPv6 settings:

1. In the web interface, go to **Admin Settings** > **Network** > **LAN Properties**.
2. In the IPv6 section, configure the following IP Address (IPv6) settings.

| Setting | Description |
|---|---|
| **Enable IPv6** | Enables the IPv6 network stack and makes the IPv6 settings available. |
| **IP Address (IPv6)** | Specifies how the system obtains an IP address. Select one of the following:<br>• **Obtain IP address automatically**: If the system gets an IP address from a DHCP server on the LAN<br>• **Enter IP address manually**: If the IP address is not assigned automatically<br>• **Off:** Disables IPv6<br>**Note:** Changing this setting causes the system to restart |

| Setting | Description |
|---|---|
| **Link-Local** | Displays the IPv6 address used for local communication within a subnet. |
| **Site-Local** | Displays the IPv6 address used for communication within the site or organization. |
| **Global Address** | Displays the IPv6 Internet address. |
| **Default Gateway (IPv6)** | Displays the gateway currently assigned to the system.<br>If the system does not automatically obtain a gateway IP address, enter the gateway IP address.<br>**Note:** Changing this setting causes the system to restart. |

## Configure LAN Options Settings

You can configure the LAN Options settings for the Polycom ISDN Gateway in the web interface.

### To configure LAN Options settings:

1. In the web interface, go to **Admin Settings** > **Network** > **LAN Properties**.
2. In the **LAN Options** section, configure the following LAN Options settings.

| Setting | Description |
|---|---|
| **Host Name** | Indicates the name of the system. On IPv4 networks, the system sends the host name to the DHCP server to enable the system to register the hostname with the local DNS server and/or look up the domain where the endpoint is registered (if supported). This function is not supported on IPv6, so do not configure this field if you are using an IPv6 network. Polycom recommends configuring the field to contain the registered host name. |
| **Domain Name** | Displays the domain name currently assigned to the system.<br>If the system does not automatically obtain a domain name, enter domain name. |
| **Autonegotiation** | Specifies whether the system should automatically negotiate the LAN speed and duplex mode according to IEEE 802.3 autonegotiation procedures. If this setting is enabled, the **LAN Speed** and **Duplex Mode** settings become read-only. Polycom recommends that you use autonegotiation to avoid network issues. |
| **LAN Speed POE** | Specifies whether to use 10 Mbps, 100 Mbps, or 1000 Mbps for the LAN speed.<br>**Note**: The speed you choose must be supported by the switch. |
| **Duplex Mode POE** | Specifies the duplex mode to use.<br>**Note**: The Duplex mode you choose must be supported by the switch. |
| **Ignore Redirect Messages** | Enables the Polycom ISDN Gateway to ignore ICMP redirect messages from network routers. A redirect message informs the endpoint to use a different router than the one it is using. |

| Setting | Description |
|---|---|
| **ICMP Transmission Rate Limit (millisec)** | Specifies the minimum number of milliseconds between transmitted ICMP “error” packets. Enter a number between 0 and 60000. The default value of 1000 signifies that the system sends 1 packet per second. If you enter 0, the transmission rate limit is disabled.<br>This setting applies only to “error” ICMP packets. This setting has no effect on “informational” ICMP packets, such as echo requests and replies. |
| **Generate Destination Unreachable Messages** | Generates an ICMP Destination Unreachable message if a packet cannot be delivered to its destination for reasons other than network congestion. |
| **Respond to Broadcast and Multicast Echo Requests** | Sends an ICMP Echo Reply message in response to a broadcast or multicast Echo Request that is not specifically addressed to the Polycom ISDN Gateway. |
| **IPv6 DAD Transmit Count** | Specifies the number of Duplicate Address Detection (DAD) messages to transmit before acquiring an IPv6 address. The Polycom ISDN Gateway sends DAD messages to determine whether the address it needs is already in use.<br>Select whether to transmit 0, 1, 2, or 3 DAD requests for an IPv6 address. |
| **Bridge LAN Ports** | Specifies bridge LAN port for PC/EP. Sets speed and duplex mode for bridge LAN port by enabling bridge LAN port. |
| **Enable EAP/802.1X** | Specifies whether EAP/802.1X network access is enabled.<br>Polycom ISDN Gateway supports the following authentication protocols:<br>• EAP-MD5<br>• EAP-PEAPv0 (MSCHAPv2)<br>• EAP-TTLS<br>• EAP-TLS |
| **Identity** | Specifies the system’s identity used for 802.1X authentication. This setting is available only when EAP/802.1X is enabled. This field must not be blank. |
| **Password** | Specifies the password used for 802.1X authentication. |
| **Enable 802.1p/Q** | Specifies whether VLAN and link layer priorities are enabled. |
| **VLAN ID** | Specifies the identification of the Virtual LAN.This setting is available only when 802.1p/Q is enabled. The value ranges from 1 to 4094. |
| **Video Priority** | Sets the link layer priority of video traffic on the LAN. Video traffic is any RTP traffic consisting of video data and any associated RTCP traffic. This setting is available only when 802.1p/Q is enabled. The value ranges from 0 to 7 but Polycom does not recommend using the values 6 and 7. |

| Setting | Description |
|---|---|
| **Audio Priority** | Sets the priority of audio traffic on the LAN. Audio traffic is any RTP traffic consisting of audio data and any associated RTCP traffic. This setting is available only when 802.1p/Q is enabled. The value ranges from 0 to 7, but Polycom does not recommend using the values 6 and 7. |
| **Control Priority** | Sets the priority of control traffic on the LAN. Control traffic is any traffic consisting of control information associated with a call:<br>• H.323: H.225.0 Call Signaling<br>• H.225.0 RAS<br>• H.245<br>• Far End Camera Control (FECC): Allows participants to control the camera attached to the RealPresence Group Series system<br>This setting is available only when 802.1p/Q is enabled. The value ranges from 0 to 7, but Polycom does not recommend using the values 6 and 7. |

## Configure DNS Servers

You can configure the DNS servers for the Polycom ISDN Gateway in the web interface.

### To configure DNS Servers settings:

1. In the web interface, go to **Admin Settings** > **Network** > **LAN Properties**.
2. In the **DNS Servers** section, configure the following DNS servers settings.

| Setting | Description |
|---|---|
| **DNS Servers** | Displays the DNS servers currently assigned to the system.<br>If the system does not automatically obtain a DNS server address, enter up to four DNS servers here.<br>• **IPv6:** Specify IPv6 DNS server addresses for IP addresses entered manually or obtained automatically (in the case of a system on a hybrid network that obtains IPv4 DNS server addresses through DHCPv4).<br>• **IPv4:** Specify IPv4 DNS server addresses only when the IPv4 address is entered manually. When the IPv4 address is obtained automatically, the DNS server addresses are also obtained automatically.<br>**Note:** Changing this setting causes the system to restart. |

# Configuring H.323 Settings

If your network uses a gatekeeper, the system can automatically register its H.323 name and extension. This allows others to call the system by entering the H.323 name or extension instead of the IP address.

A gatekeeper manages functions such as bandwidth control and admission control. The gatekeeper also handles address translation, which allows users to make calls using static aliases instead of IP addresses that may change each day.

## Configure H.323 Settings

You can configure the H.323 settings in the web interface.

### To configure H.323 settings:

1. In the web interface, go to **Admin Settings** > **Network** > **IP Network** > **H.323**.
2. Configure the following settings on the **H.323 Settings** screen.

| Setting | Description |
|---|---|
| **H.323 Name** | Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper.<br>The **H.323 Name** is the same as the **System Name**, if you have changed the system name. Your organization's dial plan might define the names you can use. |
| **H.323 Extension (E.164)** | Allows users to place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension or prefix that gatekeepers and gateways use to identify this system.<br>Your organization's dial plan might define the extensions you can use. |
| **Enable IP H.323** | Enables the H.323 interface. |
| **Registration Status** | Displays the registration status of the gatekeeper. It displays if the gatekeeper registration is successful or not. This is a read-only field. |

## Configure Polycom ISDN Gateway to Use a Gatekeeper

A gatekeeper manages functions such as bandwidth control and admission control. The gatekeeper also handles address translation, which allows users to make calls using static aliases instead of IP addresses that can change each day.

### To configure the system to use a gatekeeper:

1. In the web interface, go to **Admin Settings > Network > IP Network > H.323**.
2. Configure the following settings.

| Setting | Description |
|---|---|
| **Use Gatekeeper** | Select this setting to use a gatekeeper.<br>• **Off**: Calls do not use a gatekeeper<br>• **Auto**: System attempts to automatically find an available gatekeeper<br>• **Specify**: Calls use the specified gatekeeper. You must select the **Specify** option to enable H.235 Annex D Authentication.<br>When you select a setting other than **Off**, the **Registration Status** is displayed below the **Use Gatekeeper** setting. |
| **Require Authentication** | Enables support for H.235 Annex D Authentication.<br>When H.235 Annex D Authentication is enabled, the H.323 gatekeeper ensures that only trusted H.323 endpoints are allowed to access the gatekeeper.<br>This setting is available when **Use Gatekeeper** is set to **Specify**. |
| **User Name** | When authentication is required, specifies the username for authentication with H.235 Annex D. |
| **Enter Password** | When authentication is required, specifies the password for authentication with H.235 Annex D. |
| **Current Gatekeeper IP Address** | If you chose Off for the **Use Gatekeeper** field, the **Current Gatekeeper IP Address** field is not available.<br>Displays the IP address that the gatekeeper is currently using. |
| **Primary Gatekeeper IP Address** | • If you chose **Off** for the **Use Gatekeepe**r field, the **Primary Gatekeeper IP Addres**s field is not displayed.<br>• If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper's IP address.<br>• If you chose to specify a gatekeeper, enter the gatekeeper's IP address or name (for example, `10.11.12.13` or `gatekeeper.companyname.usa.com`).<br>The primary gatekeeper IP address contains the IPv4 or IPv6 address the system registers with. As part of the gatekeeper registration process, the gatekeeper might return alternate gatekeepers. If communication with the primary gatekeeper is lost, the Polycom ISDN Gateway registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system re-establishes communications with the primary gatekeeper, the Polycom ISDN Gateway unregisters from alternate gatekeeper and re-registers with the primary gatekeeper. |

# Configure Network Quality Settings

You must set the Network Quality options for the way your network handles IP packets during video calls.

### To configure Network Quality settings:

1. In the web interface, go to **Admin Settings > Network > IP Network > Network Quality**.
2. Configure the following settings.

| Setting | Description |
|---|---|
| **Automatically Adjust People/Content Bandwidth** | Specifies whether the system should automatically adjust the bandwidth necessary for the People stream or Content stream depending on the relative complexity of the people video, content video, or both. |
| **Type of Service** | Specifies your service type and lets you choose how to set the priority of IP packets sent to the system for video, audio, FECC, and OA&M:<br>• **IP Precedence**: Represents the priority of IP packets sent to the system. The value can be between 0 and 7.<br>• **DiffServ**: Represents a priority level between 0 and 63 |
| **Video** | Specifies the IP Precedence or Diffserv value for video RTP traffic and associated RTCP traffic. |
| **Audio** | Specifies the IP Precedence or Diffserv value for audio RTP traffic and associated RTCP traffic. |
| **Control** | Specifies the IP Precedence or Diffserv value for control traffic on any of the following channels:<br>• H.323: H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control (FECC, allows the participants to control the camera attached to the RealPresence Group Series system) |
| **OA&M** | Specifies the IP Precedence or Diffserv value for traffic not related to video, audio, or FECC. |
| **Maximum Transmission Unit Size** | Specifies whether to use the default Maximum Transmission Unit (MTU) size for IP calls or select a maximize size. |
| **Maximum Transmission Unit Size Bytes** | Specifies the MTU size, in bytes, used in IP calls. If the video becomes blocky or network errors occur, packets might be too large; decrease the MTU value. If the network is burdened with unnecessary overhead, packets might be too small; increase the MTU value. |
| **Enable RSVP** | Allows the system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP for reservation requests to be made to routers on the connection path. |
| **Enable Lost Packet Recovery** | Allows the system to use LPR (Lost Packet Recovery) if packet loss occurs. |
| **Dynamic Bandwidth** | Specifies whether to let the system automatically find the optimum call rate for a call. |
| **Maximum Transmit Bandwidth** | Specifies the maximum transmit call rate between 64 kbps and the system's maximum line rate. This setting can be useful when the system is connected to the network using an access technology that provides different transmit and receive bandwidth (such as cable or DSL access). |
| **Maximum Receive Bandwidth** | Specifies the maximum receive call rate between 64 kbps and the system's maximum line rate. This setting can be useful when the system is connected to the network using an access technology that provides different transmit and receive bandwidth (such as cable or DSL access). |

# Configuring NAT or Firewall Settings

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with H.323 video conferencing equipment, you must configure the system and the firewall to allow video conferencing traffic to pass in and out of the network.

Network Address Translation (NAT) network environments use private internal IP addresses for devices within the network, while using one external IP address to allow devices on the LAN to communicate with other devices outside the LAN. If your system is connected to a LAN that uses a NAT, you must enter the NAT Public (WAN) Address so that your system can communicate outside the LAN.

## Configure NAT or Firewall Traversal

You can configure the NAT or Firewall settings in the web interface.

### To configure the system to work with a firewall or NAT:

1. In the web interface, go to **Admin Settings** > **Network** > **IP Network** > **Firewall**.
2. Configure the following settings.

| Setting | Description |
|---|---|
| **Fixed Ports** | Allows you to specify whether to define the TCP and UDP ports.<br>• If the firewall is not H.323 compatible, enable this setting. The Polycom ISDN Gateway assigns a range of ports starting with the TCP and UDP ports you specify. The system defaults to a range beginning with port 3230 for both TCP and UDP.<br>**Note**: You must open the corresponding ports in the firewall. For H.323, you must also open the firewall's TCP port 1720<br>• If the firewall is H.323 compatible or the system is not behind a firewall, disable this setting.<br>For IP H.323, you need two TCP and eight UDP ports per connection.<br>**Range of UDP Ports**: The Polycom ISDN Gateway cycles through the available ports from call to call. After the system restarts, the first call begins with the first port number, either 49152 or 3230. Subsequent calls start with the last port used, for example, the first call uses ports 3230 to 3236, the second call uses ports 3236 to 3242, the third call uses ports 3242 through 3248, and so on. |
| **TCP Ports**<br>**UDP Ports** | Specifies the beginning value for the range of TCP and UDP ports used by the system. The system automatically sets the range of ports based on the beginning value you set.<br>**Note:** You must also open the firewall's TCP port 1720 to allow H.323 traffic. |
| **Enable H.460 Firewall Traversal** | Allows the system to use H.460-based firewall traversal for IP calls. For more information, refer to Enable the H.460 NAT Firewall Traversal. |

| Setting | Description |
|---|---|
| **NAT Configuration** | Specifies whether the system should determine the NAT Public WAN Address automatically.<br>• If the system is not behind a NAT or is connected to the IP network through a Virtual Private Network (VPN), select **Off**.<br>• If the system is behind a NAT that allows HTTP traffic, select **Auto**.<br>• If the system is behind a NAT that does not allow HTTP traffic, select **Manual**. |
| **NAT Public (WAN) Address** | Displays the address that callers from outside the LAN use to call your system. If you chose to configure the NAT manually, enter the NAT Public Address here.<br>This field is editable only when **NAT Configuration** is set to **Manual**. |
| **NAT is H.323 Compatible** | Specifies that the system is behind a NAT that is capable of translating H.323 traffic.<br>This field is editable only when **NAT Configuration** is set to **Manual**. |

**Caution:** Systems deployed outside a firewall are potentially vulnerable to unauthorized access. Visit the Polycom Security section of the Knowledge Base at support.polycom.com for timely security information. You can also register to receive periodic email updates and advisories.

## Enable the H.460 NAT Firewall Traversal

You can enable the H.460 NAT firewall traversal in the web interface.

### To use this traversal, configure the Polycom ISDN Gateway and firewalls as follows:

1. Enable firewall traversal on the Polycom ISDN Gateway.
   a. In the web interface, go to **Admin Settings > Network > IP Network > Firewall**.
   b. Select **Enable H.460 Firewall Traversal**.
2. Register the Polycom ISDN Gateway to an external Polycom VBP device that supports the H.460.18 and H.460.19 standards.
3. Ensure that firewalls being traversed allow Polycom ISDN Gateway systems behind them to open outbound TCP and UDP connections.
   - Firewalls with a stricter rule set should allow Polycom ISDN Gateway systems to open at least the following outbound TCP and UDP ports: 1720 (TCP), 14085-15084 (TCP) and 1719 (UDP), 16386-25386 (UDP).
   - Firewalls should permit inbound traffic to TCP and UDP ports that have been opened earlier in the outbound direction.

# Configure Contact Information

You can configure contact information for your Polycom ISDN Gateway so that others know who to call when they need assistance.

### To configure system contact information:

1. In the web interface, go to **Admin Settings** > **General Settings** > **My Information** > **Contact Information**.
2. Configure these settings and click **Save**.

| Setting | Description |
|---|---|
| **Contact Person** | Name of the system administrator |
| **Contact Number** | Phone number for the system administrator |
| **Contact Email** | Email address for the system administrator |
| **Contact Fax** | Fax number for the system administrator |
| **Tech Support** | Name of the person who provides technical support |
| **City** | City where the system administrator is located |
| **State/Province** | State or province where the system administrator is located |
| **Country** | Country where the system administrator is located |

# Configure Location Settings

You can configure Location settings for the Polycom ISDN Gateway in the web interface.

### To configure location settings:

1. In the web interface, go to **Admin Settings** > **General Settings** > **My Information** > **Location**.
2. Configure these settings and click **Save**.

| Setting | Description |
|---|---|
| **Country** | Country where the system is located<br>Changing the country automatically adjusts the country code associated with your system |
| **Country Code** | Country code associated with the country where the system is located |

# Connect Polycom ISDN Gateway to ISDN or Other Networks

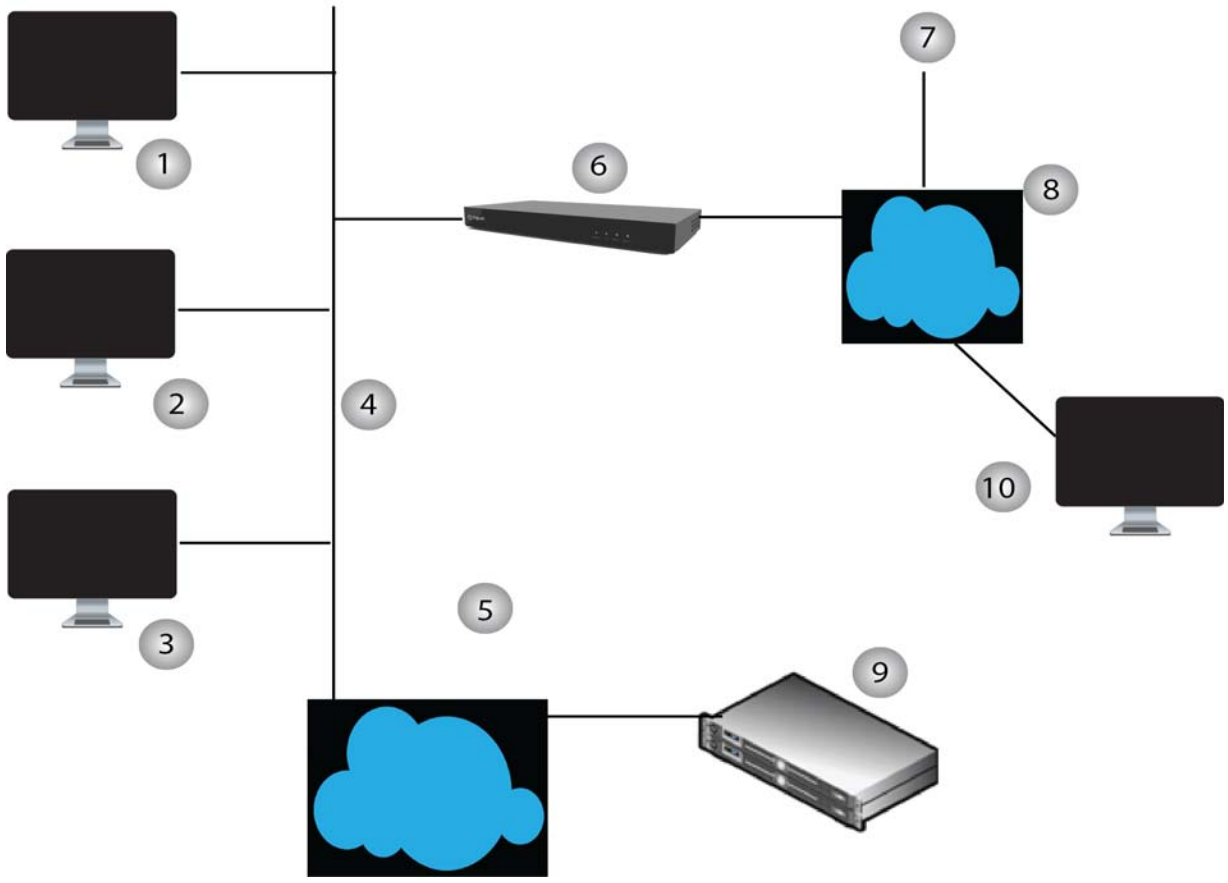
The following network interfaces are available in the Polycom ISDN Gateway:

- BRI: Allows connection to an ISDN network using up to four BRI lines
- PRI: Allows connection to an ISDN T1 or E1 network using a PRI line
- V.35/RS-449/RS-530: Allows connection to third-party network equipment, including encryption equipment and RS-366 terminal adapters and inverse multiplexers

Depending upon your environment, you might need the following network hardware:

| Network Interface | Requirements |
|---|---|
| BRI | • NT-1 device, if the system is connected to a network that provides a U interface. Do not use an NT-1 device if your PBX network provides an S/T interface<br>• Up to four BRI lines that are not shared with other equipment<br>If you connect fewer than four BRI ports on the Polycom ISDN Gateway, connect them in ascending order, starting with port 1. |
| PRI (North America and Japan) | • PBX crossover cable, if required for your PBX<br>• Channel Service Unit (CSU): Not required if you connect the system to a PBX network<br>• PRI line |
| PRI (outside North America and Japan) | • 75 W coaxial adapter, if the network connection is through a 75 W coaxial cable<br>• PBX crossover cable, if required for your PBX<br>• PRI line |
| Serial V.35/RS-449/ RS-530 (with RS-366 dialing) | • Third-party network equipment and cables<br>Contact your network equipment vendor to obtain the appropriate cables for the equipment you connect to this interface. If you use only one cable, connect it to port 1 of the Polycom ISDN Gateway and to the lowest-numbered port of the data communications equipment. |

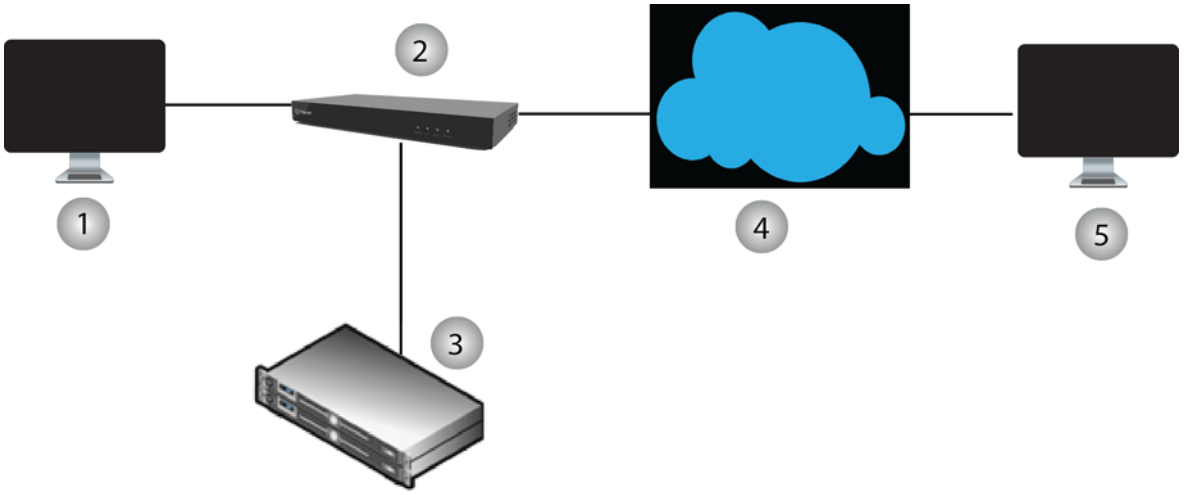
The following diagram shows multiple RealPresence Group Series systems connected to the Polycom ISDN Gateway.




| Ref. Number | Description |
|---|---|
| 1 | H.323 Terminal (RealPresence Group Series system) |
| 2 | H.323 Terminal (RealPresence Group Series system) |
| 3 | H.323 Terminal (RealPresence Group Series system) |
| 4 | LAN |
| 5 | IP Network |
| 6 | Polycom ISDN Gateway |
| 7 | ISDN phone |
| 8 | ISDN |
| 9 | Gatekeeper |
| 10 | H.320 Terminal |

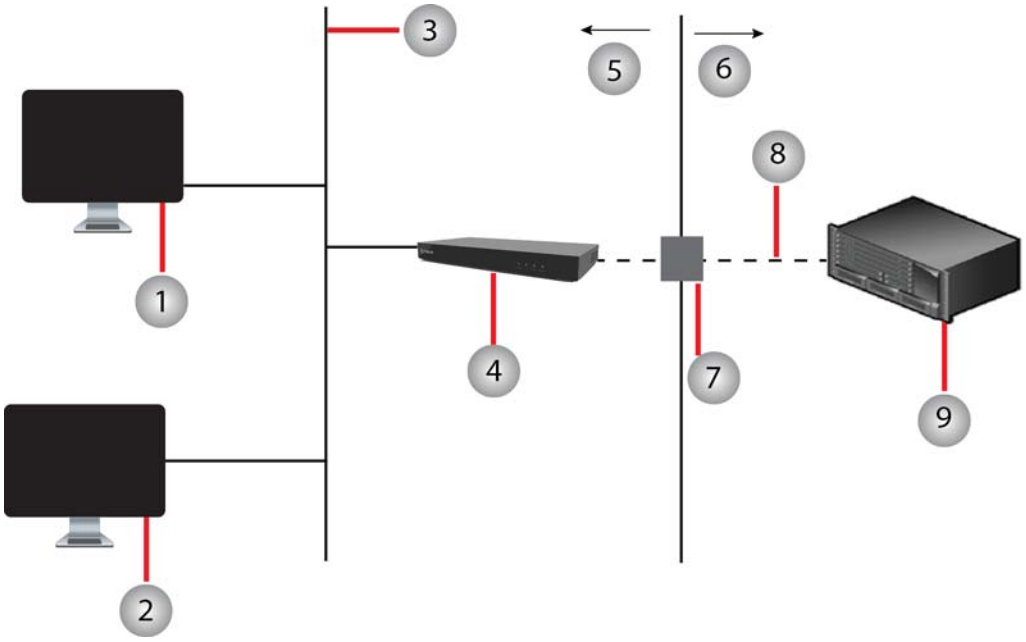
The Polycom ISDN Gateway enables point-to-point communication, for example, video, audio, and data communication between an H.320 (ISDN) terminal and H.323 (IP) terminals.

The following diagram shows point-to-point video conferencing using the Polycom ISDN Gateway.



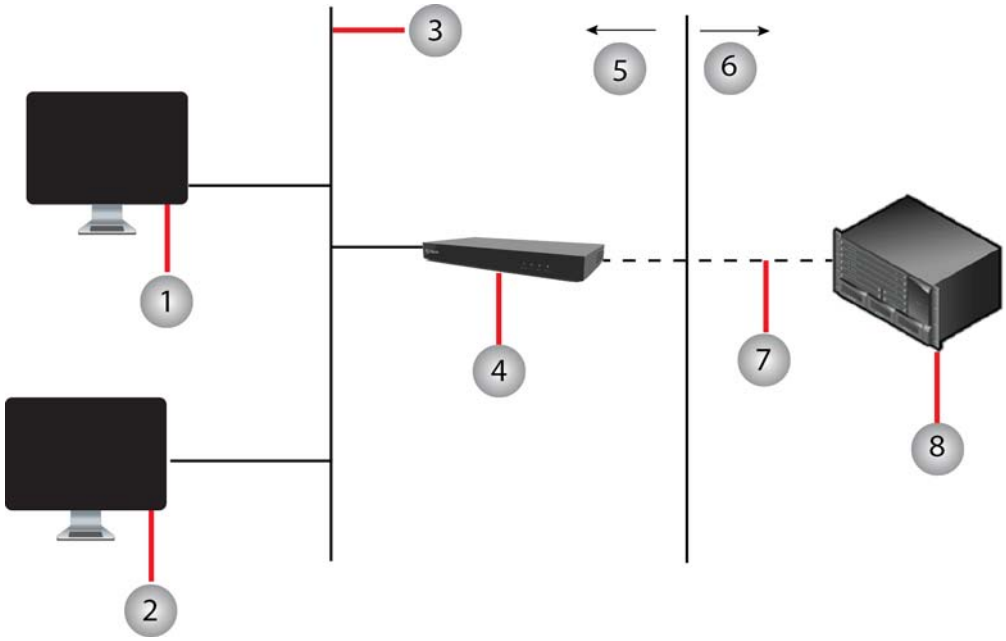

| Ref. Number | Description |
|---|---|
| 1 | H.323 Terminal (RealPresence Group Series system) |
| 2 | Polycom ISDN Gateway |
| 3 | Gatekeeper |
| 4 | ISDN |
| 5 | H.320 Terminal |

**Connecting the Polycom ISDN Gateway using a BRI line**



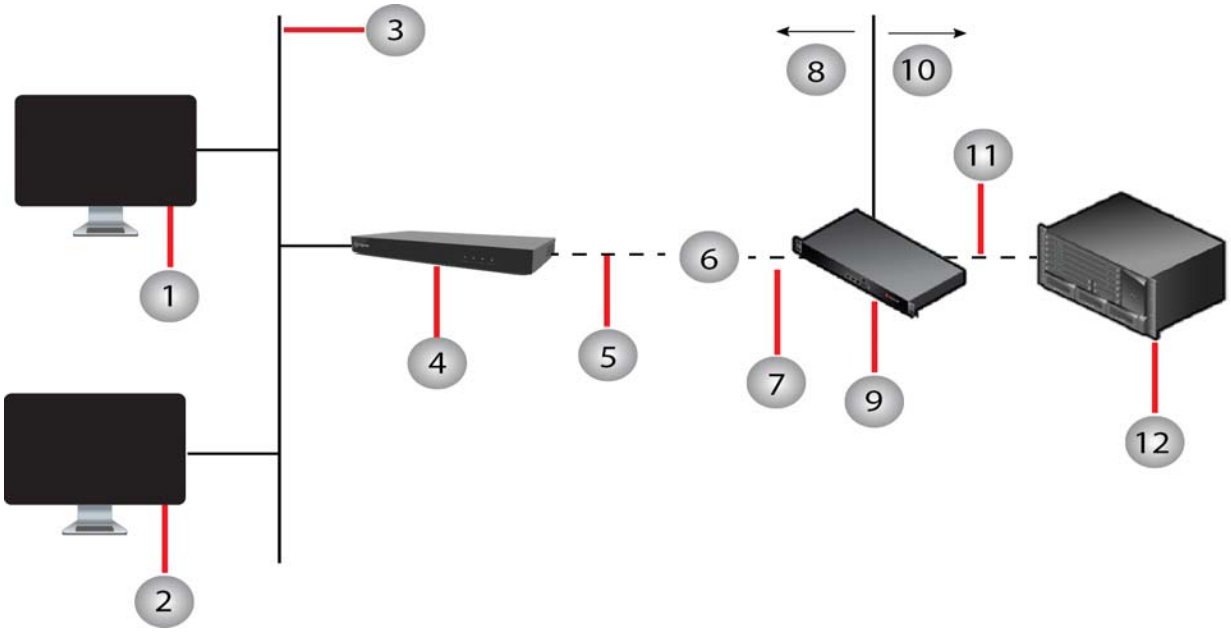
| Ref. Number | Description |
|---|---|
| 1 | H.323 Terminal (RealPresence Group Series system) |
| 2 | H.323 Terminal (RealPresence Group Series system) |
| 3 | IP Network |
| 4 | Polycom ISDN Gateway |
| 5 | Private Network |
| 6 | Public Network |
| 7 | NT1 device |
| 8 | BRI Line |
| 9 | Central Office Switch |

**Connecting the Polycom ISDN Gateway using a PRI line**



| Ref. Number | Description |
|---|---|
| 1 | H.323 Terminal (RealPresence Group Series system) |
| 2 | H.323 Terminal (RealPresence Group Series system) |
| 3 | IP Network |
| 4 | Polycom ISDN Gateway |
| 5 | Private Network |
| 6 | Public Network |
| 7 | PRI T1/E1 |
| 8 | Central Office Switch |

**Connecting Polycom ISDN Gateway Using V.35**




| Ref. Number | Description |
|---|---|
| 1 | H.323 Terminal (RealPresence Group Series system) |
| 2 | H.323 Terminal (RealPresence Group Series system) |
| 3 | IP Network |
| 4 | Polycom ISDN Gateway |
| 5 | DTE |

| Ref. Number | Description |
|---|---|
| 6 | V.35 |
| 7 | DCE |
| 8 | Private Network |
| 9 | V 8X MUX |
| 10 | Public Network |
| 11 | PRI/BRI |
| 12 | Central Office Switch |

## Indicator Lights for BRI, PRI and V.35

The following figure shows the indicator lights on the rear of the Polycom ISDN Gateway.

The indicator lights on the back of the Polycom ISDN Gateway device provide the following information about the interface status:

### Quad BRI Network Interface Status Lights

| Interface Light State | Description |
|---|---|
| Green light off | BRI is disabled |
| Green light is on | BRI is enabled and interface is up |
| Yellow light is off | No alarm |
| Yellow light is on | Loss of signal |

### PRI Network Interface Status Lights

| Interface Light State | Description |
|---|---|
| Green light off | PRI is disabled |
| Green light is on | PRI is enabled and interface is up |
| Yellow light is off | No alarm |
| Yellow light is on | Loss of signal |

### Serial V.35/RS-449/RS-530 Network Interface Status Lights

| Interface Light State | Description |
|---|---|
| Green light | V.35 interface is up |
| Blinking Green light | Data is being transferred |
| Red light | Alarm is on or no connection |

## ISDN and Other Network Interface Settings

You can configure network interface settings for the corresponding ISDN interfaces.

**Note:** You can configure only one network interface (BRI, PRI, or V.35) to be operational at any one time.

### Configure the BRI Network Interface

You can configure the settings for the BRI network interface in the web interface.

#### To configure the BRI network interface settings:

1. In the web interface, go to **Admin Settings > Network > ISDN Configuration**.
2. Select **BRI** from ISDN Configuration drop down menu and click **Save**.

   If any other ISDN interface is selected, click on **Click Here** beside **To Change the interface** to change the ISDN interface.

   You can change to a different ISDN interface in **ISDN Configuration** page. To change an ISDN interface, click on **Click Here** beside **To Change the interface**.

   Note that changing this setting causes the system to restart.
3. Configure the following settings for the BRI interface:

| Setting | Description |
|---|---|
| **Number of ISDN Channels to Dial in Parallel** | Specifies how many channels to dial at one time.<br>You can specify up to eight channels for BRI. If you experience network problems, decrease the number. |
| **Outside Line Dialing Prefix** | Specifies the ISDN dialing prefix used to call outside the network. |
| **Numbering Plan** | Select the appropriate numbering plan for your location, if it differs from the default. |
| **ISDN Voice Algorithm** | Specifies which voice algorithm (**aLaw** or **uLaw**) is used for ISDN voice calls.<br>Do not change this setting unless you experience audio issues in all ISDN voice calls. |
| **ISDN Switch Protocols** | Specifies the protocol used by your network's switch. |

| Setting | Description |
|---|---|
| **Auto BRI Configuration** | Allows the NI-1 or NI-2 switch to automatically configure the directory numbers and Service Profile Identifiers (SPID).<br>This setting is only available if you have selected the NI-1 or NI-2 switch protocol. |
| **Country,**<br>**Country Code** | Displays the location of the system based on the country and the country code you have selected. To specify the system's location, go to **System** > **Admin Settings** > **General Settings** > **Location**. The system automatically sets the country code when you specify the country. |
| **Area Code** | Specifies the area code for this system's location. |
| **Directory Numbers** | Specifies the numbers assigned to the B1 and B2 channels for each BRI line.<br>The two numbers for a line may be the same or different, depending on the switch protocol in use. |
| **Enable** | Specifies whether to enable the associated ISDN line. If you selected Standard ETSI Euro-ISDN protocol, you must enable all BRI lines that you expect to be active, and you must not enable lines that are not connected.<br>You may want to disable a particular line if there are problems with the line that generate continuous error messages. |
| **Dial plan** | Specifies an ISDN number to IP address mapping used by the Polycom ISDN Gateway to route an ISDN initiated call to a RealPresence Group Series system (IP endpoint). |

4 If you have configured the ISDN switch protocol to be AT&T 5ESS Multipoint, NI-1, NI-2, or Nortel DMS-100, and enter the ISDN BRI SPIDs provided by your service provider.

After you enter the SPIDs, the system verifies them. If the system is unable to verify the SPIDs, ensure that the system is connected and the ISDN numbers you entered are correct. If you do not have the SPIDs from your service provider, you can click **Start to Auto Detect SPIDs**.

## Configure the PRI Network Interface

You can configure settings for the PRI network interface in the web interface.

**Note the following points about the fractional PRI:**

- Assigned channels must begin with channel 1, and the channel numbers must be consecutive
- A D channel must be provided
- Outbound call bandwidth must not exceed the available bandwidth

### To configure the PRI network interface settings:

1 In the web interface, go to **Admin Settings** > **Network** > **ISDN Configuration**.

2 Select **PRI** from ISDN Configuration drop down menu and click **Save.**

You can change to a different ISDN interface in **ISDN Configuration** page. To change an ISDN interface, click on **Click Here** beside **To Change the interface**.

Note that changing this setting causes the system to restart.

3 Configure the following settings for the PRI interface.

| Setting | Description |
|---|---|
| **Area Code** | Specifies the area code for this system's location. |
| **PRI Video Number** | Specifies the ISDN number assigned to this system. |
| **Outside Line Dialing Prefix** | Specifies the ISDN dialing prefix used to call outside the network. |
| **BONDING:**<br>**Calling Endpoint Uses the Original ISDN Number** | Specifies the use of a bonding standard. Incoming bonded calls use the original number received to connect all remaining lines required for the call. |
| **Switch Protocol** | Specifies the Network switch protocol. The available choices are determined by the system's country settings.<br>This setting is read-only for PRI E1, configurable for PRI T1.<br>Your ISDN service provider can tell you which protocol your network uses. If you later change the **Country** setting, the PRI switch protocols available may also change, and you may be prompted to configure a different PRI switch protocol. |
| **Numbering Plan** | Select the appropriate numbering plan for your location, if it differs from the default. |
| **International Dialing Prefix** | Specify the dialing prefix needed for international calls. |
| **Call-by-Call** | Specifies a code that the system sends to the telephone company switch to request a special service, if such a code is required.<br>Consult your telephone service provider to determine the proper call-by-call value. |
| **Number of ISDN Channels to Dial in Parallel** | Specifies how many channels to dial at one time.<br>You can specify up to 12 channels. If you experience network problems, decrease the number.<br>Set this value to 1 for serial dialing. Serial dialing is not recommended unless you have trouble connecting calls using parallel dialing. |
| **PRI Line Type** | Specifies the PRI line type. Upon selecting the line as E1, you need to set the switch protocol as NET5/CTR4. If you change the switch protocol, the system reboots. |
| **Line Termination PRI E1 only** | Displays read-only information about the system and its configuration. |
| **Number of Active Channels** | Displays read-only information about the system and its configuration. Number of active channels for PRI T1 is 23, and for PRI E1 is 30. |
| **Dial plan** | Specifies an ISDN number to IP address mapping used by the Polycom ISDN Gateway to route an ISDN initiated call to a RealPresence Group Series system (IP endpoint). |

4 To activate or deactivate a channel, click the channel indicator and then click **Update**. Active channels are represented by a green icon and inactive channels are represented by a gray icon.

**Caution:** Ensure that channels are activated and deactivated only by a knowledgeable network professional so that the system operates properly and can dial at the desired rates.

## Configure the Serial V.35/RS-449/RS-530 Network Interface

You can configure settings for the V.35 network interface in the web interface.

### To configure the V.35/RS-449/RS-530 network interface settings:

1. In the web interface, go to **Admin Settings > Network > ISDN Configuration**.
2. Select **V.35** from ISDN Configuration drop down menu and click **Save.**

   You can change to a different ISDN interface in ISDN Configuration page. To change an ISDN interface, click on **Click Here** beside **To Change the interface.**

   Note that changing this setting causes the system to restart.
3. Configure the following settings for V.35 interface:

| Setting | Description |
|---|---|
| **Enable V.35/RS-449/RS-530** | Allows the system to connect to a terminal adapter using a V.35, RS-449, or RS-530 connection. |
| **V.35 Ports Used** | Specifies whether one or two lines are connected. |
| **RS-366 Dialing** | Allows users to dial calls from this system.<br>Clear this setting if this is a dedicated connection or if another device is used for dialing calls. |
| **Area Code**<br>**Port 1**<br>**Port 2** | Specifies the area code and number or numbers that other sites dial to reach this system.<br>If this is a dedicated connection, leave these fields blank. |
| **ST** | Allows you to specify the signaling required by the external device connected to the system. Specify normal or inverted, as appropriate. In most cases, normal signaling is appropriate. |
| **RT** | |
| **RTS** | |
| **CTS** | If your system is connected to Ascend equipment, you may need to set CTS to **Ignore**. |
| **DSR** | |
| **DTR** | |
| **DCD** | |
| **Answer on DSR** | Specifies that the system should begin the call when it detects a DSR signal. |
| **Delayed DCD Hangup** | Specifies how long the system waits to end the call after a DCD signal is lost (for example, during a call through satellite). |
| **DTR Pulse Duration (secs)** | Specifies how long the DTR signal goes low after the far site hangs up. When the pulse is too short, the call may not clear. The recommended pulse duration is three seconds. If your system is connected to ADTRAN equipment, you may need to adjust DTR pulse duration. |
| **Trigger Call on H.320 Data** | Specifies whether the call starts when H.320 data is detected at the V.35 interface while set for direct connect. |

| Setting | Description |
|---|---|
| **Crypto Resync** | Allows a Polycom ISDN Gateway connected to cryptographic equipment to signal when it loses video synchronization during a call. The cryptographic equipment can then resynchronize with the far site. |
| **Use RTS Signal for Resync Pulse** | Allows the system to send the resynchronization pulse on the RTS signal. Select this setting if your data communications equipment uses the V.35 or RS-449 capability of the serial V.35/RS-449/RS-530 network interface.<br>**Note**: When you select this setting, the RTS no longer functions as the Request To Send signal. |
| **Time Between Pulses (sec)** | Specifies whether the system should set the time between resync pulses automatically or use the number of seconds you enter. |
| **Pulse Width (millisec)** | Specifies whether the system should set the pulse duration automatically or use the number of milliseconds you enter. |
| **Enable Broadcast Mode** | Enables support for H.331 broadcast transmissions from the Polycom ISDN Gateway.<br>Broadcast mode enables the system to send video and audio to many other systems, such as large satellite networks. |
| **Enable People+Content** | Enables People+Content for broadcast mode. |
| **Video Format** | Specifies the resolution at which video is transmitted. |
| **Video Protocol** | Specifies the protocol used to transmit video. Choose the lowest protocol supported by all systems in the conference. |
| **Audio Protocol** | Specifies the protocol used to transmit audio. |
| **Frame Rate** | Specifies the frame rate to use. |
| **Dial plan** | Specifies an ISDN number to IP address mapping used by the Polycom ISDN Gateway to route an ISDN initiated call to a RealPresence Group Series system (IP endpoint). |

# Dial Plan Settings

You can configure the dial plan settings for the Polycom ISDN Gateway.

## Prerequisites for the Dial Plan Configuration

Before you configure the dial plan settings, ensure that you perform the following tasks:

- Test the cable connectivity (LAN/ISDN) to the device.
- Before making an encrypted call, ensure that both H.323 and ISDN endpoints have the same encryption.
- Before making an unencrypted call, ensure that both H323 and ISDN (H.320) endpoints have encryption disabled.
- Enable the IP H.323 setting on the Polycom ISDN Gateway.
- For an H.323 call with a Gatekeeper, register both the Polycom ISDN Gateway and the H.323 endpoint with the Gatekeeper.

**Note:** The RealPresence Group Series system should register with Gatekeeper (DMA) using Polycom ISDN Gateway's ISDN number.

## Configure the BRI Dial Plan

You can configure the BRI dial plan for the Polycom ISDN Gateway.

### To configure the dial plan settings for the BRI interface:

1. In the web interface, go to **Admin Settings > Network > ISDN Configuration**.
2. In the dial plan settings, enter one of the eight available ISDN numbers.

   **Note**: A maximum of eight ISDN directory numbers are available using the quad BRI interfaces. This enables users to add routing for eight IP endpoints.
3. Click **Save**.

**Note:** When there are four BRI lines and Group series has registered with Gatekeeper using the first ISDN Gateway BRI number, you need to manually add the remaining BRI numbers with Polycom Group Series MCU IP address.

## Configure the PRI Dial Plan

You can configure the PRI dial plan for the Polycom ISDN Gateway.

### To configure the dial plan settings for the PRI interface:

1. In the web interface, go to **Admin Settings > Network > ISDN Configuration**.
2. In the dial plan settings, enter the Polycom ISDN Gateway number and the respective destination IP address of the Polycom RealPresence Group Series system.

   **Note:** The service provider facilitates a ghost ISDN number for a single PRI line, this enables to route multiple IP calls through multiple ISDN numbers.
3. Select the PRI Line Type:
   - **E1**: Can include up to 30 dial plan entries.
   - **T1**: Can include up to 23 dial plan entries.
4. Click **Save**.

## Configure the V.35 Dial Plan

You can configure the V.35 dial plan for the Polycom ISDN Gateway.

### To configure the dial plan settings for the V.35 interface:

1. In the web interface, go to **Admin Settings > Network > ISDN Configuration**.
2. In the dial plan settings, enter the IP address of destination IP endpoint against V.35 port available.

   **Note:** If dual port is enabled, the same IP address will be entered against the second port.

3 Click **Save**.

For information on how to dial an ISDN call, refer to Dialing from a Video Endpoint.

# Security

To configure your Polycom ISDN Gateway security settings using the web interface, see the following topics:


- Security Options and Passwords
- Configure Security Profiles
- Manage System Access
- Configure Remote Access
- Configure Port Lockout
- View the Remote Sessions List
- Enable a Whitelist
- View the Remote Sessions List
- Certificates and Revocation
- Configure Security Banners


## Security Options and Passwords

Global and local security settings can be found in the web interface.

### To configure security options and passwords:

» In the web interface, go to **Admin Settings** > **Security**.

**Note:** In accordance with local laws and regulations, not all security options are available in all countries.

## Configure Security Profiles

Polycom ISDN Gateway security profiles provide varying levels of secure access to your Polycom ISDN Gateway. The security profile that your Polycom ISDN Gateway uses provides the basis for secure access within the system and determines how users can operate the system.

The security profile is selected during the system setup, but this setting is configurable through the web interface Admin Settings. The default values and ability to change the settings of the Polycom ISDN Gateway are affected by the security profile your system uses. To see how these settings are affected for each security profile, refer to the tables in Appendix D: Security Profile Settings.

Consider each security profile as a set of default values for all configuration settings that affect product security and that achieves some level of base product security. You can choose from four profiles, including Maximum, High, Medium, and Low. Each profile provides a basic security posture, ranging from the most secure to the least secure, which allows you to select a level of security that is appropriate for the deployment of the device in your environment.

Because you can change most of the individual configuration settings regardless of the security profile you choose, Polycom recommends that you select the profile that is closest to the level of security you want in your environment and then customize the settings from there depending on your requirements. In the higher profiles, however, some settings are either not changeable at all or have restricted ranges of values. For specific configuration information, refer to each profile's settings in Appendix D: Security Profile Settings.

### To view or change a security profile:

1. In the web interface, go to **Admin Settings** > **Security** > **Global Security**.
2. Determine which of the following **Security Profile** settings your system uses.

| Setting | Description |
|---|---|
| **Maximum** | Configures the system to be compliant with U.S. DoD security requirements. Some configuration settings are made read-only in this profile; other settings have restricted ranges of values. This profile represents the highest level of security. You might be required to change the password in this profile. |
| **High** | Configures the system with most security controls enabled, but does not mandate the use of some controls that are mandated in Maximum profile. Some configuration settings are not changeable in this profile; other settings have restricted ranges of values. This profile is most appropriate for enterprise deployments that demand high security. |
| **Medium** | Configures the system with some of the basic security controls enabled, but not all. Most settings are changeable in this profile. |
| **Low** | Configures the system with no mandated security controls, although all controls can be enabled as needed. This is the default profile. |

3. To change the profile setting, select the **Security Profile** you want to use.

   You can increase or decrease the level of security.

**Note:** Changing the security profile from a lower level to higher level might require users to change the password.

4. Follow the prompts in the **Security Profile Change** wizard.

# Manage System Access

Managing access to the Polycom ISDN Gateway is essential for security. This section includes the following topics:

- Login and Credentials
- Enable a Whitelist
- Setting Up Local Accounts


## Login and Credentials

Login credentials are user IDs and passwords that identify the user and define the user's ability to access the Polycom ISDN Gateway.

### To configure access to the system:

1. In the web interface, go to **Admin Settings > Security > Local Accounts > Login Credentials**.
2. Configure the following settings.

| Setting | Description |
|---|---|
| **Admin ID** | Specifies the ID for the administrator account. The default Admin ID is `admin`. The administrator can change the **User Name** at any point of time. |
| **Admin Password** | Specifies the password for the local administrator account used when logging in to the system. Passwords are case sensitive and should not have spaces. The maximum length of the password is 40 characters. The default password is the 14-digit system serial number. The serial number can be viewed either on the **System Information** screen or at the bottom of the Polycom ISDN Gateway. |
| **User ID** | Specifies the ID for the user account. The default User ID is `user`. The administrator can change the **User Name** at any point of time. |
| **User Password** | Specifies the password for the local user account used when logging in to the system. Passwords are case sensitive and should not have spaces. The maximum length of the password is 40 characters. The default password is `user`. |
| **Auditor ID** | Specifies the ID for the auditor account. The default Auditor ID is `Auditor`. The administrator can change the **User Name** at any point of time. |
| **Auditor Password** | Specifies the password for the auditor account used when logging in to the system. Passwords are case sensitive and should not have spaces. The maximum length of the password is 40 characters. The default password is `auditor`. |

**Note:** When you enable the Maximum Security profile, the system forces you to change the default values of the following parameters or fields:

- Admin account User ID
- User account User ID
- Auditor account User ID

# Configure Remote Access

*Remote access* means using an Polycom ISDN Gateway through the web, a serial port, or telnet. A *session* is an instance of a user connected to the system through one of these interfaces. Sessions include an indication of how you are logged in to the Polycom ISDN Gateway, such as the web interface or telnet.

**Caution:** The HTTPS protocol ensures that the configuration of all login information (such as user names and passwords) is transmitted using an encrypted channel, including those user names and passwords used to communicate with third-party systems on your network. Using HTTPS severely limits the ability of anyone on the network to discover these credentials. If required, you can also use HTTP to access the web interface. However, you can configure an option that allows access to the web interface with HTTPS only. The HTTP is disabled for higher security profiles, so it will be redirected to HTTPS. It is also redirected for sensitive security information, such as security pages.

### To configure remote access settings:

1. In the web interface, go to **Admin Settings > Security > Global Security > Access**.
2. Configure the following settings. The visibility of some settings is affected by the type of security profile your system uses.

| Setting | Description |
|---|---|
| **Enable Network Intrusion Detection System (NIDS)** | Enables you to log entries to the security log when the system detects a possible network intrusion. By default, this setting is either enabled or disabled. If required, you can change this setting. |
| **Enable Telnet Access** | Specifies whether to allow remote access to the system by telnet. |
| **Enable SSH** | Provides an option to enable SSH. |
| **Enable Serial Port Idle Session Timeout** | Specifies whether to allow the diagnostics port to time out at the configured time interval or not. The timeout setting is set under **Idle Session Timeout in Minutes.** |
| **Enable API Port Idle Session Timeout** | Specifies whether to allow the API port to time out at the configured time interval or not. The timeout setting is set under **Idle Session Timeout in Minutes.** |
| **Enable SNMP Access** | Provides an option to enable remote access to the system by SNMP. |
| **Lock Port after Failed Logins** | Protects against brute-force attacks by temporarily locking the login port after a specified number of unsuccessful login attempts have been made, regardless of which account was used. For more information, refer to Configure Port Lockout. |
| **Enable Whitelist** | Provides an option to enable a whitelist. For more information, refer to Enable a Whitelist. |
| **Idle Session Timeout in Minutes** | Specifies the number of minutes your web interface session can remain idle before the session times out. |
| **Maximum Number of Active Sessions** | Specifies the maximum number of users who can be logged in to and using your system through telnet or the web interface at the same time. |

## Detect Intrusions

The Polycom ISDN Gateway logs an entry to the security log when it detects a possible network intrusion. This logging is controlled by the setting **Admin Settings > Security > Global Security > Access > Enable Network Intrusion Detection System (NIDS)**. The security log prefix identifies the type of packet detected, as shown in the following table.

| Prefix | Packet Type |
|---|---|
| SECURITY: NIDS/unknown_tcp | Packet that attempts to connect or probe a closed TCP port |
| SECURITY: NIDS/unknown_udp | Packet that probes a closed UDP port |
| SECURITY: NIDS/invalid_tcp | TCP packet in an invalid state |
| SECURITY: NIDS/invalid_icmp | ICMP or ICMPv6 packet in an invalid state |
| SECURITY: NIDS/unknown | Packet with an unknown protocol number in the IP header |
| SECURITY: NIDS/flood | Stream of ICMP or ICMPv6 ping requests or TCP connections to an opened TCP port |

Following the message prefix, the security log entry includes the time stamp and the IP, TCP, UDP, ICMP, or ICMPv6 headers. For example, the following security log entry shows an “unknown_udp” intrusion:

```
2015-05-08 21:32:52 WARNING kernel: SECURITY: NIDS/unknown_udp IN=eth0
OUT= MAC=00:e0:db:08:9a:ff:00:19:aa:da:11:c3:08:00 SRC=172.18.1.80
DST=172.18.1.170 LEN=28 TOS=0x00 PREC=0x00 TTL=63 ID=22458 PROTO=UDP
SPT=1450 DPT=7788 LEN=8
```

## Setting Up Local Accounts

For the Polycom ISDN Gateway accounts, you must set up account lockout, login credentials, and password policies.

To mitigate the risk of such an attack, two access control mechanisms are available on Polycom ISDN Gateway. The first type of access control, account lockout, protects local accounts from being vulnerable to brute-force attacks, while the second, port lockout, protects login ports themselves from being vulnerable to brute-force attacks. For more information about that mechanism, refer to Configure Port Lockout.

### Configure Password Policies

You can configure password policies for Admin, User, Auditor, and SNMP passwords.

These password settings can ensure that strong passwords are used. Polycom strongly recommends that you create an Admin password for your system.

#### To configure password policies:

1. In the web interface, go to **Admin Settings > Security > Local Accounts > Password Requirements**.
2. Configure the following settings for **Admin**, **User**, **Auditor**, or **SNMP** passwords. Click **Save**.

| Setting | Description |
|---|---|
| **Minimum Length** | Specifies the minimum number of characters required for a valid password |
| **Require Lowercase Letters** | Specifies whether a valid password must contain one or more lowercase letters |
| **Require Uppercase Letters** | Specifies whether a valid password must contain one or more uppercase letters |
| **Require Numbers** | Specifies whether a valid password must contain one or more numbers |
| **Require Special Characters** | Specifies whether a valid password must contain one or more special characters. Supported characters include:<br>@ - _ ! ; $ , \ / & . # * |
| **Reject Previous Passwords** | Specifies the number of most recent passwords that cannot be reused. If set to **Off**, all previous passwords can be reused. |
| **Minimum Password Age in Days** | Specifies the minimum number of days that must pass before the password can be changed. |
| **Maximum Password Age in Days** | Specifies the maximum number of days that can pass before the password can be changed<br>**Note**: This setting is unavailable for SNMP passwords. |
| **Minimum Changed Characters** | Specifies the number of characters that must be different or change position in a new password. If this is set to **3**, `123abc` can change to `345cde` but not to `234bcd`.<br>**Note**: This setting is unavailable for SNMP passwords. |
| **Maximum Consecutive Repeated Characters** | Specifies the maximum number of consecutive repeated characters in a valid password. If this is set to **3**, **aaa123** is a valid password, but `aaaa123` is not. |
| **Password Expiration Warning** | Specifies how many days in advance the system displays a warning that the password soon expire, if a maximum password age is set.<br>**Note**: This setting is unavailable for SNMP passwords. |
| **Can Contain ID or its Reverse Form** | Specifies whether the associated ID or the reverse of the ID can be part of a valid password. If this setting is enabled and the ID is `admin`, passwords `admin` and `nimda` are allowed. |

Changes to most password policy settings do not take effect until the next time the password is changed. Changes take effect immediately for **Minimum Password Age in Days**, **Maximum Password Age in Days**, and **Password Expiration Warning**. Changing **Minimum Length** from **Off** to some other value also takes effect immediately.

## Account Lockout

Account lockout temporarily locks a local account from accepting logins after a configurable number of unsuccessful attempts to log in to the account. It protects the Polycom ISDN Gateway's Admin, User, and Auditor accounts from unauthorized use by using separate account lockout controls.

You can invoke an account lock due to login failures on the following login ports:

- Web interface
- Telnet interface

- Serial Port

### Configure Account Lockout

You can configure the account lockout in the web interface.

### To configure the account lockout:

1. In the web interface, go to **Admin Settings > Security > Local Accounts > Account Lockout**.
2. Configure these settings for the appropriate account on the **Account Lockout** page, then click **Save**.

| Setting | Description |
|---|---|
| **Lock Admin/User/Auditor Account after Failed Logins** | Specifies the number of failed login attempts allowed before the system locks the account. If set to **Off**, the system does not lock the account due to failed login attempts. |
| **Admin/User/Auditor Account Lock Duration in Minutes** | Specifies the amount of time that the account remains locked due to failed login attempts. After this time period has expired, the failed login attempts counter is reset to zero and logins to the account are once again allowed. |
| **Reset Account Lock Counter After** | Specifies the “failed login window” period of time, starting with the first failed login attempt, during which subsequent failed login attempts will be counted against the maximum number allowed (**Lock Admin/User Account after Failed Logins**). If the number of failed login attempts made during this window does not reach the maximum number allowed, the failed login attempts counter is reset to zero at the end of this window. **Note:** The failed login attempts counter is always reset to zero anytime a user successfully logs in. |

# View Connections to Your System in a Sessions List

You can view a sessions list to see information about everyone logged in to a RealPresence Group system including:

- Type of connection, for example, Web
- ID associated with the session, typically Admin or User
- Remote IP address (addresses of people logged in to the Polycom ISDN Gateway from their computers)

### To view the Sessions List:

1. From the web interface, go to **Diagnostics > System > Sessions**.

# Enable a Whitelist

When a whitelist is enabled, the Polycom ISDN Gateway web interface and SNMP ports accept connections only from specified IP addresses. The whitelist supports both IPv4 and IPv6 addresses.

**Note:** If you use dynamic IP address assignment, ensure that you keep the whitelist up to date with the latest assigned addresses for computers authorized to access the system. Failing to update the whitelist means these computers cannot connect to the system.

### To enable a whitelist:

1. In the web interface, go to **Admin Settings > Security > Global Security > Access**.
2. Select **Enable Whitelist**.

## Add IP Addresses

You can add IP addresses to an enabled whitelist in the web interface.

### To add addresses to an enabled whitelist:

1. In the web interface, go to **Admin Settings > Security > Global Security > Access**.
2. Click the **Edit Whitelist** link.
3. Select address type **IPv4** or **IPv6**.
4. In the address field, enter the IP address of the system you want to allow. Follow the format suggested by the address type you selected. Select **Add**.

   Repeat this step for all the IP addresses you want to add. You can add web server and SNMP addresses.

   If you entered an address in error, highlight the address in the list and select **Clear**.

## IP Address Format

Refer to the following topics for information on the IP address formats for IPv4 and IPv6 addresses.

### IPv4 Address Formats

The whitelist configuration requires single IP addresses, a range of addresses, or an IP and netmask. The netmask represents the number of valid bits of the IPv4 address to use. The following are valid IPv4 formats:

- `10.12.128.7`
- `172.26.16.0/24`

### IPv6 Address Formats

For IPv6 addresses, you can use Classless Inter-Domain Routing (CIDR) notation to represent a range of IP addresses. The following are valid IPv6 formats:

- `::1`
- `2001:db8:abc:def:10.242.12.23`
- `2001:db8::/48`
- `2001:db8:abcd:0012::0/64`
- `2001:0db8:85a3:0000:0000:1234:0abc:cdef`

**Note:** The Polycom ISDN Gateway can accept up to 30 IP address entries for the whitelist.

# Configure Port Lockout

You can configure port lockout in the web interface. Port lockout protects against brute-force attacks by temporarily locking the login port after a specified number of unsuccessful login attempts have been made, regardless of which account was used.

The telnet port has a port lock feature that is enabled regardless of the state of the port lock feature configuration. Specifically, the telnet server disconnects a telnet login session after five failed login attempts. If a new session is started, another five attempts are allowed.

### To configure port lockout:

1. In the web interface, go to **Admin Settings > Security > Global Security > Access**.
2. Select **Lock Port after Failed Logins** and click **Save**.

   The **Lock Port after Failed Logins** setting specifies the number of failed login attempts allowed before the system locks the web interface or Serial Port from accepting logins. If set to **Off**, the system does not lock the web interface due to failed login attempts.

| Setting | Description |
|---|---|
| **Lock Port after Failed Logins** | Specifies the number of failed login attempts allowed before the system locks the account. If set to **Off**, the system does not lock the account due to failed login attempts. |
| **Port Lock Duration** | Specifies the amount of time that a web interface remains locked due to failed login attempts. After this time period expires, the failed login attempts counter is reset to zero and logins to the web interface are once again allowed. |
| **Reset Port Lock Counter After** | Specifies a “failed login window” period of time, starting with the first failed login attempt, during which subsequent failed login attempts will be counted against the maximum number allowed (**Lock Port after Failed Logins)**. If the number of failed login attempts made during this window does not reach the maximum number allowed, the failed login attempts counter is reset to zero at the end of this window.<br>**Note:** The failed login attempts counter is always reset to zero anytime a user successfully logs in. |

# View the Remote Sessions List

You can use the sessions list to see information about remote sessions connected to the Polycom ISDN Gateway system, including:

- Type of connection, for example, Web
- User ID associated with the session, typically Admin or User

- Remote IP address (that is, the addresses of people logged in to the Polycom ISDN Gateway from their computers)

**To view the Sessions List:**

» In the web interface, go to **Diagnostics > System > Sessions**.

# Certificates and Revocation

If your organization has deployed a public key infrastructure (PKI) for securing connections between devices on your network, Polycom recommends that you have a strong understanding of certificate management and how it applies to Polycom ISDN Gateway before you integrate it with the PKI.

Polycom ISDN Gateway can use certificates to authenticate network connections to and from the Polycom ISDN Gateway. Other web applications also use certificates, as you might notice when you navigate the Internet. The system uses configuration and management techniques typical of PKI to manage certificates, certificate signing requests, and revocation checking. ANSI X.509 standards regulate the characteristics of certificates and revocation.

Polycom ISDN Gateway can generate requests for certificates (CSRs) that can be then sent to a certificate authority (CA) for official issuance. The CA is the trusted entity that issues, or signs, digital certificates for others. Once signed by the CA, you can install the certificate on the Polycom ISDN Gateway for use in all TLS connections used by the system.

Polycom ISDN Gateway supports, and typically requires, the generation and use of two separate certificates when used in an environment that has a fully deployed PKI:

- A Server certificate: the Polycom ISDN Gateway device's web server presents this certificate after receiving connection requests from browsers attempting to connect to the web interface.
- A Client certificate: the Polycom ISDN Gateway presents this certificate to a remote server when challenged to provide a certificate as part of authenticating the identity of the Polycom ISDN Gateway before allowing it to connect to the remote server. An example of a remote server is the Polycom® RealPresence® Resource Manager system.

When Polycom ISDN Gateway is deployed in an environment that does not have a fully deployed PKI, you do not need to install these certificates because the Polycom ISDN Gateway system automatically generates self-signed certificates that can be used to establish secure TLS connections. However, when a full PKI has been deployed, self-signed certificates are not trusted by the PKI and so signed certificates must be used.

## Certificate Validation Settings

Certificates are authorized externally when they are signed by the CA. The certificates can be automatically validated when they are used to establish an authenticated network connection. To perform this validation, the Polycom ISDN Gateway must have certificates installed for all CAs that are part of the trust chain.

A trust chain is the hierarchy of CAs that have issued certificates from the device being authenticated, through the intermediate CAs that have issued certificates to the various CAs, leading back to a root CA, a known and trusted CA.

A certificate exchange is between a server and a client, both of which are peers. When a user is accessing the Polycom ISDN Gateway's web interface, the Polycom ISDN Gateway is the server and the web browser is the client application. In other situations, such as when the Polycom ISDN Gateway connects to the

Polycom RealPresence Resource Manager, the Polycom ISDN Gateway is the client and the RealPresence Resource Manager is the server.

### Configure Certificate Usage

You can configure certificate usage in the web interface.

#### To configure certificate usage:

1. Go to **Admin Settings > Security > Certificates > Certificate Options**.
2. Configure the following settings on the **Certificates** screen and click **Save**.

| Setting | Description |
|---|---|
| **Maximum Peer Certificate Chain Depth** | Specifies how many links a certificate chain can have. The term *peer certificate* refers to any certificate sent by the far-end host to the Polycom ISDN Gateway when a network connection is being established between the two devices. |
| **Always Validate Peer Certificates from Browser** | Controls whether the Polycom ISDN Gateway requires a browser to present a valid certificate when it tries to connect to the web interface. |
| **Always Validate Peer Certificates from Server** | Controls whether the Polycom ISDN Gateway requires the remote server to present a valid certificate when connecting to it for services. Examples are provisioning or client-type CSRs. |
| **Installed Certificates** | Allows the administrator to either view installed certificates or to add a new certificate |
| **Signing Request Server** | Allows the administrator to create a new server request certificate |
| **Signing Request Client** | Allows the administrator to create a new client request certificate |

## CSRs and Certificate Types

Before you install a CSR on the Polycom ISDN Gateway, ensure that it has been signed by a CA. CSRs include the following certificate types:

- Client certificate
- Server certificate
- CA-type certificate

## Create Certificate Signing Requests (CSRs)

The Polycom ISDN Gateway allows you to install one client and one server certificate for identification of the Polycom ISDN Gateway to network peers. To obtain these certificates you must first create a Certificate Signing Request (CSR) for each certificate. This request, also known as an unsigned certificate, must be submitted to a CA so that it can be signed, after which the certificate can be installed on the Polycom ISDN Gateway. Whether you need to generate a client-type CSR, a server-type CSR, or both depends on which features and services you intend to use, and whether your network environment supports certificate-based authentication for those services. In most cases, both certificates are needed.

For example, if your Polycom ISDN Gateway is configured to use any of the following features, and the servers providing those services perform certificate-based authentication before allowing access to them,

you must create a client-type CSR and add the resulting certificate signed by the CA. The 802.1X authentication type is supported.

The Polycom ISDN Gateway web server uses the server-type CSR and resulting certificate whenever a user attempts to connect to the Polycom ISDN Gateway web interface. The web server presents the server certificate to the browser to identify the system to the browser and allows the browser to connect to the system. Users need the server certificate if they want to be certain of the identity of the Polycom ISDN Gateway they are connecting to. Settings in the web browser typically control the validation of the server certificate, but you can also validate the certificate manually.

## Create a CSR

To obtain a client or server certificate, you must first create a CSR. You can create one client and one server CSR and submit each to the appropriate CA for signing. After the CSR is signed by a CA, it becomes a certificate that you can add to the Polycom ISDN Gateway. You can perform these steps to create a request for server and client CSRs.

### To create a CSR:

1. Go to **Admin Settings** > **Security** > **Certificates** > **Certificate Options**.
2. In the **Create Signing Request section,** configure the following settings and click **Create**.

| Setting | Description |
|---|---|
| **Hash Algorithm** | Specifies the hash algorithm for the CSR. You may select SHA-256 or keep the default SHA-1. |
| **Common Name (CN)** | Specifies the name that the system assigns to the CSR.<br>Polycom recommends the following guidelines for configuring the Common Name:<br>• For systems registered in DNS, use the Fully Qualified Domain Name (FQDN) of the system.<br>• For systems not registered in DNS, use the IP address of the system.<br>Maximum Characters: 64; truncated if necessary.<br>By default, this is blank |
| **Organizational Unit (OU)** | Specifies the unit of business defined by your organization. Default is blank. Maximum Characters: 64 |
| **Organization (O)** | Specifies your organization's name. Default is blank. Maximum Characters: 64 |
| **City or Locality (L)** | Specifies the city where your organization is located. Default is blank. Maximum Characters: 128 |
| **State or Province (ST)** | Specifies the state or province where your organization is located. Default is blank.<br>Maximum Characters: 128. |
| **Country (C)** | Displays the country selected in **Admin Settings > General Settings > My Information**. Not editable |

**Note:** The Polycom ISDN Gateway supports only one OU field. If you want the signed certificate to include more than one OU field, you must download and edit the CSR manually.

After you create the CSR, the system displays a message that the CSR has been created. Two links appear next to the signing request that you have created.

- **Download Signing Request** enables you to download the CSR so that it can be sent to a CA for signature.
- **Create** enables you to view the fields of the CSR as they are currently set in the CSR. If you change any of the values you previously configured, you can click **Create** to generate a new CSR that can then be downloaded.

**Note:** Only a single outstanding CSR of either type can exist at a time. After the CSR is generated, it is important to get it signed and installed before attempting to generate a different CSR of the same type. For example, if you generate a client CSR and then, prior to having it signed and installed on the Polycom ISDN Gateway, another client CSR is generated, the previous CSR is discarded and invalidated, and any attempt to install a signed version of it result in an error.

## Add a Signed Certificate

You can add a signed certificate in the web interface.

### To add a signed certificate:

1. In the web interface, go to **Admin Settings > Security > Certificates > Certificate Options**.
2. In the **Installed Certificates** section, click **View and Add**.
3. To add a certificate, click **Browse** to search for and select a certificate.

   You might need to install a client or server certificate that has been signed by a CA after having been previously generated as a CSR; or you might need to install a CA certificate needed by the Polycom ISDN Gateway to validate a certificate it receives from another system.
4. Click **Open**.

   The system checks the certificate data and adds it to the list. If you do not see the certificate in the list, the system was unable to recognize the certificate. This process is sometimes referred to as *installing* a certificate.
5. To view the contents of a certificate, select the certificate in the list.
6. To remove a certificate from the list, click **Remove**.
7. Click **Close** to close the certificate section.
8. Click **Save** to save any changes.

When you add a CA certificate to the Polycom ISDN Gateway system, the certificate becomes trusted for the purpose of validating peer certificates.

**Note:** If you do not add the server certificate to the Polycom ISDN Gateway before using the web interface, you might receive error messages from your browser stating that the security certificate for the web site “Polycom” cannot be verified. Most browsers allow the user to proceed after this warning is displayed. For instructions on how to do this, refer to the Help section of your browser.

## View a Signed Certificate

You can view a signed certificate in the web interface.

### To view an installed certificate:

» Go to **Admin Settings > Security > Certificates > Certificate Options**.

# Certificate Revocation Settings

When certificate validation is enabled, the Polycom ISDN Gateway tries to validate the peer certificate chain on secure connection attempts for the applicable network services.

Part of the validation process includes a step called *revocation checking*. This type of check involves consulting with the CA that issued the certificate to see whether the certificate is still active or has been revoked. Revoked certificates are considered invalid because they might have been compromised or improperly issued. The CA is responsible for maintaining the revocation status of every certificate that it issues. The Polycom ISDN Gateway can check this revocation status using either of the following methods:

- Certificate revocation lists (CRLs). A CRL is a list of certificates that have been revoked by the CA. A CRL must be installed on the Polycom ISDN Gateway for each CA whose certificate has been installed on the system.
- The Online Certificate Status Protocol (OCSP). OCSP allows the Polycom ISDN Gateway to contact an *OCSP responder*, which is a network server that provides real-time certificate status through a query/response message exchange.

**Note:** The Polycom ISDN Gateway automatically downloads CRLs from the Certificate Authorities (CAs) that make CRLs available for retrieval by HTTP.

However, for CAs that do not allow HTTP retrieval of CRLs, the Polycom ISDN Gateway system administrator is responsible for manually installing and updating CRLs ahead of their expiration. It is extremely important that CRLs be kept up to date

## Add Certificates and CRLs

You can add certificates and CRLs to the certificate list in the web interface.

### To add a certificate or CRL:

1. Go to **Admin Settings > Security > Certificates > Revocation**.
2. Configure the following settings on the **Revocation** screen.

| Setting | Description |
|---|---|
| **Revocation Method** | Indicates the method for checking the revocation status for a certificate.<br>• **Certificate revocation lists (CRLs)** A CRL is a list of certificates that have been revoked by the CA.<br>A CRL must be installed on the Polycom ISDN Gateway for each CA whose certificate has been installed on the system.<br>• **Online Certificate Status Protocol (OCSP)** OCSP allows the Polycom ISDN Gateway to contact an OCSP responder, which is a network. Select the OCSP method. |
| **Allow Incomplete Revocation Checks** | When this field is enabled, a certificate in the chain is verified without a revocation status check if no corresponding CRL for the issuing CA is installed.<br>The Polycom ISDN Gateway assumes that the lack of a CRL means the certificate is not revoked. If a CRL is installed, the system performs a revocation check when validating the certificate. |

3 Click **Browse** to search for and select a certificate or CRL.

4 Click **Open** to add the certificate or CRL to the list.

5 Click **Save**.

### Remove Certificates and CRLs

You can remove certificates and CRLs from the certificate list in the web interface.

#### To remove a certificate or CRL:

1 Go to **Admin Settings > Security > Certificates > Revocation**.

2 Click **Browse** to search for and select a certificate or CRL.

3 To remove a certificate or CRL from the list, click **Remove**.

4 Click **Save**.

**Note:** If the **Always Validate Peer Certificates from Browsers** setting is enabled and the expired CRL is for a CA that is part of the trust chain for the client certificate sent by your browser, you can no longer connect to the Polycom ISDN Gateway web interface because the revocation check always fails. In this case, unless the Polycom ISDN Gateway web interface can be accessed by a user whose client certificate's trust chain does not include the CA with the expired CRL, you must delete all certificates and CRLS from the system and then reinstall them. For more information, refer to Delete Certificates and CRLs.

## Use the OCSP Revocation Method for Certificates

You can configure the OCSP revocation method on the web interface.

#### To use OCSP:

1 Go to **Admin Settings** > **Security** > **Certificates** > **Revocation**.

2 At **Revocation Method**, select **OCSP**.

3 Configure the following settings.

| Setting | Description |
|---|---|
| **Revocation Method** | Indicates the method for checking the revocation status for a certificate.<br>• **Certificate revocation lists (CRLs)**: A CRL is a list of certificates that have been revoked by the CA.<br>A CRL must be installed on the Polycom ISDN Gateway for each CA whose certificate has been installed on the system.<br>• **Online Certificate Status Protocol (OCSP)**: OCSP allows the Polycom ISDN Gateway to contact an OCSP responder, which is a network.Select the OCSP method. |
| **Allow Incomplete Revocation Checks** | When this field is enabled, the Polycom ISDN Gateway treats the following response from the OCSP responder as a successful revocation checks that would otherwise be considered a failed check:<br>• If the OCSP responder responds that the status is *unknown* or if no response is received, the system treats this as a successful revocation check.<br>Regardless of the state of this setting, the following statements apply:<br>• If the OCSP responder indicates a known *revoked* status, the Polycom ISDN Gateway treats this as a revocation check failure and does not allow the connection.<br>• If the OCSP responder indicates a known *good* status, the Polycom ISDN Gateway treats this as a successful revocation check and allows the connection. |

## Delete Certificates and CRLs

In some cases, expired certificates or CRLs might prevent you from accessing the web interface. You can delete these certificates or CRLs in the web interface.

### To delete all certificates and CRLs the Polycom ISDN Gateway is using:

1 In the web interface, go to **Admin Settings > Security > Certificates**.

2 In the certificates list, click **Delete** next to any certificates that you want to delete.

3 After deleting all installed certificates and CRLs, power off the Polycom ISDN Gateway device and then power it back on.

If you still cannot connect to the device due to access problems, you might need to restore the device to the default factory settings. For details on performing a Factory Restore, see Perform a Factory Restore.

# Configure Security Banners

Security banners consist of text that displays when you log in using both API and web interface.

The following is an example of banner text:

```
This machine is the property of Polycom, Inc., and its use is governed by company
guidelines. You have NO right of privacy when using this machine.
```

### To configure a security banner:

1. In the web interface, go to **Admin Settings > Security > Security Banner**.
2. Configure the following settings.

| Setting | Description |
|---|---|
| **Enable Security Banner** | Specifies whether to display a security banner |
| **Banner Text** | **Custom**: Allows you to enter text to use for the banner<br>**DoD**: Specifies that the system displays a default security banner of the U.S. Department of Defense. You cannot view or change this text on the local interface, but you can change the text on the web interface. |

# Dialing

## Dialing from a Video Endpoint

You can place a video call through the Polycom ISDN Gateway from a Polycom video endpoint, such as a RealPresence Group Series system. Ensure that the dial string contains both the Polycom ISDN Gateway IP address and the destination ISDN number.

The supported dial string format is as follows:

```
<ISDN GW IP address> ## <ISDN number>
```

**Example:**

```
10.200.25.77##5125559696
```

For information on configuring a dial plan and other settings, refer to ISDN and Other Network Interface Settings.

# Polycom ISDN Gateway Software Updates

To keep your device software current, you must perform software updates. Refer to the following topics for software update information:


- Polycom ISDN Gateway Software Updates
- Update System Software from a Web Server
- Update System Software from a USB Storage Device
- Update System Software manually


## Polycom ISDN Gateway Software Updates

You can configure the Polycom ISDN Gateway to get software updates using any of the following methods:

- A server on your network
- Distribution files uploaded from your computer using a web interface to access the system
- A USB 2.0 storage device that you connect to the system

**Note:**
If you use your system within a Department of Defense (DoD) environment, contact your Information Assurance Office (IAO) for approval before using a USB device with your system.

## Update System Software from a Web Server

You can manually install software updates from your own web server.

### *Manually Update Software*

You can manually install software updates from your own web server.

**To manually install software updates:**

1. In the Polycom ISDN Gateway web interface, select **Admin Settings**.

   If necessary, enter the Admin ID as the user name (default is `admin`), and then enter the Admin remote access password.
2. Go to **General Settings > Software Update > Software Server**.
3. In the **Server Address** field, enter the path and address of the update site where you posted the software (for example, `http://10.11.12.100/rpsystem_repo`).
4. Click **Check for Software Updates** to have the system detect updates. The system contacts the designated server to find available updates.

5 If the system indicates an update is available, click **Start Update** to install it.

6 When the Export Restrictions notice appears, click **Accept Agreement**. Follow the on-screen instructions to complete the update.

## Automatically Apply Software Updates

You can automatically check for and apply software updates in the web interface.

### To automatically check for and apply software updates:

1 In the web interface, go to **Admin Settings > General Settings > Software Updates**.

2 Select **Automatic Software Updates**.

3 Configure the following settings.

| Setting | Description |
|---|---|
| **Automatically Check for and Apply Software Updates** | Enables settings that allow you to set up a schedule for automatically checking for and applying software updates to your system. |
| **Start Time** | Specifies the **Hour**, **Minute**, and **AM/PM** setting to start checking for updates. |
| **Duration** | Specifies how long the system should wait to determine whether updates are available. |

4 Click **Save**.

# Update System Software from a USB Storage Device

You can use a USB storage device to update your Polycom ISDN Gateway. A setup wizard guides you through the process.

**Note**: If you use your Polycom ISDN Gateway within a DoD environment, be sure to contact your Information Assurance Office (IAO) for approval before using a USB device with your system.

### To update the software using a USB storage device:

1 Get an installation (.pup) file at support.polycom.com.

2 Copy the file to root directory of the USB storage device and connect it to the Polycom ISDN Gateway.

Please make sure that USB storage device has only one pup file in the root directory.

3 In the web interface, go to **Admin Settings > General Settings > Software Updates > USB Server Update**.

4 Click on **Start Update**.

You can view the update status until the process finishes.

5 Wait for the system to power off and back on if there are no calls on the Polycom ISDN Gateway. If there is an ongoing call, then the gateway should wait to disconnect the call to reboot the Polycom ISDN Gateway.

# Update System Software manually

You can use .pup file to update the software manually for your Polycom ISDN Gateway.

### To update the software manually:

1 In the Polycom ISDN Gateway web interface, go to **Admin Settings > General Settings > Software update > Manual Software update**.

2 Click on **Browse** to select the .pup file, then click **Start Transfer** to begin the update**.**

You can view the update status until the process finishes.

3 Wait for the system to power off and back on. The gateway will be offline during the reboot process.

# Using the API

The Application Programming Interface (API) is a set of commands for advanced users who want to automate the Polycom ISDN Gateway. You can access the API by doing the following.

- Connecting a control system or computer RS-232 serial port to the Polycom ISDN Gateway
- Using with Telnet over the LAN

For more details about using the API, refer to the following topics:

- Using the API with an RS-232 Interface
- Use the API with a LAN Connection
- Secure API Access

## 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 Polycom ISDN Gateway for serial communication.

### Configure the RS-232 Interface

If you use the API with a serial connection, ensure that the RS-232 interfaces of the Polycom ISDN Gateway and your computer are configured appropriately.

#### To configure the RS-232 settings on your system:

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

| Option | Configure your computer | Configure Polycom ISDN Gateway |
|---|---|---|
| Baud rate get | Baud must be the same rate for both devices. The available baud rate is:<br>• 115200 | |
| RS-232 Mode | — | Control |

The RS-232 port on the Polycom ISDN Gateway supports the following modes:

- **Off**: Disables the serial port.
- **Control**: Allows any device connected to the RS-232 port to control the system using API commands.

## Start an API Session using an RS-232 Interface

The Polycom ISDN Gateway can run API sessions from the RS-232 interface. The serial port on a Polycom ISDN Gateway is a DB-9 connector. After you have verified that the Polycom ISDN Gateway and your computer or control system are both configured correctly, set up both devices as follows.

### To start an API session:

1. Use an RS-232 cable to connect the RS-232 port on the computer or control system to the RS-232 port on the Polycom ISDN Gateway as shown in the following figure. This connection may require the Null Modem Adapter. For details, refer to Null Modem Adapter.

2. From the computer or control system, start a serial session using HyperTerminal or another appropriate utility.
3. If prompted for a password, log in with admin account. If prompted for admin or user name, refer to Using the API with Maximum Security Profile Enabled.

## Using the API with Maximum Security Profile Enabled

If the Polycom ISDN Gateway is configured for the Maximum Security profile, API sessions using a LAN Connection (Telnet) are not available. For API sessions using an RS-232 port or SSH, you must log on using a valid user ID and password.

# Use the API with a LAN Connection

If you have a computer connected to the LAN, you can send API commands to the Polycom ISDN Gateway through telnet port 23 or port 24 and SSH.

### To use the API with a LAN connection:

1. On the computer, open a command line interface.
2. Start a Telnet session using the IP address of the Polycom ISDN Gateway and port number that is currently configured for telnet API, for example, telnet `10.11.12.13 24`.
3. Login, if prompted, using the admin account's access password.

# Secure API Access

You can access a Polycom ISDN Gateway using the Secure Shell (SSH) protocol. Secure API access is authenticated for Admin accounts.

**Note:** When a password is empty, users are not allowed to log in because SSH does not validate credentials. Polycom recommends that you consistently use passwords for secure access.

## Enable Secure API Access

Secure API access using SSH is enabled by default. The **Enable SSH Access** option in the web interface can be used to enable the feature.

### To enable SSH for secure API access:

- In the web interface of the Polycom ISDN Gateway, go to **Admin Settings > Security > Global Security > Access** and click the **Enable SSH Access** setting.

## Disable Secure API Access

The **Enable SSH Access** option in the web interface can be used to disable the feature.

### To disable SSH for secure API access:

- In the web interface of the Polycom ISDN Gateway, select **Admin Settings > Security > Global Security > Access** and click the **Enable SSH Access** setting.

## 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. Enable the SSH feature.
3. Start an SSH session using the Polycom ISDN Gateway IP address and port 22.
4. When prompted, enter the access credentials.

# System Commands

This topic describes the API commands for the Polycom ISDN Gateway. For an alphabetical list of all the commands, refer to the table of contents of this document.

**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 contains the API commands used to access the Polycom ISDN Gateway.

### 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 | List of parameters that are defined for the command |
| Description (parameter) | Description of each parameter that is defined for the command |
| User Accessible | Indicates (with a check mark) that user role API sessions are permitted to execute the command or command parameter combination. Otherwise, the field is empty to indicate user role API sessions are not permitted.<br>The role of an API session is determined when the API session is created. All API sessions can be created as **admin** sessions and thus have permission to use all API commands. API sessions can also be created as **user** sessions, which are permitted to use only a subset of the API commands that are authorized for normal users. For more information on user roles, refer to Manage System Access.<br>**Note**: User sessions are available only through SSH or on the serial port (when the configured serial port Login Mode is **username/password**). User sessions with telnet are also available only when you have selected low security profile. |
| Additional Restrictions | Additional restrictions that apply to using the command or command/parameter combination. Otherwise, the field is empty to indicate there are no additional restrictions. |
| Feedback Examples | Examples of expected results when a command and variant are executed |
| Limitations | Polycom ISDN Gateway does not support the command |
| Comments | Important notes about the command |

### Syntax Conventions

The following conventions are used for the API command descriptions in this chapter. All of the commands

are case sensitive.

| Convention | Meaning |
|---|---|
| `<param1\|param2\|param3>` | Multiple valid parameters are enclosed in angle brackets and separated by the pipe (“|”) character.<br>**Example**: `allowdialing <yes\|no\|get>` shows that the `allowdialing` command must be followed by one of the parameters listed. |
| `[param]`<br>`[“param”]` | Optional parameters are enclosed in square brackets. Quotation marks indicate strings to be supplied by the user.<br>**Example**: `teleareacode set ["telephone_area_code"]` shows that you can supply a value for the area code, or omit it and let the default value apply. You do not need to enclose the actual value in quotes unless it contains a space. |
| `{a..z}` | A range of possible alphanumeric values is enclosed in braces.<br>**Example**: `abk letter {a..z}` shows that the `abk` command can be used to return address book entries that begin with an alphanumeric character in the range specified. |
| `“x”` | Quotation marks indicate strings to be supplied by the user. You do not need to enclose the value in quotes unless it contains a space. |

The API command parser can accept minimum number of characters in a command but it is recommended that you always use the full command string.

### Availability of Commands

The availability of API commands depends on the type of system, optional equipment installed or connected, security settings and the software version installed on the system. If a particular command is not supported on the system, the command returns feedback, such as “`error: this command is not supported on this model`” or “`command is not available in current system configuration`”.

Commands that are not listed in this chapter are not supported by Polycom. Commands might change or be removed at any time. Polycom discourages the use of unpublished commands.

**Note:** API support is not available for telnet ports 23 and 24 when Security Mode is enabled.

## Command Response Syntax

When you send a command, the Polycom ISDN Gateway returns responses using the syntax described in the following sections, where <CR> indicates a carriage return and <LF> indicates a line feed.

## Commands that restart the Polycom ISDN Gateway

The commands that restart the Polycom ISDN Gateway without a prompt:

- `reboot now`
- `resetsystem`

## Additional Tips

- The system does not provide flow control. If the connection is lost through restarting the system or other means, you must re-establish the connection.
- The API processes one command at a time.
- Polycom does not recommend sending multiple commands simultaneously without a pause or delay between them.
- For commands with a single action and a single response: A delay of 200 milliseconds between commands is usually sufficient. Examples of these commands include the commands:

  `ipaddress get`

  `isdninterface get`
- For commands with a single action and a more extensive response: The time required to receive the response, and thus the time between commands, may be longer than 200 milliseconds. The response length, which can vary in size, determines the time required to receive the response. Examples of these commands include the commands for retrieving IP statistics (`ipstat`), the list of system settings, and system session information (such as `whoami`).
- The API provides feedback status in two ways: registrations or polling.
- Only send registration and notification API commands once. Registrations are written to Flash memory and retained when the system restarts.
- Registrations are specific to the port from which they are registered. If you register for notifications from com port 1, registration will not be sent to com port 2 or Telnet port 24.

## areacode

Sets or gets the area code for all ISDN lines. This command is only applicable if you have a network interface connected to your system and the ISDN interface is set to BRI, PRI or V.35.

### Syntax

```
areacode get
areacode set "areacode"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the area code information. | Yes | |
| `set` | Sets the ISDN area code when followed by the area code parameter. To erase the current setting, omit `"areacode"` | | |
| `"areacode"` | Area code to use for all lines. | | |

### Feedback Examples

- `areacode set 212`

  returns

  `areacode 212`

- `areacode get`

  returns

  `areacode 212`

### Comments

This area code is associated with the area where the system is used.

## bri1enable, bri2enable, bri3enable, bri4enable

Sets or gets the configuration of the specified ISDN BRI line. This command is only applicable if the ISDN interface is set to BRI.

### Syntax

`bri1enable <get|yes|no>`

`bri2enable <get|yes|no>`

`bri3enable <get|yes|no>`

`bri4enable <get|yes|no>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the status of the BRI line. Yes if enabled, no if disabled | Yes | |
| `yes` | Enables the BRI line | | |
| `no` | Disables the BRI line | | |

### Feedback Examples

- `bri1enable yes`

  returns

  `bri1enable yes`
- `bri1enable no`

  returns

  `bri1enable no`
- `bri1enable get`

  returns

  `bri1enable no`

## briallenable

Sets or gets the configuration of all ISDN BRI lines. This command is only applicable if the ISDN interface set to BRI.

### Syntax

```
briallenable <get|yes|no>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the status of the BRI line. Yes if enabled, no if disabled | Yes | |
| `yes` | Enables the BRI line | | |
| `no` | Disables the BRI line | | |

### Feedback Examples

- `briallenable yes`

  returns

  ```
  bri1enable yes
  bri2enable yes
  bri3enable yes
  bri4enable yes
  ```

- `briallenable no`

  returns

  ```
  bri1enable no
  bri2enable no
  bri3enable no
  bri4enable no
  ```

- `briallenable get`

  returns

  ```
  bri1enable no
  bri2enable no
  bri3enable no
  bri4enable no
  ```

### Comments

`briallenable yes` only enables lines where the directory numbers have been populated.

## calldetailreport

Turns on or turns off the option to generate a report of all calls made with the system.

### Syntax

```
calldetailreport <get|yes|no>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes` | Turns on call detail reporting | | |
| `no` | Turns off call detail reporting | | |

### Feedback Examples

- `calldetailreport yes`
  returns
  `calldetailreport yes`
- `calldetailreport no`
  returns
  `calldetailreport no`
- `calldetailreport get`
  returns
  `calldetailreport no`

### Comments

`calldetailreport no` disables the Call Detail Report.

Do not use the `no` parameter with the `calldetailreport` command if the Polycom ISDN Gateway is configured with Maximum Security Profile. Call Detail Reports are automatically generated when the Polycom ISDN Gateway is configured with the Maximum Security Profile.

## callstats

Returns call summary information.

### Syntax

`callstats`

### Feedback Examples

- `callstats`
  returns
  `totalnumberofcalls 23`
  `totalnumberofIPtoISDNcalls 23`
  `totalnumberofISDNtoIPcalls 0`

## calldetail

Displays all call detail records, a specific call detail record, or the call detail range.

### Syntax

```
calldetail <"Nth_item"|all>
calldetail range
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| "Nth item" | Displays the Nth call record | ü | |
| all | Displays all call detail record | | |
| range | Displays the range of records in the call detail report | | |

### Feedback Examples

- `calldetail 1`

  returns

  ```
  1,02/Nov/2008,16:34:34,02/Nov/2008,16:34:34,0:00:00,---,Polycom HDX
  Demo,192.168.1.101,---,h.323,384Kbps,"Polycom/HDX 9004/
  2.5",Out,2,1,---,---,---,terminal,192.168.1.101,Siren22,Siren22,
  H.264,H.264,4SIF,----,"The call has ended.; Local user initiated
  hangup.",16,---,0.00,0.00,0.00,0.00,0,0,0,0,0,0,0,0
  ```

- `calldetail range`

  returns

  ```
  1..29
  ```

## country

Gets the country setting for the system.

### Syntax

```
country get
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| get | Returns the country setting | Yes | |

### Feedback Examples

- `country get`

  returns

  ```
  country "united states"
  ```

## cts

Sets or gets the CTS serial interface control signal (clear to send) configuration. This command is only applicable if the ISDN interface is set to V.35.

### Syntax

```
cts <get|normal|inverted|ignore>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the country setting | Yes | |
| `normal` | Sets the signal to normal (high voltage is logic 1) | | |
| `inverted` | Sets the signal to inverted (low voltage is logic 1) | | |
| `ignore` | Ignores the signal | | |

### Feedback Examples

- `cts normal`

  returns

  `cts normal`
- `cts inverted`

  returns

  `cts inverted`
- `cts get`

  returns

  `cts inverted`

### Comments

The default setting for this signal is “normal”.

## daylightsavings

Sets or gets the daylight saving time setting. When you enable this setting, the system clock automatically changes for daylight saving time.

### Syntax

```
daylightsavings <get|yes|no>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes` | Enables automatic adjustment for daylight savings time | | |
| `no` | Disables automatic adjustment for daylight savings time | | |

### Feedback Examples

- `daylightsavings no`

  returns

  `daylightsavings no`
- `daylightsavings yes`

  returns

  `daylightsavings yes`
- `daylightsavings get`

  returns

  `daylightsavings yes`

## dcd

Sets the configuration for the DCD serial interface control signal (data carriers detect). This command is only applicable if the ISDN interface is set to V.35.

### Syntax

`dcd <normal|inverted>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `normal` | Sets the signal to normal (high voltage is logic 1) | Yes | |
| `inverted` | Sets the signal to inverted (low voltage is logic 1) | | |

### Feedback Examples

- `dcd normal`

  returns

  `dcd normal`

- `dcd inverted`

  returns

  `dcd inverted`

### Comments

The default setting for this signal is “normal”.

## dcdfilter

Sets or gets the filter setting of the DCD serial interface control signal (data carrier detect). This command is only applicable if the ISDN interface is set to V.35

### Syntax

`dcdfilter <get|on|off>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `on` | Enables the DCD filter | | |
| `off` | Disables the DCD filter | | |

### Feedback Examples

- `dcdfilter on`

  returns

  `dcdfilter on`
- `dcdfilter off`

  returns

  `dcdfilter off`
- `dcdfilter get`

  returns

  `dcdfilter off`

### Comments

When this filter is enabled, DCD drops for 60 seconds before changing the call state. The default setting for this signal is `"off"`.

## defaultgateway

Sets or gets the default gateway.

### Syntax

```
defaultgateway get
defaultgateway set "xxx.xxx.xxx.xxx"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the default gateway IP address | Yes | |
| `set` | Sets the default gateway when followed by the “xxx.xxx.xxx.xxx” parameter | | |
| `xxx.xxx.xxx.xxx` | IP address to use as the default gateway | | |

### Feedback Examples

- `defaultgateway set 192.168.1.101`

  returns

  `defaultgateway 192.168.1.101`

### Comments

This setting can only be changed if DHCP is turned off. After making a change, you must restart the system for the setting to take effect.

## destunreachabletx

Sets or gets the system’s ability to generate a Destination Unreachable ICMP message in response to a packet that cannot be delivered to its destination for reasons other than congestion.

### Syntax

`destunreachabletx <yes|no>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes` | Enables the system’s ability to generate a destination unreachable ICMP message in response to a packet that cannot be delivered to its destination for reasons other than congestion | | |
| `no` | Enables the system’s ability to generate a destination unreachable ICMP message in response to a packet that cannot be delivered to its destination for reasons other than congestion | | |

### Feedback Examples

- `destunreachabletx`

  returns

  `destunreachabletx no`
- `destunreachabletx yes`

  returns

  `destunreachabletx yes`

### Comments

This setting is applicable for both IPv4 and IPv6 configurations. After making a change, you must restart the system for the setting to take effect.

## dhcp

Sets or gets DHCP options.

### Syntax

`dhcp <get|off|client>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the selected DHCP option | ü | |
| `off` | Disables DHCP | | |
| `client` | Enables DHCP client, setting the system to obtain an IP address from a server on your network | | |

### Feedback Examples

- `dhcp off`

  returns

  `dhcp off`
- `dhcp client`

  returns

  `dhcp client`
- `dhcp get`

  returns

  `dhcp client`

### Comments

After making a change, you must restart the system for the setting to take effect.

## dialchannels

Sets or gets whether to dial ISDN channels in parallel. This command is only applicable if the ISDN interface is set to BRI.

### Syntax

```
dialchannels get
dialchannels set n
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the number of channels to dial | | |
| `n` | Sets the number of channels to dial. `n` is 8 for QBRI, 12 for PRI | | |

### Feedback Examples

- `dialchannels set 8`

  returns

  `dialchannels 8`
- `dialchannels get`

  returns

  `dialchannels 8`

## diffservaudio, diffservfecc, diffservvideo

Sets or gets the DiffServ option and specifies a priority level for audio, far-end camera control (FECC) and other call control channels, and video, respectively. The priority level value for each can be between 0 and 63.

### Syntax

```
diffservaudio get
diffservaudio set {0..63}
diffservfecc get
diffservfecc set {0..63}
diffservvideo get
diffservvideo set {0..63}
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the command. A priority level in the range {`0..63`} is required. | | |
| `{0..63}` | Specifies the priority level | | |

### Feedback Examples

- `diffservaudio set 2`

  returns

  `diffservaudio 2`

- `diffservaudio get`

  returns

  `diffservaudio 2`

### Comments

The diffservfecc command is equivalent to the Control setting in the user interface. If the typeofservice is set to ip-precedence rather than to diffserv, these commands are not applicable.

## dns

Sets or gets the configuration for up to four DNS servers.

### Syntax

```
dns get {1..4}
dns set {1..4} "xxx.xxx.xxx.xxx"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current IP address of the specified server. A server identification number `{1..4}` is required. | Yes | |
| `{1..4}` | Specifies the server identification number | | |
| `set` | Sets the IP address of the specified DNS server when followed by the `"xxx.xxx.xxx.xxx"` parameter. A server identification number `{1..4}` is required. | | |
| `"xxx.xxx.xxx.xxx"` | Specifies the IP address for the specified server | | |

### Feedback Examples

- `dns set 1 192.168.1.205`

  returns

- `dns 1 192.168.1.205`

### Comments

After making a change, you must restart the system for the setting to take effect. These values cannot be set if the system is in DHCP client mode.

# dsr

Sets or gets the configuration of the DSR serial interface control signal (data set ready). This command is only applicable if the ISDN interface is set to V.35.

## Syntax

```
dsr <get|normal|inverted>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `normal` | Sets the signal to normal (high voltage is logic 1) | | |
| `inverted` | Sets the signal to inverted (low voltage is logic 1) | | |

## Feedback Examples

- `dsr normal`

  returns

  `dsr normal`
- `dsr inverted`

  returns

  `dsr inverted`
- `dsr get`

  returns

  `dsr inverted`

## Comments

The default setting for this signal is “normal”.

# dsranswer

Sets or gets the configuration of the DSR serial interface control signal to indicate an incoming call. This command is only applicable if the ISDN interface is set to V.35.

## Syntax

```
dsranswer <get|on|off>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `on` | Turns on the option | | |
| `off` | Turns off the option | | |

### Feedback Examples

- `dsranswer on`

  returns

  `dsranswer on`
- `dsranswer off`

  returns

  `dsranswer off`
- `dsranswer get`

  returns

  `dsranswer off`

## dtr

Sets or gets the configuration of the DTR serial interface control signal (data terminal ready). This command is only applicable if the ISDN interface is set to V.35.

### Syntax

```
dtr <get|normal|inverted|on>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `normal` | Sets the signal to normal (high voltage is logic 1) | | |
| `inverted` | Sets the signal to inverted (low voltage is logic 1) | | |
| `on` | Sets constant high voltage. If this option is selected, `inverted` is not an option. | | |

### Feedback Examples

- `dtr normal`

  returns

  `dtr normal`
- `dtr inverted`

  returns

  `dtr inverted`
- `dtr on`

  returns

  `dtr on`
- `dtr get`

  returns

  `dtr on`

### Comments

The default setting for the signal is "normal".

## e164ext

Sets or gets an H.323 (IP) extension, also known as an E.164 name.

### Syntax

```
e164ext get
e164ext set "e.164name"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| get | Returns the current setting | Yes | |
| set | Sets the E.164 extension when followed by the "e.164name" parameter. To erase the current setting, omit "e.164name". "e.164name" A valid E.164 extension (usually a four-digit number). | | |

### Feedback Examples

- `e164ext set`

  returns

  `e164ext <empty>`
- `e164ext set 7878`

  returns

  `e164ext 7878`
- `e164ext get`

  returns

  `e164ext 7878`

### Comments

The extension number is associated with a specific LAN device.

## enablefirewalltraversal

Sets or gets the Enable H.460 Firewall Traversal setting. This feature requires a border controller that supports H.460.

### Syntax

```
enablefirewalltraversal <get|on|off>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `on/true` | Enables the firewall traversal feature | | |
| `off/false` | Disables the firewall traversal feature | | |

### Feedback Examples

- `enablefirewalltraversal on`

  returns

  `enablefirewalltraversal on`
- `enablefirewalltraversal off`

  returns

  `enablefirewalltraversal off`
- `enablefirewalltraversal get`

  returns

  `enablefirewalltraversal off`

## enablersvp

Sets or gets the RSVP (Resource Reservation Protocol) setting on the system, which requests that routers reserve bandwidth along an IP connection path.

### Syntax

`enablersvp <get|yes/true|no/false>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes/true` | Enables the RSVP option | | |
| `no/false` | Disables the RSVP option | | |

### Feedback Examples

- `enablersvp yes`

  returns

  `enablersvp yes`
- `enablersvp no`

  returns

  `enablersvp no`

- `enablersvp get`
  returns
  `enablersvp no`

### Comments

This option is enabled by default.

## enablesnmp

Sets or gets the SNMP configuration.

### Syntax

`enablesnmp <get|yes/true|no/false>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes/true` | Enables the SNMP option | | |
| `no/false` | Disables the SNMP option | | |

### Feedback Examples

- `enablesnmp yes`
  returns
  `enablesnmp yes`
- `enablesnmp no`
  returns
  `enablesnmp no`
- `enablesnmp get`
  returns
  `enablesnmp no`

### Comments

After making a change, you must restart the system for the setting to take effect.

## gatekeeperip

Sets or gets the IP address of the gatekeeper.

### Syntax

```
gatekeeperip get
gatekeeperip set ["xxx.xxx.xxx.xxx"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the gatekeeper IP address when followed by the "`xxx.xxx.xxx.xxx`" parameter. To erase the current setting, omit "`xxx.xxx.xxx.xxx`". "`xxx.xxx.xxx.xxx`" IP address of the gatekeeper. The gatekeeperip get command feedback may include the port number after the IP address | | |

### Feedback Examples

- `gatekeeperip set 192.168.1.205`

  returns

  `gatekeeperip 192.168.1.205`

- `gatekeeperip get`

  returns

  `gatekeeperip 192.168.1.205`

## getconfiguredipaddress

Retrieves the currently configured IPv4 address from the system.

### Syntax

`getconfiguredipaddress`

### Feedback Examples

- `getconfiguredipaddress`

  returns

  `getconfiguredipaddress 1.2.3.4`

### Comments

`getconfiguredipaddress`s returns the currently configured IPv4 address of the system regardless of the status of the LAN connection. This differs from the `ipaddress get` command, which returns the current IP address of the system if it has an active LAN connection, else it returns `0.0.0.0`.

The definition of "currently configured IPv4 address" depends on the IPv4 address configuration settings:

- If the **Connect to My LAN** setting is disabled, then `0.0.0.0` is returned. Otherwise, the definition depends on the IP Address (IPv4) setting.
- If the IP address is set manually the configured IP address is returned, regardless of whether the LAN connection is currently active.
- If the IP address is obtained automatically, the currently-assigned address is returned, or `0.0.0.0` is returned if there is no active connection

## h323name

Sets or gets the system's H.323 name.

### Syntax

```
h323name get
h323name set ["H.323name"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the H.323 name when followed by the `"H.323name"` parameter. To erase this setting, omit the `"H.323name"` parameter. | | |
| `"H.323name"` | Character string specifying the H.323 name. Use quotation marks around strings that contain spaces. For example: `"Polycom ISDN Gateway"` | | |

### Feedback Examples

- `h323name set My`

  returns

  `h323name my`
- `h323name set "Polycom ISDN Gateway"`

  returns

  `h323name "polycom isdn gateway"`
- `h323name get`

  returns

  `h323name "polycom isdn gateway"`

## hostname

Sets or gets the LAN host name, which is assigned to the system for TCP/IP configuration and can be used in place of an IP address when dialing IP calls.

### Syntax

```
hostname get
hostname set ["hostname"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the system's LAN host name when followed by the "`hostname`" parameter. If "`hostname`" is omitted, the system automatically sets it to Admin. | | |
| "`hostname`" | Character string specifying the LAN host name of the system. The LAN host name follows these format rules:<br>• Starts with a letter (A-a to Z-z). It is not case sensitive.<br>• Ends with a letter (A-a to Z-z) or a number (0 to 9).<br>• May include letters, numbers, and a hyphen. May not be longer than 63 characters.<br>**Note:** The LAN host name is initialized during the setup wizard sequence. The LAN host name is the same as the system name, if the system name conforms to the rules above. If the system name does not conform to these rules, the invalid characters are removed from the system name. If the resulting string is empty, the default LAN host name is Admin. | | |

### Feedback Examples

- `hostname set`

  returns

  `hostname ADMIN`
- `hostname set "My"`

  returns

  `hostname My`
- `hostname get`

  returns

  `hostname My`

### Comments

A LAN host name is required; it cannot be deleted or left blank. After making a change, you must restart the system for the setting to take effect.

## ipaddress

Sets or gets the LAN IP address (IPv4) of the system.

### Syntax

```
ipaddress get
ipaddress set "xxx.xxx.xxx.xxx"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the LAN IP address to the `"xxx.xxx.xxx.xxx"` parameter. This setting can only be changed when DHCP is off. | | |
| `"xxx.xxx.xxx.xxx"` | IP address of the system | | |

### Feedback Examples

- `ipaddress set 192.168.1.101`

  returns

  `ipaddress 192.168.1.101`
- `ipaddress get`

  returns

  `ipaddress 192.168.1.101`

### Comments

Use this command when you need to allocate a static IP address to your system. After making a change, you must restart the system for the setting to take effect.

## ipprecaudio, ipprecfecc, ipprecvideo

Sets or gets the IP Precedence priority level (Type of Service Value) for audio, far-end camera control (FECC) and other call control channels, and video. The value for each can be between 0 and 7.

### Syntax

```
ipprecaudio get
ipprecaudio set {0..7}
ipprecfecc get
ipprecfecc set {0..7}
ipprecvideo get
ipprecvideo set {0..7}
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the IP precedence. A priority level is required. This must be an integer in the range `{0..7}`. | | |

### Feedback Examples

- `ipprecaudio set 5`
  returns
  `ipprecaudio 5`
- `ipprecaudio get`
  returns
  `ipprecaudio 5`

### Comments

The `ipprecfecc` command is equivalent to the Control setting in the user interface.

If the typeofservice command is set to `diffserv`, these commands are not applicable.

## ipv6addrmode

Sets or gets the ability for the system to act as a client and receive an address, specify an address manually, or completely disable IPv6.

### Syntax

`ipv6addrmode <get|client|manual|off>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `client` | IPv6 addresses from network elements | | |
| `manual` | Allows full configuration of IPv6 addresses | | |
| `off` | Disables IPv6 addressing | | |

### Feedback Examples

- `ipv6addrmode get`
  returns
  `ipv6addrmode client`

- `ipv6addrmode off`

  returns

  `ipv6globaladdress off`

### Comments

This setting is applicable for IPv6 configurations. After making a change, you must restart the system for the setting to take effect.

## ipv6globaladdress

Sets or gets the IPv6 link global address.

### Syntax

```
ipv6globaladdress get
ipv6globaladdress set "ipv6 global address"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the IPv6 global address | | |
| `"ipv6 global address"` | The local IPv6 global address | | |

### Feedback Examples

- `ipv6globaladdress get`

  returns

  `ipv6globaladdress 2002:ac1a:140:0:2e0:dbff:fe08:a03a/64`

- `ipv6globaladdress set 2002:ac1a:140:0:2e0:dbff:fe08:a03a/64`

  returns

  `ipv6globaladdress 2002:ac1a:140:0:2e0:dbff:fe08:a03a/64`

### Comments

After making a change, you must restart the system for the setting to take effect. This setting can be changed only when ipv6addrmode is set to manual.

## ipv6defaultgateway

Sets or gets the IPv6 default gateway.

### Syntax

```
ipv6defaultgateway get
ipv6defaultgateway set "ipv6 link local address"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the IPv6 default gateway | | |
| `"ipv6 link local address"` | The local IPv6 default gateway | | |

### Feedback Examples

- `ipv6defaultgateway get`

  returns

  `ipv6defaultgateway fe80::213:5fff:fe2f:2e4a`
- `ipv6defaultgateway set fe80::213:5fff:fe2f:2e4a`

  returns

  `ipv6defaultgateway fe80::213:5fff:fe2f:2e4a`

### Comments

After making a change, you must restart the system for the setting to take effect. This setting can be changed only when ipv6addrmode is set to manual.

## ipv6linklocal

Sets or gets the IPv6 link local address.

### Syntax

```
ipv6linklocal get
ipv6linklocal set "ipv6 link local address"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the IPv6 link local address | | |
| `"ipv6 link local address"` | The local IPv6 link local address | | |

### Feedback Examples

- `ipv6linklocal get`

  returns

  `ipv6linklocalfe80::2e0:dbff:fe08:a03a/64`

- `ipv6linklocal set fe80::2e0:dbff:fe08:a03a/64`

  returns

  `ipv6linklocalfe80::2e0:dbff:fe08:a03a/64`

### Comments

After making a change, you must restart the system for the setting to take effect. This setting can be changed only when ipv6addrmode is set to **manual**.

## ipv6sitelocal

Sets or gets the IPv6 site local address.

### Syntax

`ipv6sitelocal get`

`ipv6sitelocal set "ipv6 site local address"`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the IPv6 site local address | | |
| `"ipv6 site local address"` | The local IPv6 site local address | | |

### Feedback Examples

- `ipv6sitelocal get`

  returns

  `ipv6sitelocal fed0:0:140:1:2e0:dbff:fe08:a03a/64`
- `ipv6sitelocal set fed0:0:140:1:2e0:dbff:fe08:a03a/64`

  returns

  `ipv6sitelocal fed0:0:140:1:2e0:dbff:fe08:a03a/64`

### Comments

After making a change, you must restart the system for the setting to take effect. This setting can be changed only when ipv6addrmode is set to **manual**.

## ipstat

Returns the LAN host name, DHCP, IP address, DNS servers 1-4, default gateway, and subnet mask.

### Syntax

`ipstat`

### Feedback Examples

- `ipstat`

  returns

  ```
  hostname My
  domainname domain.polycom.com
  winsresolution no
  dhcp client
  ipaddress 192.168.1.101
  dnsserver 192.168.1.102
  dnsserver1 192.168.1.103
  dnsserver2 192.168.1.104
  dnsserver3 0.0.0.0
  defaultgateway 192.168.1.105
  subnetmask 255.255.255.0
  winsserver 192.168.1.106
  lanport auto
  ```

## isdncountrycode

Sets or gets the ISDN country code associated with the country where the system is used.

### Syntax

```
isdncountrycode get
isdncountrycode set ["country code"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the country code information | Yes | |
| `set` | Sets the ISDN country code when followed by the `"country code"` parameter. To erase the current setting, omit `"country code"`. | | |
| `"country code"` | The ISDN country code | | |

### Feedback Examples

- `isdncountrycode set 1`

  returns

  ```
  isdncountrycode 1
  ```

- `isdncountrycode get`

  returns

  `isdncountrycode 1`

### Comments

The system is generally able to automatically determine the country code based on the country you selected during initial system setup.

## isdndialingprefix

Sets or gets the ISDN dialing prefix used to access an outside line if the system is behind a PBX.

### Syntax

```
isdndialingprefix get
isdndialingprefix set ["isdn prefix"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the ISDN dialing prefix information | Yes | |
| `set` | Sets the ISDN dialing prefix when followed by the "`isdn prefix`" parameter. To erase the current setting, omit "`isdn prefix`". | | |
| "`isdn prefix`" | The digit(s) that must be dialed to reach an outside line | | |

### Feedback Examples

- `isdndialingprefix set 9`

  returns

  `isdndialingprefix 9`

- `isdndialingprefix get`

  returns

  `isdndialingprefix 9`

## isdninterface

Sets or gets the ISDN interface.

### Syntax

```
isdninterface <get|v35|bri|pri|none>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| get | Returns the ISDN interface | Yes | |
| v35 | Sets the V.35 interface | | |
| bri | Sets the BRI interface | | |
| pri | Sets the PRI interface | | |
| none | This is the default selection. With this parameter, the interface is set to unknown. | | |

### Feedback Examples

- `isdninterface bri`
  returns
  `isdninterface bri`
- `isdninterface get`
  returns
  `isdninterface bri`

### Comments

Changing the ISDN interface will reboot system automatically.

## isdnnum

Sets or gets the ISDN video number or numbers assigned to the system. This command is only applicable if the ISDN interface is set to BRI.

### Syntax

```
isdnnum get <1b1|1b2|2b1|2b2|3b1|3b2|4b1|4b2>
isdnnum set <1b1|1b2|2b1|2b2|3b1|3b2|4b1|4b2> ["number"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| get | Returns the current ISDN number associated with the specified B channel | Yes | |
| set | Sets the ISDN number for a B channel line when followed by the "number" parameter. To erase the current setting, omit "number". This paramater is not allowed while in a call. | | |

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `1b1\|1b2\|2b1\|2b2\|3b1\|3b2\|4b1\|4b2` | The line and B channel. Valid values are:<br>1b1BRI line 1, B channel 1<br>1b2BRI line 1, B channel 2<br>2b1BRI line 2, B channel 1<br>2b2BRI line 2, B channel 2<br>3b1BRI line 3, B channel 1<br>3b2BRI line 3, B channel 2<br>4b1BRI line 4, B channel 1<br>4b2BRI line 4, B channel 2 | | |
| `"number"` | The ISDN number(s) provided by your network service provider for the specified B channel. | | |

### Feedback Examples

- `isdnnum set 1b1 "700 555 1212"`

  returns

  `isdnnum 1b1 7005551212`
- `isdnnum get 1b1`

  returns

  `isdnnum 1b1 7005551212`

### Comments

The `isdnnum set 1b1` and `isdnnum get 1b1` commands can be used for BRI and for PRI lines.

## isdnswitch

Sets or gets the ISDN switch protocol. This command is only applicable if the ISDN interface is set to BRI.

### Syntax

```
isdnswitch get
isdnswitch <pt-to-pt_at&t_5_ess|multipoint_at&t_5_ess|ni-1>
isdnswitch <nortel_dms-100|standard_etsi_euro-isdn|ts-031|ntt_ins-64>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current switch protocol | Yes | |
| • `pt-to-pt_at&t_5_ess\|multipoint_at&t_5_ess\|ni-1`<br>• `nortel_dms-100\|standard_etsi_euro-isdn\|ts-031\|ntt_ins-64` | Specifies the ISDN switch protocol to use | | |

### Feedback Examples

- `isdnswitch pt-to-pt_at&t_5_ess`

  returns

  `isdnswitch pt-to-pt_at&t_5_ess`
- `isdnswitch nortel_dms-100`

  returns

  `isdnswitch nortel_dms-100`
- `isdnswitch get`

  returns

  `isdnswitch nortel_dms-100`

### Comments

If more than one switch protocol is supported, you must find out from your telephone service provider which protocol to select. If you change the country settings, a new set of ISDN switch protocols is loaded.

## lanport

Sets or gets the LAN port settings of the system.

### Syntax

`lanport <poe|ep> <get|auto|autohdx|autofdx|10hdx|10fdx|100hdx|100fdx|1000hdx|1000fdx>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `auto\|autohdx\|autofdx\|10hdx\|10fdx\|100hdx\|100fdx\|1000hdx\|1000fdx` | Sets the LAN speed and duplex mode. This parameter is not allowed while in a call.<br>• `auto`: Automatically negotiates the LAN speed and duplex mode<br>• `autohdx`: Automatically negotiates the LAN speed but specifies half-duplex mode<br>• `autofdx`: Automatically negotiates the LAN speed but specifies full-duplex mode<br>• `10hdx`: 10 Mbps, half duplex<br>• `10fdx`: 10 Mbps, full duplex<br>• `100hdx`: 100 Mbps, half duplex<br>• `100fdx`: 100 Mbps, full duplex<br>• `1000hdx`: 1000 Mbps, half duplex<br>• `1000fdx`: 1000 Mbps, full duplex | | |

### Feedback Examples

- `lanport epauto`

  returns

  `lanport auto`

  `restart system for changes to take effect. restart now? <y,n>`

- `lanport poe get`

  returns

  `lanport auto`

### Comments

After making a change, you are prompted to restart the system.

## mtumode

Sets or gets the MTU mode. The `mtumode` and `mtusize` commands allow you to change the Maximum Transmission Unit (MTU) size, to adjust for the best interoperability with the host network. Set mtumode to `specify`, then use `mtusize` to specify a value. If mtumode is set to `default`, the system automatically sets the MTU value to 1260.

### Syntax

`mtumode <get|default|specify>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `default` | Sets the Maximum Transmission Unit size to the default value of 1260 | | |
| `specify` | Specify a Maximum Transmission Unit size other than the default setting | | |

### Feedback Examples

- `mtumode default`

  returns

  `mtumode default`
- `mtumode specify`

  returns

  `mtumode specify`
- `mtumode get`

  returns

  `mtumode specify`
- `mtusize 660`

  returns

  `mtusize 660`
- `mtumode foo`

  returns

  `error: command has illegal parameters`

## mtusize

Sets or gets the MTU size. The `mtumode` and `mtusize` commands allow you to change the Maximum Transmission Unit (MTU) size, to adjust for the best interoperability with the host network. Set mtumode to `specify`, then use `mtusize` to specify a value. If mtumode is set to `default`, the system automatically sets the MTU value to 1260.

### Syntax

`mtusize <get|660|780|900|1020|1140|1260|1500>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `660\|780\|900\|1020\|1140\|1260\|1500` | Sets the value of the Maximum Transmission Unit size | | |

### Feedback Examples

- `mtumode specify`

  returns

  `mtumode specify`
- `mtusize 660`

  returns

  `mtusize 660`
- `mtusize 1140`

  returns

  `mtusize 1140`
- `mtusize get`

  returns

  `mtusize 1140`

## natconfig

Sets or gets the NAT configuration.

### Syntax

`natconfig <get|auto|manual|off>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `auto` | Specifies that the system is behind a NAT and specifies that the system will automatically discover the public (WAN) address | | |
| `manual` | Specifies that the system is behind a NAT. Requires the WAN address to be assigned using the wanipaddress command. | | |
| `off` | Disables the option when the system is not behind a NAT | | |

### Feedback Examples

- `natconfig auto`

  returns

  `natconfig auto`
- `natconfig manual`

  returns

  `natconfig manual`
- `natconfig off`

  returns

  `natconfig off`
- `natconfig get`

  returns

  `natconfig off`

## ntpmode

Sets or gets the mode of the system's Network Time Protocol (NTP) server. NTP server time is used to ensure synchronized time data in the local Call Detail Report.

### Syntax

`ntpmode <get|auto|off|manual>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current time server mode | Yes | |
| `auto` | Automatically selects an NTP server from the Internet | | |
| `off` | Turns off the use of an NTP server | | |
| `manual` | Lets you specify a server using the `ntpserver` command | | |

### Feedback Examples

- `ntpmode auto`

  returns

  `ntpmode auto`
- `ntpmode off`

  returns

  `ntpmode off`

- `ntpmode manual`

  returns

  `ntpmode manual`
- `ntpmode get`

  returns

  `ntpmode manual`

## ntpsecondaryserver

Sets or gets a secondary Network Time Protocol (NTP) server using the IP address or DNS name of the server.

### Syntax

```
ntpsecondaryserver get
ntpsecondaryserver set ["xxx.xxx.xxx.xxx"|"server name"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Gets the IP address of the secondary NTP server | Yes | |
| `set` | Sets the IP address of the secondary NTP server when followed by a valid parameter. To erase the current setting, omit the `["xxx.xxx.xxx.xxx"\|"servername"]` parameter. | | |
| `"xxx.xxx.xxx.xxx"` | IP address of the secondary NTP server | | |
| `manual` | DNS name of the secondary NTP server | | |

### Feedback Examples

- `ntpsecondaryserver set`

  returns

  `ntpsecondaryserver <empty>`
- `ntpsecondaryserver set 172.26.44.22`

  returns

  `ntpsecondaryserver 172.26.44.22`
- `ntpsecondaryserver get`

  returns

  `ntpsecondaryserver 172.26.44.22`

### Comments

The primary NTP server must be configured in order to configure the secondary NTP server.

### See Also

See the ntpserver command.

## ntpserver

Sets or gets an Network Time Protocol (NTP) server, using the IP address or the DNS name of the server.

### Syntax

```
ntpserver get
ntpserver set [“xxx.xxx.xxx.xxx”|“server name”]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Gets the IP address of the NTP server | Yes | |
| `set` | Sets the IP address of the NTP server when followed by a valid parameter. To erase the current setting, omit the `["xxx.xxx.xxx.xxx"\|"servername"]` parameter. | | |
| `"xxx.xxx.xxx.xxx"` | The IP address of the NTP server | | |
| `manual` | The DNS name of the NTP server | | |

### Feedback Examples

- `ntpserver set`

  returns

  `ntpserver <empty>`
- `ntpserver set 192.168.1.205`

  returns

  `ntpserver 192.168.1.205`
- `ntpserver get`

  returns

  `ntpserver 192.168.1.205`

### Comments

This command allows you to use an internal time server and thus synchronize the system’s time with the time on your internal network. The system uses this time only for the local Call Detail Report.

## pricallbycall

Sets or gets the PRI call-by-call value. This command is only applicable if the ISDN interface is set to PRI.

### Syntax

```
pricallbycall get
```

```
pricallbycall set {0..31}
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets PRI call-by-call when followed by a value from `{0..31}` | | |
| `{0..31}` | Range of call-by-call values | | |

### Feedback Examples

- `pricallbycall set 1`

  returns

  `pricallbycall 1`
- `pricallbycall get`

  returns

  `pricallbycall 1`

### Comments

Call-by-call is a number from 0 to 31, which is optionally sent to an upstream telephone company switch, if required. For example, specify a value of 6 for a T1 PRI network interface module that is directly connected to an ATT 5ESS switch, which is provisioned with Accunet. You must consult with the telephone company service provider to determine whether a call-by-call value is required for a particular PRI line. For most cases, the default value of 0 is correct. Always use the value 0 when connected to a PBX. A non-zero value should not be required in Europe. Values greater than 31 are reserved for internal use and must not be used.

## prichannel

Sets or gets the PRI channels that will be active for the PRI line. This command is only applicable if the ISDN interface is set to PRI.

### Syntax

```
prichannel get all
prichannel get {n}
prichannel set all
prichannel set {n} <on|off>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current status of the channel number if is on or off | Yes | |
| `set` | Enables the status of the specified PRI channel | | |
| `n` | The number of the specified channel. The range for T1 is `0 to 23` and E1 range is `0 to 32`. | | |

## Feedback Examples

- `prichannel set 1 on`

  returns

  `prichannel 1 on`
- `prichannel set 23 off`

  returns

  `prichannel 23 off`
- `prichannel get 23`

  returns

  `prichannel 23 off`

## Important PRI Channel Information

For an outgoing call, the Polycom ISDN Gateway uses the first active and available channel starting with the lowest number from the channel range (1-23 for a PRI T1 and 1-30 for a PRI E1). If an additional channel is needed, the system chooses the next incremental number. For example, if channels 1 through 7 are inactive, but 8 is active and available, then 8 is the first channel that can be used by the system to place an outgoing call. If an additional channel is needed, the system will use the next available active channel in the range (which could be 9, and so on).

For incoming calls, the system may use the highest numbered channel in the range and, if needed, proceed to the next channel number in descending order, depending on the type of third-party equipment attached to the system. For example, an incoming call arrives on channel 23, then 22, 21, and so on.

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting. Requires a parameter from `<all\|{1..n}>.all`. Selects all PRI channels and returns all channels and settings, similar to `briallenable.{1..n}` range of available PRI channels. For PRI T1, the range is 1-23. For PRI E1, the range is 1-30. | Yes | |
| `set` | Sets the PRI channels to be active when followed by a parameter from `<all\|{1..n}>` and from `<on\|off>` | | |
| `on` | Activates the selected PRI channels | | |
| `off` | Disables the selected PRI channels | | |

**Dedicated full PRI T1 or E1 Line**: All channels should be active for a full T1 or E1 line dedicated to your system.

**Fractional PRI T1 or E1**: Channel selection should be handled by your PRI network administrator.

**PRI E1 Channel Information**: The PRI Status screen (for E1) shows 30 channels. However, E1 trunk lines have 32 timeslots, numbered 0 - 31. Timeslot 0 is used for framing, and timeslot 16 is used for call signaling (the D channel). The remaining 30 timeslots are used as bearer (data) channels. In call signaling between our equipment and the switch, these channels are numbered 1-15, 17-31. But the PRI Status screen

numbers these channels contiguously in the range 1-30. Therefore, on the PRI Status screen, channels 1-15 control the status of timeslots 1-15, and channels 16-30 control the status of timeslots 17-31.

## pridialchannels

Sets or gets the number of PRI channels to dial in parallel. This command is only applicable if the ISDN interface is set to PRI.

### Syntax

```
pridialchannels get
pridialchannels set {1..n}
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current number of channels dialed in parallel. `{1..n}`. To erase the current setting, omit the parameter. | Yes | |
| `set` | Sets the number of PRI channels to be dialed in parallel when followed by a parameter from `{1..n}` | | |
| `{1..n}` | Range of numbers of PRI channels that can be dialed in parallel. For PRI T1, the range is `1..12`. For PRI E1, the range is `1..15`. | | |

### Feedback Examples

- `pridialchannels set 3`

  returns

  `pridialchannels 3`
- `pridialchannels get`

  returns

  `pridialchannels 3`

### Comments

By default, ISDN channels are dialed three at a time. On PRI systems, you can choose the number of channels to dial in parallel.

## prilinetype

Sets or gets the PRI line type. It works only when ISDN interface is set to PRI.

### Syntax

```
prilinetype get
prilinetype <t1 | e1>
```

### Feedback Examples

- `prilinetype t1`
  returns
  `prilinetype t1`
- `prilinetype get`
  returns
  `prilinetype t1`

## isdnintlprefix

Sets or gets the ISDN international dialing prefix.

### Syntax

```
isdnintlprefix get
isdnintlprefix set ["prefix"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the PRI and BRI international dialing prefix when followed by the parameter “prefix”. To erase the current setting, omit the parameter. | | |
| `"prefix"` | Numeric string | | |

### Feedback Examples

- `isdnintlprefix set 011`
  returns
  `isdnintlprefix 011`
- `isdnintlprefix get`
  returns
  `isdnintlprefix 011`

### Comments

The international prefix defaults to 011 for North America and 00 for European countries. The default depends on the country.

## isdnoutsideline

Sets or gets the PRI and BRI number that is dialed for outside line access. This command is only applicable if the ISDN interface is set to PRI and BRI.

### Syntax

```
isdnoutsideline get
isdnoutsideline set ["outside_line"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the outside-line-access PRI and BRI number when followed by the parameter `"outside_line"`. To erase the current setting, omit the parameter. | | |
| `"outside_line"` | Numeric string. Number is provided by your network service provider | | |

### Feedback Examples

- `isdnoutsideline set 9`
  returns
  `isdnoutsideline 9`
- `isdnoutsideline get`
  returns
  `isdnoutsideline 9`

### Comments

This number is needed if your system is on a PBX.

## priswitch

Sets or gets the PRI switch.

### Syntax

```
priswitch get
priswitch  <att5ess|att4ess|norteldms|ni2>
priswitch  <net5/ctr4|nttins-1500|ts-038>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current switch protocol. | Yes | |

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `set` | Sets the PRI switch. One of the switch protocol parameters is required. | | |
| `att5ess\|att4ess\|norteldms\|ni2\|net5/ctr4\|nttins-1500\|ts-038` | Switch protocol values. For E1, net5/ctr4 is the default. net5/ctr4 is the standard ETSI protocol derived from ITU Q.931.<br>For T1, net5/ctr4 is also provided for certain Asian countries, such as Japan, Hong Kong, and Taiwan. | | |

### Feedback Examples

- `priswitch att5ess`

  returns

  `priswitch att5ess`
- `priswitch get`

  returns

  `priswitch att5ess`

### Comments

If more than one switch protocol is supported, you must find out from your telephone service provider which protocol to select. NET5/CTR4 is the default. It is the standard ETSI protocol derived from ITU Q.931. If you change the country settings, a new set of PRI switch protocols is loaded.

## reboot

Restarts the system.

### Syntax

`reboot [y|now|n]`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `y` | Restarts the system without prompting you | Yes | |
| `now` | Restarts the system without prompting you | | |
| `n` | Does not restart the system | | |

### Feedback Examples

- `reboot y`

  does not prompt the user to confirm and restarts the system with no other feedback returned
- `reboot now`

  does not prompt the user to confirm and restarts the system with no other feedback returned

- `reboot n`
  does not restart the system and returns
  enter `reboot y` or `reboot now` to initiate system reboot

### Comments

The preferred format is `reboot now`.

## resetsystem

Resets system settings, CDRs, logs, and certificates.

### Syntax

```
resetsystem [deletesystemsettings]
[deletecdr][deletelogs][deletecertificates]
```

### Feedback Examples

- `resetsystem`
  returns
  `resetsystem`
- `resetsystem deletelogs`
  returns
  `resetsystem deletelogs`
- `resetsystem deletesystemsettings`
  returns
  `resetsystem deletesystemsettings`
- `resetsystem deletecertificates`
  returns
  `resetsystem deletecertificates`

## rs232 mode

The rs232 mode command sets or gets the operational mode of the first RS-232 port.

### Syntax

```
rs232 mode <get|off|control>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current mode setting | Yes | |
| `off` | Sets the operational mode of the RS-232 port to off | | |
| `control` | Sets the RS-232 port to Control mode | | |

### Feedback Examples

- `rs232 mode control`

  returns

  `rs232 mode control`

## rs366dialing

Sets or gets RS-366 dialing. This command is only applicable if the ISDN interface is set to V.35.

### Syntax

`rs366dialing <get|yes|no>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes` | Enables RS-366 dialing | | |
| `no` | Disables RS-366 dialing | | |

### Feedback Examples

- `rs366dialing yes`

  returns

  `rs366dialing yes`
- `rs366dialing no`

  returns

  `rs366dialing no`
- `rs366dialing get`

  returns

  `rs366dialing no`

### Comments

Enable this option if you call a far-site video conferencing system from the system through the DCE connection.

Disable this option if you are using one of the following:

- DCE to dial the call
- Dedicated connection to the far site

## rt

Sets or gets the RT serial interface control signal (receive timing: clock). This command is only applicable if the ISDN interface is set to V.35.

### Syntax

```
rt <get|normal|inverted>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `normal` | Sets the signal to normal (rising edge receives data) | | |
| `inverted` | Sets the signal to inverted (falling edge receives data) | | |

### Feedback Examples

- `rt normal`
  returns
  `rt normal`
- `rt inverted`
  returns
  `rt inverted`
- `rt get`
  returns
  `rt inverted`

### Comments

The default setting is `normal`.

## rts

Sets or gets the RTS serial interface control signal (request to send). This command is only applicable if the ISDN interface is set to V.35.

### Syntax

```
rts <get|normal|inverted>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `normal` | Sets the signal to normal (high voltage is logic 1) | | |
| `inverted` | Sets the signal to inverted (low voltage is logic 1) | | |

### Feedback Examples

- `rts normal`
  returns
  `rts normal`
- `rts inverted`
  returns
  `rts inverted`
- `rts get`
  returns
  `rts inverted`

### Comments

The default setting is `normal`.

## serialnum

Returns the serial number of the system.

### Syntax

```
serialnum
```

### Feedback Examples

- `serialnum`
  returns
  `serialnum 82065205E72EC1`

## servervalidatepeercert

Enables certificate validation by specifying whether the Polycom ISDN Gateway requires a browser to present a valid certificate when it tries to connect to the web interface of the Polycom ISDN Gateway.

### Syntax

```
servervalidatepeercert get
servervalidatepeercert <yes|no>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the setting for peer certificate validation for web servers | Yes | |
| `yes` | Enables requirement for peer certificate validation for web servers | | |
| `no` | Disables requirement for peer certificate validation for web servers | | |

### Feedback Examples

- `servervalidatepeercert get`

  returns

  `servervalidatepeercert no`
- `servervalidatepeercert yes`

  returns

  `servervalidatepeercert yes`

### Comments

After making a change, you must restart the system for the setting to take effect.

## clientvalidatepeercert

Enables certificate validation by specifying whether the Polycom ISDN Gateway requires a server to present a valid certificate when it tries to connect to the server of the Polycom ISDN Gateway.

### Syntax

```
clientvalidatepeercert get
clientvalidatepeercert <yes|no>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the setting for peer certificate validation for clients | Yes | |
| `yes` | Enables requirement for peer certificate validation for clients | | |
| `no` | Disables requirement for peer certificate validation for clients | | |

### Feedback Examples

- `clientvalidatepeercert get`

  returns

  `clientvalidatepeercert no`
- `clientvalidatepeercert yes`

  returns

  `clientvalidatepeercert yes`

### Comments

After making a change, you must restart the system for the setting to take effect.

## setpassword

Sets the password for admin, auditor, and user accounts of the Polycom ISDN Gateway.

### Syntax

```
setpassword admin passwd "currentacctpasswd" "newacctpasswd"
setpassword auditor passwd "currentacctpasswd" "newacctpasswd"
setpassword userpasswd "currentacctpasswd" "newacctpasswd"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `admin` | Specifies the local admin account for Polycom ISDN Gateway | Yes | |
| `auditor` | Specifies the local auditor account for Polycom ISDN Gateway | Yes | |
| `user` | Specifies the local user account for Polycom ISDN Gateway | Yes | |
| `passwd` | Changes the password | | |
| `"currentacctpasswd"` | The current account password | | |
| `"newacctpasswd"` | The new account password | | |

### Feedback Examples

`setpassword admin passwd 123 456`

returns

`password changed`

- `setpassword admin passwd '' 456`

  returns

  `password changed`

- `setpassword admin passwd 123 ''`

  returns

  `password changed`

### Comments

If the account has no administrator/auditor/user password, enter a pair of single quotes ('') to denote an empty Password.

## snmpadmin

Sets or gets the name of the SNMP administrator.

### Syntax

```
snmpadmin get
snmpadmin set ["admin name"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the administrator name when followed by the `"admin name"` parameter. To erase the current setting, omit `"admin name"`. | | |
| `"admin name"` | Name of the SNMP administrator. Character string. Enclose the character string in quotation marks if it includes spaces. **Example**: `"John Admin"` | | |

### Feedback Examples

- `snmpadmin set`

  returns

  `error: command needs more parameters to execute successfully`
- `snmpadmin set "John Admin"`

  returns

  `snmpadmin "John Admin"`
- `snmpadmin get`

  returns

  `snmpadmin "John Admin"`

### Comments

After making a change, you must restart the system for the setting to take effect.

## snmpcommunity

Sets or gets the SNMP community name.

### Syntax

```
snmpcommunity get
snmpcommunity set ["community name"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the SNMP community name when followed by the `"community name"` parameter. To erase the current setting, omit the parameter. | | |
| `"community name"` | Name of the SNMP community. This is a character string, enclose the character string in quotation marks if it includes spaces. | | |

### Feedback Examples

- `snmpcommunity set`

  returns

  `snmpcommunity <empty>`
- `snmpcommunity set Public`

  returns

  `snmpcommunity Public`
- `snmpcommunity get`

  returns

  `snmpcommunity Public`

### Comments

After making a change, you must restart the system for the setting to take effect.

## snmplocation

Sets or gets the SNMP location name.

### Syntax

```
snmplocation get
snmplocation set["location name"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | SNMP location name. Enclose the location name in quotation marks if it includes spaces. To erase the current setting, omit the parameter. | | |

### Feedback Examples

- `snmplocation`

  returns

  `snmplocation <empty>`
- `snmplocation set “Mary_Polycom in United States”`

  returns

  `snmplocation “Mary_Polycom in United States”`
- `snmplocation get`

  returns

  `snmplocation “Mary_Polycom in United States”`

### Comments

After making a change, you must restart the system for the setting to take effect.

## snmpsystemdescription

Sets or gets the SNMP system description.

### Syntax

```
snmpsystemdescription get
snmpsystemdescription set ["system description"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the SNMP system description when followed by the "`system description`" parameter. To erase the current setting, omit the parameter. | | |
| "`system description`" | SNMP system description | | |

### Feedback Examples

- `snmpsystemdescription set`

  returns

  `snmpsystemdescription <empty>`
- `snmpsystemdescription set "videoconferencing system"`

  returns

  `snmpsystemdescription "videoconferencing system"`
- `snmpsystemdescription get`

  returns

  `snmpsystemdescription "videoconferencing system"`

### Comments

After making a change, you must restart the system for the setting to take effect.

## snmpengineid

Sets or gets the SNMP engine ID.

### Syntax

```
snmpengineid get
snmpengineid set <"SNMP Engine ID">
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the SNMP system engine ID when followed by the `snmp engineid` parameter. To erase the current setting, omit the parameter “snmp engineid” SNMP snmp engineid. | | |

### Feedback examples

- `snmpengineid set`

  returns

  `snmpengineid <empty>`
- `snmpsystemdescription set 10:56:78:88:78:AA:BB:66`

  returns

  `snmpengineid “10:56:78:88:78:AA:BB:66”`
- `snmpsystemdescription get`

  returns

  `snmpengineid “10:56:78:88:78:AA:BB:66”`

### Comments

After making a change, you must restart the system for the setting to take effect.

## snmpconsoleip

Sets or gets the SNMP console IP.

### Syntax

`snmpconsoleip get <1|2|3>`

`snmpconsoleip set <1|2|3>["xxx.xxx.xxx.xxx"]`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the SNMP console IP | | |
| `<1\|2\|3>` | Sets the 1,2,3 SNMP console IP for SNMP | | |

### Feedback examples

- `snmpconsoleip set 1`
  returns
  `snmpconsoleip 1 <empty>`
- `snmpconsoleip set 1 192.168.1.1111`
  returns
  `snmpconsoleip 192.168.1.1111`
- `snmpconsoleip get 1 192.168.1.1111`
  returns
  `snmpconsoleip 1 192.168.1.1111`

### Comments

After making a change, you must restart the system for the setting to take effect.

## snmptrapversion

Sets or gets the SNMP trap version.

### Syntax

`snmptrapversion get`

snmpconsoleip set <v1|v2c|v3> `<true|false>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the SNMP version v1, v2c, v3 | | |
| `<1\|2\|3>` | Sets the SNMP version v1, v2c, v3 to true or false | | |

### Feedback examples

- `snmptrapversion set v1 true`
  returns
  `snmpconsoleip v1 true`
- `snmptrapversion set v2c true`
  returns
  `snmpconsoleip v2c true`
- `snmptrapversion get`
  returns
  `snmptrapversion v2c`
  `snmptrapversion v1`

### Comments

After making a change, you must restart the system for the setting to take effect.

## st

Sets or gets the st serial interface control signal (send timing: clock) setting. This command is only applicable if the ISDN interface is set to V.35.

### Syntax

`st <get|normal|inverted>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `normal` | Sets the signal to normal (falling edge sends data) | | |
| `inverted` | Sets the signal to inverted (rising edge sends data) | | |

### Feedback Examples

- `st normal`
  returns
  `st normal`
- `st inverted`
  returns
  `st inverted`
- `st get`
  returns
  `st inverted`

### Comments

The default setting is "normal".

## subnetmask

Sets or gets the subnet mask of the system.

### Syntax

```
subnetmask get
subnetmask set ["xxx.xxx.xxx.xxx"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| get | Returns the current setting | Yes | |
| set | Sets the subnet mask of the system when followed by the "xxx.xxx.xxx.xxx" parameter. To erase the current setting, omit "xxx.xxx.xxx.xxx". This parameter is not allowed while in a call. | | |
| "xxx.xxx.xxx.xxx" | Subnet mask of the system | | |

### Feedback Examples

- `subnetmask set 255.255.255.0`

  returns

  `subnetmask 255.255.255.0`

- `subnetmask get`

  returns

  `subnetmask 255.255.255.0`

### Comments

After making a change, you must restart the system for the setting to take effect.

## systemname

Sets or gets the name of the system.

### Syntax

```
systemname get
systemname set "system name"
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `set` | Sets the system name to "`system name`" | | |
| "`system name`" | Character string specifying the system name. Enclose the string in quotation marks if it includes spaces. Example: "`Polycom ISDN Gateway`" | | |

### Feedback Examples

- `systemname set "Polycom ISDN Gateway"`

  returns

  `systemname "Polycom ISDN Gateway"`
- `systemname  get`

  returns

  `systemname "Polycom SDN Gateway"`

### Comments

In the system name, the first character must be a numeric (a digit) or an alphabetic (a letter) character including foreign language characters. The system name must not be blank; can be any combination of alphanumeric characters and can be up to 30 characters in length.

## systemsetting telnetenabled

Sets or gets the telnet ports.

### Syntax

```
systemsetting telnetenabled <true|false>
systemsetting get telnetenabled
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `true` | Enables port 23 and port 24 | | |
| `false` | Disables port 23 and port 24 | | |

### Feedback Examples

- `systemsetting telnetenabled true`

  returns

  `systemsetting telnetenabled true`

- `systemsetting get telnetenabled`

  returns

  `systemsetting telnetenabled true`

### Comments

After making a change, you must restart the system for the setting to take effect. If a security profile is enabled on the system, you cannot activate telnet ports.

## systemsetting sshenabled

Sets or gets the status of SSH ports.

### Syntax

```
systemsetting sshenabled <true|false>
systemsetting get sshenabled
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `true` | Enables port 23 and port 24 | | |
| `false` | Disables port 23 and port 24 | | |

### Feedback Examples

- `systemsetting sshenabled true`

  returns

  `systemsetting sshenabled true`

- `systemsetting get sshenabled`

  returns

  `systemsetting sshenabled true`

### Comments

After making a change, you must restart the system for the setting to take effect. If a security profile is enabled on the system, you cannot activate SSH ports.

## systemsetting webenabled

Specifies if remote access to the system using the web interface must be allowed.

### Syntax

```
systemsetting webenabled <True|False>
systemsetting get webenabled
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `True` | Enables remote access from the web interface | Yes | |
| `False` | Disables remote access from the web interface | | |
| `get` | Returns the current setting | | |

### Feedback Examples

- `systemsetting webenabled True`
  returns
  `systemsetting webenabled True`
- `systemsetting get webenabled`
  returns
  `systemsetting webenabled True`

## tcpports

Sets or gets the TCP ports on the system.

### Syntax

```
tcpports get
tcpports set [{1024..49150}]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current TCP port setting | Yes | |
| `set` | Sets the TCP ports when followed by a value from the range `{1024..49150}`. To erase the current setting, omit the value. This parameter is not allowed while in a call. | | |

### Feedback Examples

- `tcpports set 3233`
  returns
  `tcpports 3233`
- `tcpports get`
  returns
  `tcpports 3233`

### Comments

The **Fixed Ports** option on the Firewall screen must be selected for the **TCP Ports** option to be available.

## typeofservice

Sets or gets the type of service for Quality of Service.

### Syntax

```
typeofservice <get|ipprecedence|diffserv>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `ipprecedence` | Selects IP precedence service | | |
| `diffserv` | Selects DiffServ service | | |

### Feedback Examples

- `typeofservice diffserv`
  returns
  `typeofservice diffserv`
- `typeofservice ipprecedence`
  returns
  `typeofservice ipprecedence`
- `typeofservice get`
  returns either
  `typeofservice ipprecedence`
  or
  `typeofservice diffserv`

## udpports

Sets or gets the UDP ports on the system.

### Syntax

```
udpports get
udpports set [{1024..49150}]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current UDP port setting | Yes | |
| `set` | Sets the UDP ports when followed by a value from the range `{1024..49150}`. To erase the current setting, omit the value. This parameter is not allowed while in a call. | | |

### Feedback Examples

- `udpports set 3230`

  returns

  `udpports 3230`
- `udpports get`

  returns

  `udpports 3230`

### Comments

The **Fixed Ports** option on the Firewall screen must be selected for the **UDP Ports** option to be available.

## updatefactory

Update the factory image of the Polycom ISDN Gateway when a USB storage device is plugged into the device.

### Syntax

`updatefactory`

### Feedback Examples

- `updatefactory`

### Comments

After running this command, navigate to /var/log/messages to ensure that the factory image has been updated successfully.

## usefixedports

Sets or gets the Fixed Ports configuration.

### Syntax

`usefixedports <get|yes|no>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes` | Enables the use of Fixed Ports | | |
| `no` | Disables the use of Fixed Ports | | |

### Feedback Examples

- `usefixedports yes`

  returns

  `usefixedports yes`
- `usefixedports no`

  returns

  `usefixedports no`
- `usefixedports get`

  returns

  `usefixedports no`

## usegatekeeper

Sets or gets the gatekeeper mode.

### Syntax

`usegatekeeper <get|off|specify|auto>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting<br>**Note**: A gatekeeper is not required to make IP-to-IP LAN calls. In these situations, select the `off` option. | Yes | |
| `off` | Select this option if no gatekeeper is required or if you make IP-to-IP LAN calls. | | |
| `specify` | Specifies a gatekeeper. If this option is selected, you must enter the gatekeeper IP address or name using the gatekeeperip command. | | |
| `auto` | Sets the system to automatically find an available gatekeeper | | |

### Feedback Examples

- `usegatekeeper off`

  returns

  `usegatekeeper off`
- usegatekeeper specify

  returns

  `usegatekeeper specify`
- `usegatekeeper auto`

  returns

  `usegatekeeper auto`

- `usegatekeeper get`

  returns

  `usegatekeeper auto`

## v35broadcastmode

Sets or gets the V.35 broadcast mode. This command is only applicable if the ISDN interface is set to V.35.

### Syntax

`v35broadcastmode <get|on|off>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `on` | Turns on V.35 broadcast. This parameter is not allowed while in a call. | | |
| `off` | Turns off V.35 broadcast. This parameter is not allowed while in a call. | | |

### Feedback Examples

- `v35broadcastmode on`

  returns

  `v35broadcastmode on`
- `v35broadcastmode off`

  returns

  `v35broadcastmode off`
- `v35broadcast get`

  returns

  `v35broadcast off`

## v35num

Sets or gets the ISDN video numbers assigned to the system. This command is only applicable if the ISDN interface is set to V.35.

### Syntax

`v35num get <1b1|1b2>`
`v35num set <1b1|1b2> ["v35 number"]`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current ISDN video number associated with a B channel of a particular line. Requires `<1b1\|1b2>` | Yes | |
| `1b1\|1b2` | B1 and B2 channels:<br>• `1b1` designates line 1, B channel 1 (B1)<br>• `1b2` designates line 1, B channel 2 (B2) | | |
| `set` | Sets the ISDN video number for a B channel line when followed by a `"v35 number"` parameter. To erase the current setting, omit the `"v35 number"` parameter. `1b1` is port 1 and `1b2` is port 2. This parameter is not allowed while in a call. | | |
| `"v35 number"` | Numeric string. This ISDN video number(s) is provided by your network service provider. | | |

### Feedback Examples

- `v35num set 1b1`

  returns

  `v35num 1b1 <empty>`
- `v35num set 1b2 7005551212`

  returns

  `v35num 1b2 7005551212`
- `v35num get 1b2`

  returns

  `v35num 1b2 7005551212`

### Comments

The `1b1` and `1b2` parameters follow the convention and nomenclature of the user interface and the isdnnum command.

## v35portsused

Sets or gets the number of ports to use on the V.35/RS-449/RS-530 network interface module.

### Syntax

`v35portsused <get|1|1+2>`

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| 1 | Selects one port for one-channel calls | | |
| 1+2 | Selects two ports for two-channel calls (2 x 56 kbps or 2 x 64 kbps) | | |

### Feedback Examples

- `v35portsused 1`
  returns
  `v35portsused 1`
- `v35portsused 1+2`
  returns
  `v35portsused 1+2`
- `v35portsused get`
  returns
  `v35portsused 1+2`

## v35prefix

Sets or gets the V.35 dialing prefix. It assumes that a profile has already been selected.

### Syntax

```
v35prefix get "valid speed"
v35prefix set "valid speed" ["value"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| get | Returns the current setting for "valid speed" | Yes | |
| set | Sets the V.35/RS-449/RS-530 prefix when followed by a "value" parameter. To erase the current setting, omit the "value" parameter. | | |
| "valid speed" | Valid speeds are 56, 64, 2x56, 112, 2x64, 128, 168, 192,224, 256, 280, 320, 336, 384, 392, 7x64, 504, 512, 560,576, 616, 640, 672, 704, 728, 768, 784, 832, 840,14x64, 952, 960, 1008, 1024, 1064, 1088, 1120, 1152,1176, 1216, 1232, 1280, 1288, 21x64, 1400, 1408,1456, 1472, 1512, 1536, 1568, 1600, 1624, 1664, 1680,1728, 28x64, 1856, 1920, all.<br>The parameter "all" lists all the available speeds and their associated dialing prefixes | | |
| "value" | V.35/RS-449/RS-530 prefix, which is a function of your DCE. Consult the DCE user guide for information | | |

### Feedback Examples

- `v35prefix set 56`

  returns

  `v35prefix 56 <empty>`

- `v35prefix set 112 ”#005”`

  returns

  `v35prefix 112 ”#005”`

  and associates the dialing prefix 005 with the speed 112

- `v35prefix get 112`

  returns

  `v35prefix 112 ”#005”`

### See Also

See the v35profile command.

## v35profile

Sets or gets a V.35 profile associated with dialing through a DCE. It can also display all the settings (speed, prefix or suffix) of the current profile.

### Syntax

```
v35profile
<get|adtran|adtran_isu512|ascend|ascend_vsx|ascend_max|avaya_mcu|
custom_1|fvc.com|initia|lucent_mcu|madge_teleos>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current profile | Yes | |
| `adtran\|adtran_isu512\|ascend\|ascend_vsx\|ascend_max\|avaya_mcu\|custom_1\|fvc.com\|initia\|lucent_mcu\|madge_teleos` | V.35/RS-449/RS-530 profile (equipment/manufacturer) available<br>Consult your DCE user guide for additional information on setting dialing profiles. | | |

### Feedback Examples

- `v35profile adtran_isu512`

  returns

  `v35profile adtran_isu512`

  and selects adtran_isu512 as the profile

- `v35profile get`

  returns

  `v35profile adtran_isu512`

# v35suffix

Sets or gets the V.35 dialing suffix. It assumes that a profile has already been selected.

## Syntax

```
v35suffix get "valid speed"
v35suffix set "valid speed" ["value"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting for `"valid speed"` | Yes | |
| `set` | Sets the V.35/RS-449/RS-530 suffix when followed by a `"value"` parameter. To erase the current setting, omit the `"value"` parameter. | | |
| `"valid speed"` | Valid speeds are 56, 64, 2x56, 112, 2x64, 128, 168, 192,224, 256, 280, 320, 336, 384, 392, 7x64, 504, 512, 560,576, 616, 640, 672, 704, 728, 768, 784, 832, 840,14x64, 952, 960, 1008, 1024, 1064, 1088, 1120, 1152,1176, 1216, 1232, 1280, 1288, 21x64, 1400, 1408,1456, 1472, 1512, 1536, 1568, 1600, 1624, 1664, 1680,1728, 28x64, 1856, 1920, all. The parameter `"all"` lists all the available speeds and their associated dialing prefixes. | | |
| `"value"` | V.35/RS-449/RS-530 suffix, which is a function of your DCE<br>Refer to the DCE user guide for information. | | |

## Feedback Examples

- `v35suffix set 128`

  returns

  `v35suffix 128 <empty>`
- `v35suffix set 128 "#4#2"`

  returns

  `v35suffix 128 #4#2`

  and associates the dialing suffix #4#2 with the speed 128
- `v35suffix get 128`

  returns

  `v35suffix 128 #4#2`

## See Also

See the v35profile command.

## wanipaddress

Sets or gets the WAN IP address.

### Syntax

```
wanipaddress get
wanipaddress set ["xxx.xxx.xxx.xxx"]
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the WAN IP address | Yes | |
| `set` | Sets the WAN IP address when followed by the "xxx.xxx.xxx.xxx" parameter. To erase the current setting, omit the "xxx.xxx.xxx.xxx" parameter. | | |
| "xxx.xxx.xxx.xxx" | WAN IP address | | |

### Feedback Examples

- `wanipaddress set 192.168.1.101`

  returns

  `wanipaddress 192.168.1.101`

- `wanipaddress get`

  returns

  `wanipaddress 192.168.1.101`

### Comments

The **NAT Configuration** option on the Firewall screen must be set to **Auto**, **Manual** for this option to be available.

## whitelistenabled

Enables or disables the ability to restrict a Polycom ISDN Gateway's access to only those systems with IP addresses that match one of the addresses or patterns specified in the whitelist.

### Syntax

```
whitelistenabled get
whitelistenabled <yes|no>
```

| Parameter | Description | User Accessible | Additional Restrictions |
|---|---|---|---|
| `get` | Returns the current setting | Yes | |
| `yes` | Allows the Polycom ISDN Gateway to access only those systems with IP addresses that match one of the addresses or patterns specified in the whitelist | | |
| `no` | Allows the Polycom ISDN Gateway to access systems with IP addresses that are not specified in the whitelist | | |

### Feedback Examples

- `whitelistenabled get`

  returns

  `whitelistenabled no`
- `whitelistenabled yes`

  returns

  `whitelistenabled yes`

### Comments

The system will restart when the `whitelistenabled` setting is modified.

## whoami

Displays the same initial banner information as when the RS-232/Telnet session was started with the system.

### Syntax

`whoami`

## Feedback Examples

- `whoami`

  returns

```
Hi, my name is: Polycom ISDN GW
Here is what I know about myself:
Model: ISDN GW
Serial Number: ISDNA11509010003
Software Version: Alpha - 1.0.16-dev
Build Information: unknown
SNTP Time Service: Manual oosync 0.0.0.0
Local Time is: Wed, 06 Jan 2016 15:16:32
Network Interface: UNKNOWN
IP Number: 10.97.54.67
Link-Local Address: fe80::4655:4dff:fe00:5/64
Global Address: 2001:df0:8800:54:4655:4dff:fe00:5/64
ISDN Video Number: 91.9991004
H323 Enabled: True
H320 Enabled: False
HTTP Enabled: True
SNMP Enabled: True
```

## Comments

The response can vary depending on your system configuration.

# Troubleshooting

You can find information about troubleshooting the Polycom ISDN Gateway in the following topics:


- General Troubleshooting
- System Information, Status and Diagnostics Information
- System Logging
- Perform a Factory Restore
- Polycom Technical Support


## General Troubleshooting

The following table provides general troubleshooting information, including symptoms, problems and possible solutions.

### Unable to perform the software update

If you are not able to perform the software update, try the following:

- Ensure that the correct pup file is downloaded is correct (the pup file size is approximately 150 MB).
- Look at Boot LED, the LED will blink slow during software download, and the Boot LED should blink fast when the update has begun.
- Ensure that the Polycom ISDN Gateway Web UI page is not refreshed during software update process. If the web page is refreshed, then please check the following:
  - Look at BOOT LED, if the BOOT LED is blinking, this implies that the software update is in progress.
  - If the BOOT LED is stable, this implies that the software is successfully updated.
  - Check the software release version on the Polycom ISDN Gateway **System Info** page. Collect the logs and report to the Polycom ISDN Gateway team in case of any issues.
- The Polycom ISDN Gateway should not be rebooted during software update process. Performing a reboot during could lead to unsuccessful software update.
  - Check the release version on the Polycom ISDN Gateway **System Info** page.
- If the software download fails during software update, check the LAN connections of ISDN Gateway device and retry the software update process.

### Unable to establish an IP connection

If you are not able to establish an IP connection, try the following:

- Connect via a serial connection and check the IP address of the Polycom ISDN Gateway using command `ipaddress get`
- If the Polycom ISDN Gateway does not have an IP address, execute `dhcp client` command to obtain an IP address automatically through DHCP server.
- Reboot the Polycom ISDN Gateway.
- Check the IP address of the Polycom ISDN Gateway and verify that the other IP devices are on the same network.
- Check LINK LED is green, this implies that both the LAN interface and the ISDN interface are enabled and active.

## Unable to Dial a Call Using the Polycom ISDN Gateway

If you are not able to dial any calls using the Polycom ISDN Gateway, ensure the following:

- Check LINK LED is green, this will ensure that both the LAN interface and the ISDN interface are enabled and active.
- If BRI interface is selected, ensure that all BRI line interfaces are enabled in the Polycom ISDN Gateway configuration web page.
- If PRI interface is selected, ensure that all PRI channels are T1/E1 are enabled in the Polycom ISDN Gateway configuration web page.
- If V.35 interface is selected, check the following:
  - Ensure that the V.35 cables are connected in proper sequence. V.35 port1 cable should be connected to V.35 interface of the Inverse Multiplexer, and the V.35 port2 cable should be connected to other interface on the Inverse Multiplexer.
  - Ensure that the V.35 interface and RS-366 dialing should be enabled on Inverse Multiplexer and the Polycom ISDN Gateway.
  - The appropriate dialing profile should be selected as per the Inverse Multiplexer for making calls.
  - Ensure that channels are enabled for ISDN cables connected to Inverse Multiplexer for connecting the calls through the ISDN switch.
- In the Polycom ISDN Gateway web interface, verify the **PRI/BRI/V.35** interface in **System status**. If PRI/BRI/V.35 (ports) interface are RED, reboot the Polycom ISDN Gateway.

# System Information, Status and Diagnostics Information

This section has details about status and diagnostic information.

## Access the Status Screen

The Status screen includes details about system status.

### To access the Status screen:

» Go to **Admin Settings > Diagnostics > System.**

This screen includes the following system diagnostic details:

| Diagnostics Screen | Description |
|---|---|
| **System Status** | Displays the following system status information:<br>• IP Network<br>• Gatekeeper<br>• Log Threshold<br>• PRI<br>• BRI<br>• V.35<br>• Time Server<br>• Provisioning Service<br>• Temperature |
| **Download Logs** | Allows you to save system log information |
| **System Log Settings** | • Specifies the Log Level to use<br>• Enables Remote Logging, H.323 Trace and ISDN Trace<br>• Specifies the Remote Log Server Address<br>• Allows you to send diagnostics and usage data to Polycom, and get information about the Polycom Improvement Program |
| **Restart System** | Restarts the system |
| **Sessions** | View information about remote sessions connected to the Polycom ISDN Gateway |

# System Logging

System log files are essential when troubleshooting system issues. System log files contain information about system activities and the system configuration profile.

To set up system logging, you must perform the following tasks:

- Configure System Log Management
- Configure System Log Level and Remote Logging

After setting up system logging, you can retrieve a system log file. For details, refer to Download System Log Files.

## Configure System Log Management

When the system log fills up past the threshold, the following actions are triggered:

- Transfers the log to the USB device if Transfer Frequency is set to “Auto at Threshold”
- Creates a log entry indicating that the threshold has been reached
- Displays an indicator on the System Status screen

### To view the log file status:

» Go to **Diagnostics > System > System Status** and then select the **More Info** link for **Log Threshold.**

**Note:** When the Log Threshold system status indicator is red, automatic log transfers cannot be completed and data may be lost. You must manually transfer the logs to a USB device.

### To configure system log management:

1. In the web interface, go to **Admin Settings > Security > Log Management**.
2. Configure the following settings and then click **Save**.

| Setting | Description |
|---|---|
| **Current Percent Filled** | Displays how full the log file is, as a percentage of the total size |
| **Percent Filled Threshold** | Specifies a threshold for the percent filled value. Reaching the threshold triggers an alarm, creates a log entry, and transfers the log if **Transfer Frequency** is set to **Auto at Threshold**. **Off** disables logging threshold notifications. |
| **Folder Name** | Specifies the name to give the folder for log transfers. Select one of the following:<br>• **System Name and Timestamp**: Folder name is the system name and the timestamp of the log transfer, in the date and time format specified on the location screen. For example, if the system name is “Marketing”, the folder name could be `marketing_MMddyyyymmssSSS`<br>• **Timestamp**: Folder name is the timestamp of the log transfer, in the date and time format specified on the Location screen, for example `yyyyMMddhhmmssSSS`<br>• **Custom**: Optional folder name for manual log transfers |
| **Storage Type** | Specifies the type of storage device used for log file transfers. |
| **Transfer Frequency** | Specifies when the logs are transferred:<br>• **Manual**: Transfer starts when you click the **Start Log Transfer** button, which is visible only on the web interface. If the log fills before being transferred, new events overwrite the oldest events.<br>• **Auto at Threshold**: Transfer starts automatically when the Percent Filled Threshold is reached |

## Configure System Log Level and Remote Logging

The system log captures devices and server events in a consistent manner. You determine the log level, whether to enable remote logging, or to log additional H.323 details.

### To configure system log settings

1. In your web interface, click **Diagnostics > System > System Log Settings**.
2. Configure these settings and click **Save**:

| Setting | Description |
|---|---|
| **Log Level** | Sets the minimum log level of messages stored in the Polycom ISDN Gateway's flash memory<br>`DEBUG` logs all messages, and `WARNING` logs the fewest number of messages. Polycom recommends leaving this setting at the default value of `DEBUG`.<br>When **Enable Remote Logging** is on, the log level is the same for both remote and local logging. |
| **Remote Logging Enabled** | Specifies whether remote logging is enabled. Enabling this setting causes the Polycom ISDN Gateway to send each log message to the specified server in addition to logging it locally<br>The system immediately begins forwarding its log messages when you click **Save**.<br>Remote logging encryption is supported when TLS transport is the transport protocol. If you are using UDP or TCP transport, Polycom recommends remote logging only on secure, local networks. |
| **Remote Log Server** | Specifies the server address and port. If the port is not specified, a default destination port is used. The default port is determined by the configured **Remote Log Server Transport Protocol** setting as follows:<br>• UDP: 514<br>• TCP: 601<br>• TLS: 6514<br>The address and port can be specified in the following formats:<br>• **IPv4 Address** (Example: 10.11.12.13:<port>, where <port> is the optional destination port number in the range 1...65535)<br>• **IPv6 Address** (Example: [2001::abcd:1234]:<port>, where <port> is the optional destination port number in the range 1...65535)<br>• **FQDN** (Example: logserverhost.company.com:<port>, where <port> is the optional destination port number in the range 1...65535) |
| **Remote Log Server Transport Protocol** | Specifies the type of transport protocol:<br>• UDP<br>• TCP<br>• TLS (secure connection) |
| **Enable H.323 Trace** | Logs additional H.323 connectivity information |
| **Enable ISDN Trace** | Logs additional ISDN connectivity information |
| **Send Diagnostics and Usage Data to Polycom** | Sends crash log server information to Polycom to analyze and improve the product. Click the **Polycom Improvement Program** button to view information about how your data is used. |
| **Disable Logging on Console** | Provides an option to disable logs on the console. By default, this is disabled |

## Download System Log Files

You can download system log files to save system log information. Several types of log files are available that are useful for troubleshooting. The date and time of system log entries for the Polycom ISDN Gateway are shown in GMT.

### To download a system log using the web interface:

1. Click **Diagnostics > System > Download Logs**.
2. Click **Download system logs** and then specify a location on your computer to save the file.

## Download Call Detail Report (CDR)

When you enable the Call Detail Report (CDR) setting by going to **Admin Settings > General Settings > System Settings > Recent Calls** in the Polycom ISDN Gateway device's web interface, the (CDR) provides the system's call history.

Within five minutes after ending a call, the CDR is written to memory and then you can download the data in CSV format for sorting and formatting.

Every call is added to the CDR, whether it is made or received. If a call does not connect, the report shows the reason.

The size of a CDR is virtually unlimited, but can become unmanageable if you don't download the record periodically. If you consider that 150 calls result in a CDR of approximately 50 KB, you might set up a schedule to download and save the CDR after about every 1000 - 2000 calls just to keep the file easy to download and view. Remember that your connection speed also affects how fast the CDR downloads.

### To download a CDR:

1. In the web interface, click **Utilities > Services > Call Detail Report (CDR)**.
2. Click **Most Recent Call Report** and then specify whether to open or save the file on your computer.

### Information in the CDR

The following table describes the data fields in the CDR.

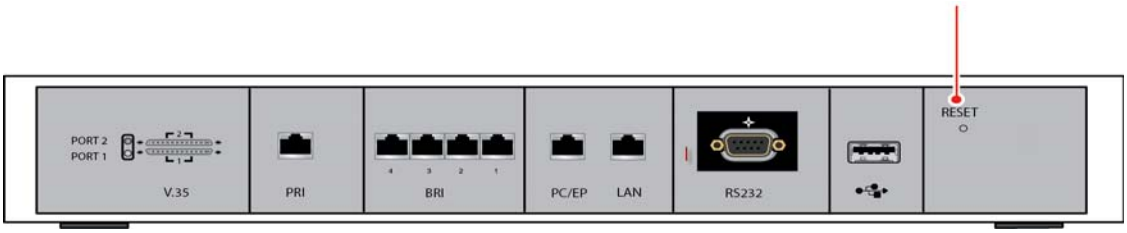
| Data | Description |
|---|---|
| Row ID | Row Index Number of generated CDR. Each call is logged on the first available row. |
| Call ID | Identifies individual calls |
| Call Direction | Indicates an ISDN to IP call or IP to ISDN call |
| Calling Number | E.164 number if the call originates from an ISDN network or an IP address (H.323 alias) if the call originates from an IP network |
| Called Number | E.164 number if the call is made to an ISDN network or an IP address (H.323 alias) if the call is made to an IP network |
| Call Duration | The length of the call in minutes and seconds |
| CDR TimeStamp | Timestamp of the generated CDR in the format dd mm yyyy hh:mm:ss |
| Start Time | The call start time, in the 24-hour format hh:mm:ss |
| Start Date | The call start date, in the format dd-mm-yyyy |
| End Date | The call end date |

| Data | Description |
|---|---|
| End Time | The call end time |
| Audio Media Type (Rx) | Type of audio codec, such as G.711, sG.722, G.728, G.722.1, Siren14 or Siren22 Stereo |
| Audio Media Type (Tx) | Type of audio codec, such as G.711, sG.722, G.728, G.722.1, Siren14 or Siren22 Stereo |
| Video Media Type (Rx) | Type of video codec, such as H.261, H.263, H.264 or H.264 Hip |
| Video Media Type (Tx) | Type of video codec, such as H.261, H.263, H.264 or H.264 Hip |
| Disconnect Reason | Indicates the reason the call was disconnected |
| Total H.320 Errors | The number of errors during an H.320 call |
| Is restricted | Indicates if the call is restricted. Call rate is in multiples of 56 kbps.<br>**Note:** The restricted state can change during the call. |
| Total H.320 Channels | Total number of ISDN B channels used in the call. For example, a 384K call would use six B channels |
| Actual Call rate | Actual call bandwidth for the current call |
| Is Down Speeded | Indicates if the connection was down speeded |

# Reset the Polycom ISDN Gateway

If the Polycom ISDN Gateway is not functioning as expected or you have forgotten the Admin Password, you can use the Reset button to reset the system.

The reset button pinhole is on the rear of the Polycom ISDN Gateway, as shown in the following figure.




### To reset the Polycom ISDN Gateway:

» When the Polycom ISDN Gateway is powered on, insert a straightened paper clip through the pinhole and press the **Reset** button.

# Perform a Factory Restore

A factory restore completely erases:

- Configuration of the Polycom ISDN Gateway and restores it to the default configuration stored in its factory partition
- Flash memory of the Polycom ISDN Gateway and reinstalls the factory software version

The factory restore resets the Polycom ISDN Gateway to default factory settings. After the factory reset, all the previous configurations, software updates, CDR data, certificates, username and passwords are lost.

**To perform a factory restore:**

» When the Polycom ISDN Gateway is powered on, insert a straightened paper clip through the pinhole and press and hold the Reset button for more than five seconds.

The factory restore takes approximately 3.5 minutes to complete. The Polycom ISDN Gateway automatically reboots when the factory reset is complete.

## Update Factory Image by USB

If you start to upgrade factory image while a USB storage device is connected, the system upgrades the factory image from the USB device.

**To upgrade factory image of the system using a USB device:**

» Copy the build package (.pup file) the root directory of a USB device.

» Run command `updatefactory` from command line interface. After running this command, navigate to /var/log/messages to ensure that the factory image has been updated successfully.

Factory image of the gateway has been upgraded successfully. To effect factory image, press **Factory Reset** button.

# Polycom Technical Support

If you cannot place calls from endpoints and you have verified that the equipment is installed and set up correctly, contact your Polycom distributor or Polycom Technical Support. To contact Polycom Technical Support, go at support.polycom.com.

Enter the following information about your Polycom ISDN Gateway, then ask a question or describe the problem. This information helps us to respond faster to your issue. In addition, please provide any diagnostic tests or troubleshooting steps that you have already tried.

- The 14-digit serial number from the System Detail screen or the back of the system.
- The software version from the System Detail screen.
- Any active alerts generated by the system.
- Information about your network.
- Troubleshooting steps you have already tried.

## Locate the System Serial Number

» In the web interface, go to **System** > **System Details**.

## Locate the Software Version

» In the web interface, go to **System** > **System Details**.

## Find Your System IP Address

» In the web interface, look on the upper left of the Home page banner, under the company logo.

## Locate the H.323 Extension Settings

» In the web interface, go to **Admin Settings> Network> IP Network**.

## Locate the LAN Status

» In the web interface, go to **Admin Settings** > **Diagnostics > Systems Status.**

## Locate Diagnostics

» In the web interface, go to **Admin Settings**> **Diagnostics**> **System**.

## Knowledge Base

For more troubleshooting information, you can search the Knowledge Base at support.polycom.com.

## Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services, and its certified Partners, to help customers successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments. UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook, Skype for Business Server 2015, and Microsoft Lync Server 2013 integrations. For additional information and details, refer to http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

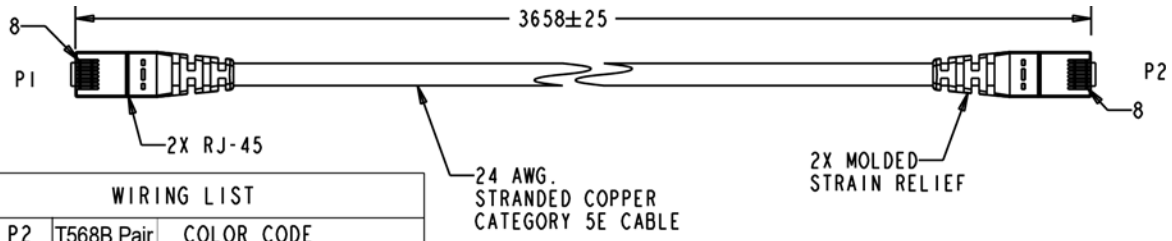
# Appendix A: Network Cables

This section includes information about cables that can be used with the Polycom ISDN Gateway. Please note that drawings and part numbers are provided for reference only. Compliance information is provided for the Restriction of certain Hazardous Substances Directive (RoHS).

## CAT 5e LAN Cable

This cable connects the Polycom ISDN Gateway to the LAN. It has orange RJ-45 connectors on both ends. It meets category 5e requirements and is wired according to EIA/TIA-568B. The maximum approved length for this cable is 328 ft (100 m) on an 802 network.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 12 ft (3.6 m) | 2457-23537-001 | Yes |

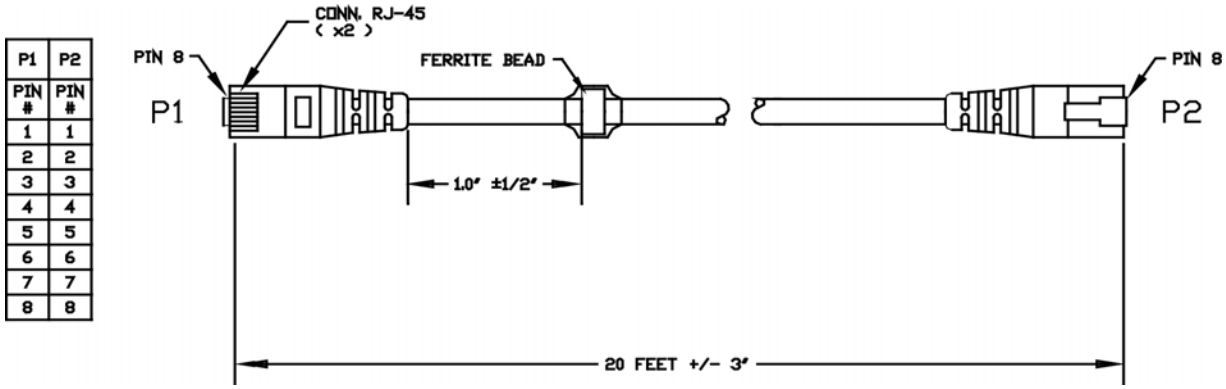



| WIRING LIST | | | |
|---|---|---|---|
| P1 | P2 | T568B Pair | COLOR CODE |
| 1 | 1 | 2 | WHITE/ORANGE |
| 2 | 2 | 2 | ORANGE |
| 3 | 3 | 3 | WHITE/GREEN |
| 4 | 4 | 1 | BLUE |
| 5 | 5 | 1 | WHITE/BLUE |
| 6 | 6 | 3 | GREEN |
| 7 | 7 | 4 | WHITE/BROWN |
| 8 | 8 | 4 | BROWN |

# ISDN Cable

This cable connects the Polycom ISDN Gateway to a BRI line. It has clear RJ-45 connectors on both ends and is used with all ISDN systems that have ISDN capability. The maximum approved length for this cable is 50 ft (15 m).

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 20 ft (6.6 m) | 2457-08548-001 | Yes |

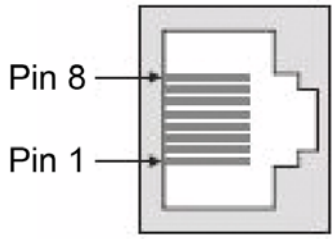



The following table describes the pin assignments for the BRI port on the Polycom ISDN Gateway.

| Pin No | Signal |
|---|---|
| 1 | No Connection |
| 2 | No Connection |
| 3 | Transmit Tip / + |
| 4 | Receive Tip / + |
| 5 | Receive Ring / - |
| 6 | Transmit Ring / - |
| 7 | No Connection |
| 8 | No Connection |

## PRI Pin Assignments

The following illustration and table show the pin assignments for the PRI port on the Polycom ISDN Gateway.



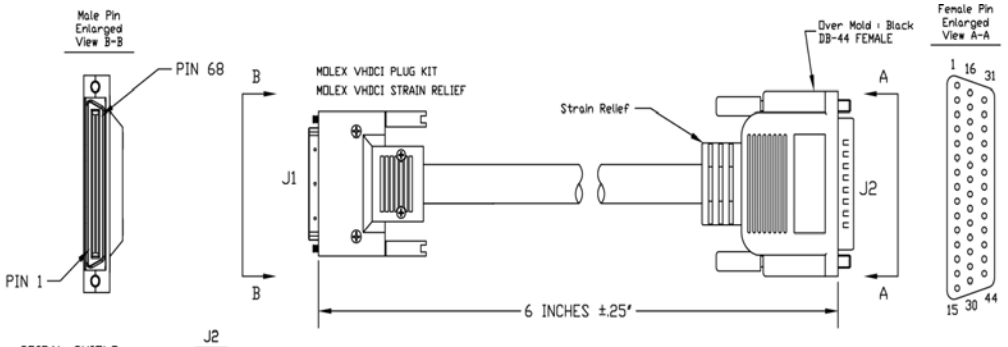

| Pin No | Signal |
|---|---|
| 1 | Receive Tip / + |
| 2 | Receive Ring / - |
| 3 | No Connection |
| 4 | Transmit Tip / + |
| 5 | Transmit Ring / - |
| 6 | No Connection |
| 7 | No Connection |
| 8 | No Connection |

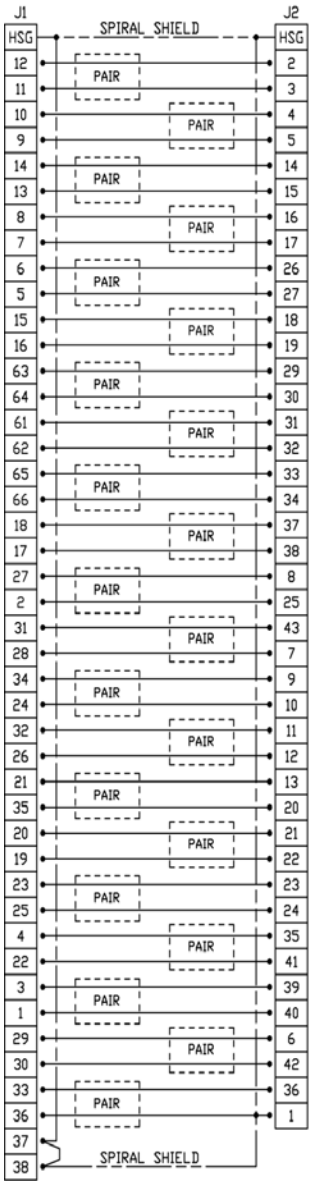
**Note:** To set up a PRI connection for your Polycom ISDN Gateway, you might need to create a PRI crossover cable using a straight cable. For details, refer to http://wiki.beronet.com/index.php/Howto_E1_/_T1_Crossover_Cable.

## V.35/RS-449/RS-530 Serial Adapter

This cable connects the Polycom ISDN Gateway to other third-party network equipment. It adapts the 68-pin interface to an industry standard 44-pin interface used by some network interface equipment.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 6 in (15.23 cm) | 2457-21264-200 | Yes |




**Peripheral Link**

**V.35 HD-68 Pinout** — **Notes (direction from V.35 module (DTE))**

| 68 pin | Signal Name | Signal Type | From card | Function | V.35 | RS530-DB25 | RS4449-DB37 | RS366-DB25 |
|---|---|---|---|---|---|---|---|---|
| | Shield | | | V.35/RS449/RS530 | A | | 19 | 7,18,19# |
| 12 | Receive Data A | Differential | in | V.35/RS449/RS530 | R | 3 | 6 | |
| 11 | Receive Data B | Differential | in | V.35/RS449/RS530 | T | 16 | 24 | |
| 10 | Send Timing A | Differential | in | V.35/RS449/RS530 | Y | 15 | 5 | |
| 9 | Send Timing B | Differential | in | V.35/RS449/RS530 | AA | 12 | 23 | |
| 29 | Data Set Ready (DSR) | Single Ended | in | V.35 | E | | | |
| 28 | Request To Send (RTS) | Single Ended | out | V.35 | C | | | |
| 27 | Data Terminal Ready (DTR) | Single Ended | out | V.35 | H | | | |
| 34 | Digit Present (DPR) | Single Ended | out | RS366 | | | | 2 |
| 24 | Abandon Call/Retry (ACR) | Single Ended | in | RS366 | | | | 3 |
| 32 | Call Request (CRQ) | Single Ended | out | RS366 | | | | 4 |
| 26 | Present Next Digit (PND) | Single Ended | in | RS366 | | | | 5 |
| 21 | Data Line Occupied (DLO) | Single Ended | in | RS366 | | | | 22 |
| 14 | Receive Timing A | Differential | in | V.35/RS449/RS530 | V | 17 | 8 | |
| 13 | Receive Timing B | Differential | in | V.35/RS449/RS530 | X | 9 | 26 | |
| 8 | Terminal Timing A | Differential | out | V.35/RS449/RS530 | U | 24 | 17 | |
| 7 | Terminal Timing B | Differential | out | V.35/RS449/RS530 | W | 11 | 35 | |
| 15 | Request To Send (RTS) A | Differential | out | RS449/RS530 | | 4 | 7 | |
| 16 | Request To Send (RTS) B | Differential | out | RS449/RS530 | | 19 | 25 | |
| 35** | Receive Common | Gnd | | RS449 | | | 20 | |
| 20 | BCD Dial Digit Bit 1 (NB1) | Single Ended | out | RS366 | | | | 14 |
| 19 | BCD Dial Digit Bit 2 (NB2) | Single Ended | out | RS366 | | | | 15 |
| 23 | BCD Dial Digit Bit 4 (NB4) | Single Ended | out | RS366 | | | | 16 |
| 25 | BCD Dial Digit Bit 8 (NB8) | Single Ended | out | RS366 | | | | 17 |
| 2** | Signal Ground | Gnd | | V.35/RS366 | B | | | 7,18,19 |
| 6 | Send Data A | Differential | out | V.35/RS449/RS530 | P | 2 | 4 | |
| 5 | Send Data B | Differential | out | V.35/RS449/RS530 | S | 14 | 22 | |
| | reserved (Ascend select line) | | | | | | | |
| 63 | Clear To Send (CTS) A | Differential | in | RS449/RS530 | | 5 | 9 | |
| 64 | Clear To Send (CTS) B | Differential | in | RS449/RS530 | | 13 | 27 | |
| 61 | Data Mode (DM-DSR) A | Differential | in | RS449/RS530 | | 6 | 11 | |
| 62 | Data Mode (DM-DSR) B | Differential | in | RS449/RS530 | | 22 | 29 | |
| 65 | Receiver Ready (RR-DCD) A | Differential | in | RS449/RS530 | | 8 | 13 | |
| 66 | Receiver Ready (RR-DCD) B | Differential | in | RS449/RS530 | | 10 | 31 | |
| 4** | Send Common | Gnd | | RS530 | | 7 | 37 | |
| 33 | Data Carrier Detect (DCD) | Single Ended | in | V.35 | F | | | |
| 18 | Terminal Ready (TR-DTR) A | Differential | out | RS449/RS530 | | 20 | 12 | |
| 17 | Terminal Ready (TR-DTR) B | Differential | out | RS449/RS530 | | 23 | 30 | |
| 3 | V.35 Cable Connected | | ground to indicate a V.35 cable is attached | | | | | 7,18,19* |
| 1 | RS449 Cable Connected | | ground to indicate a RS449 cable is attached | | | | | 7,18,19^# |
| 22 | Distant Station Connected (DSC) | Single Ended | in | RS366 | | | | 13 |
| 30 | Clear To Send (CTS) | Single Ended | in | V.35 | D | | | |
| 31 | Ring Indicate (RI) (Incoming Call | Single Ended | in | V.35/RS449 | J | | 15 | |
| | reserved (Ascend select line) | | | | | | | |
| 68 | LOS A | Differential | out | RS530 crypto | | 18 | 3 | |
| 67 | LOS B | Differential | out | RS530 crypto | | 21 | 21 | |

* For V.35, connect pin 3 of 68 pin connector to ground

^For RS449, connect pin 1 of 68 pin connector to ground

#For RS530, connect pins 1 and 3 of 68 pin connector to ground

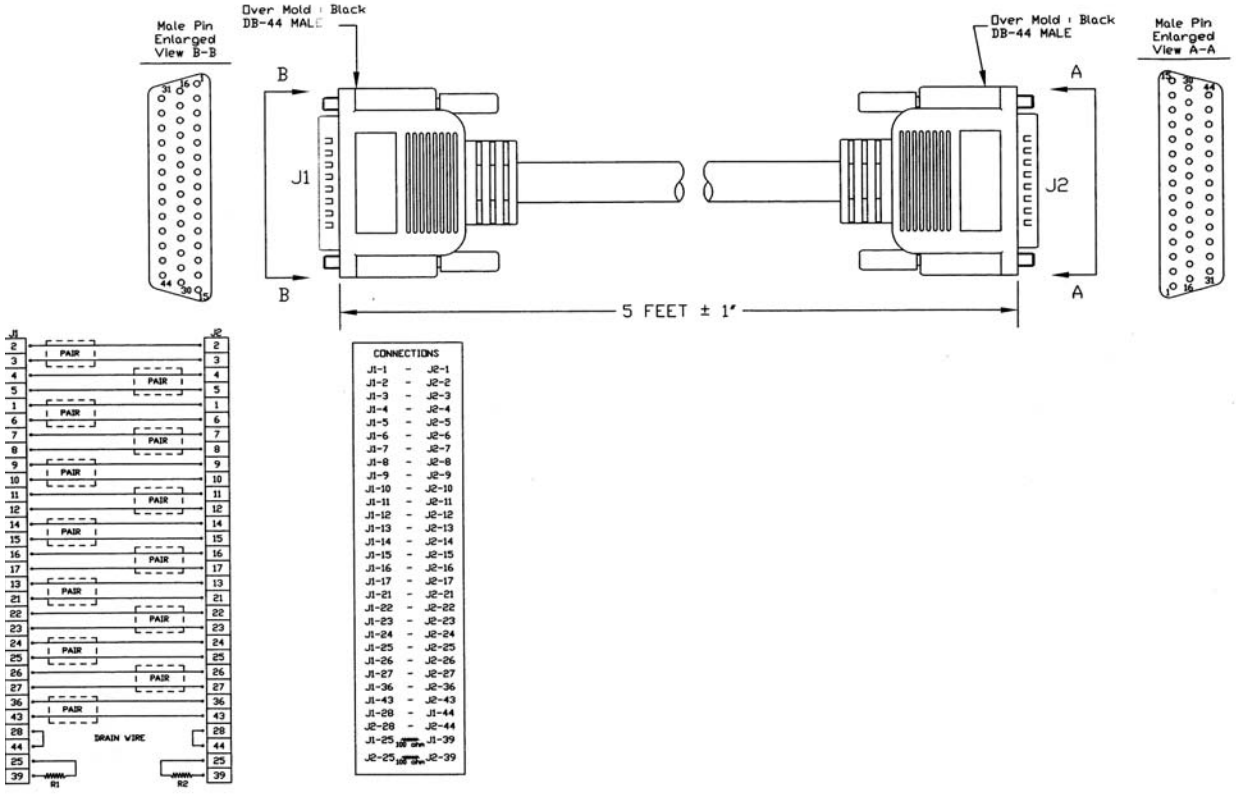
** Gnd pins are 2,4, 35-60

**Note:** Drawings and part numbers are provided for reference only. Polycom claims no responsibility or liability for the quality, performance, or reliability of cables based on these reference drawings, other than cables provided by Polycom. Contact your Polycom distributor or Polycom Custom/Vertical Products to order cables that meet the appropriate manufacturing tolerances, quality, and performance parameters for your application.

# V.35 NIC Cable

This cable connects the Polycom ISDN Gateway to Ascend network equipment. It is used with the V.35/RS-449/RS-530 Serial Adapter onto connect to network equipment that has the HD-44 pin interface. It has HD-44 M connectors on both ends and is used with ISDN systems.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 5 ft (1.65 m) | 2457-10608-200 | Yes |

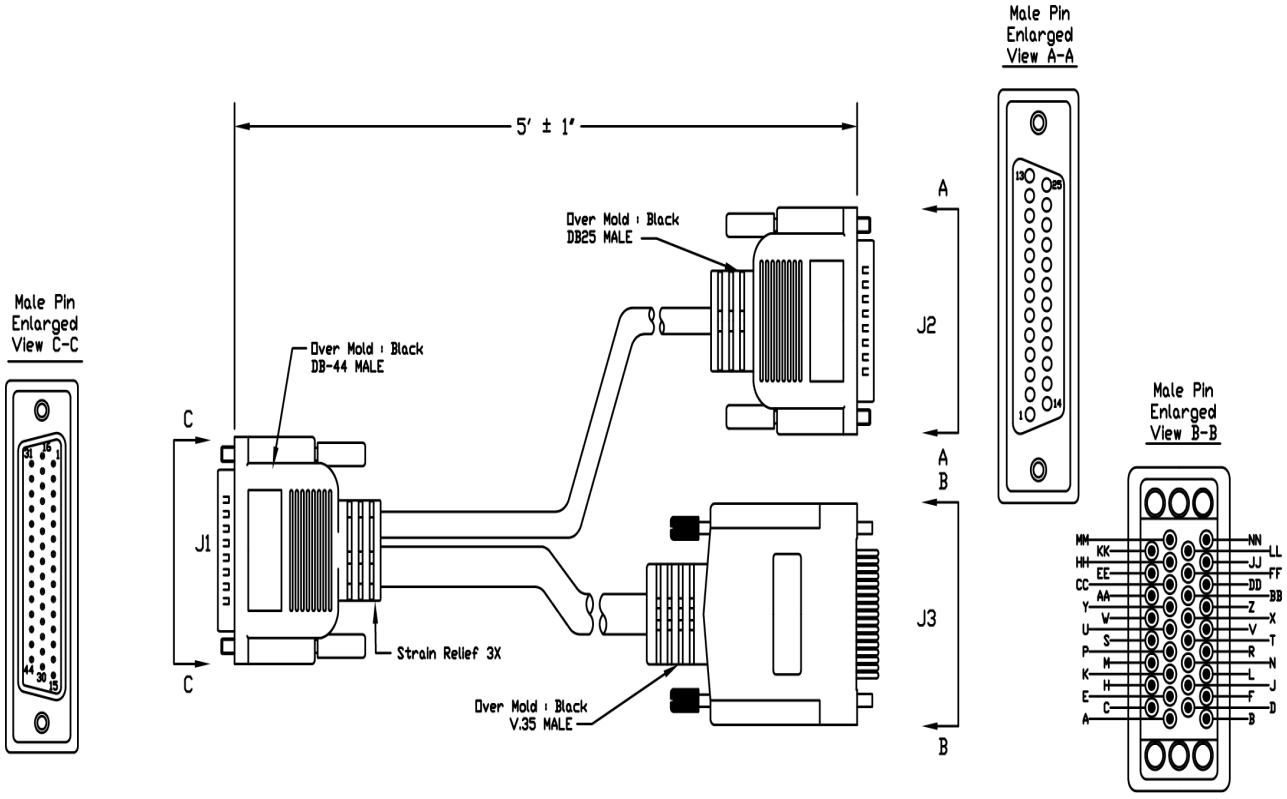


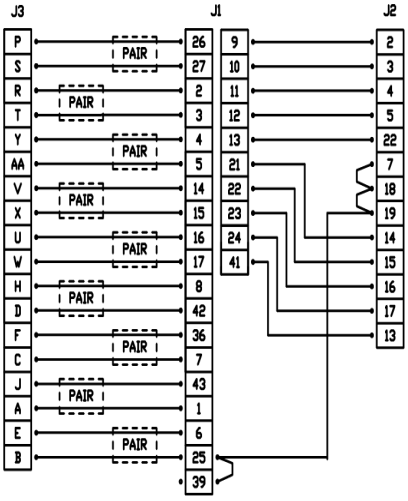

**Note:** Drawings and part numbers are provided for reference only. Polycom claims no responsibility or liability for the quality, performance, or reliability of cables based on these reference drawings, other than cables provided by Polycom. Contact your Polycom distributor or Polycom Custom/Vertical Products to order cables that meet the appropriate manufacturing tolerances, quality, and performance parameters for your application.

## V.35 and RS-366 Serial Cable

This cable connects the Polycom ISDN Gateway to third-party network equipment. It is used with the V.35/RS-449/RS-530 Serial Adapter to connect to network equipment that has a V.35/RS-366 interface. It is HD-44 M to “Y” Winchester 34M/RS-366 DB-25M and is used with ISDN systems.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 5 ft (1.65 m) | 2457-10609-200 | Yes |



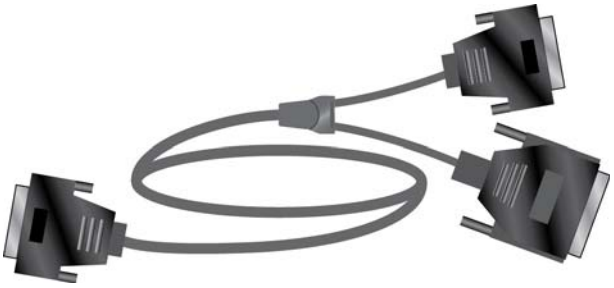




| CONNECTIONS | | |
|---|---|---|
| J1-9 | - | J2-2 |
| J1-10 | - | J2-3 |
| J1-11 | - | J2-4 |
| J1-12 | - | J2-5 |
| J1-13 | - | J2-22 |
| J1-25 | - | J2-7 |
| J1-25 | - | J2-18 |
| J1-25 | - | J2-19 |
| J1-21 | - | J2-14 |
| J1-22 | - | J2-15 |
| J1-23 | - | J2-16 |
| J1-24 | - | J2-17 |
| J1-41 | - | J2-13 |

| CONNECTIONS | | |
|---|---|---|
| J1-1 | - | J3-A |
| J1-26 | - | J3-P |
| J1-27 | - | J3-S |
| J1-2 | - | J3-R |
| J1-3 | - | J3-T |
| J1-4 | - | J3-Y |
| J1-5 | - | J3-AA |
| J1-14 | - | J3-V |
| J1-15 | - | J3-X |
| J1-16 | - | J3-U |
| J1-17 | - | J3-W |
| J1-6 | - | J3-E |
| J1-42 | - | J3-D |
| J1-36 | - | J3-F |
| J1-7 | - | J3-C |
| J1-43 | - | J3-J |
| J1-8 | - | J3-H |
| J1-25 | - | J3-B |
| J1-39 | - | J3-B |

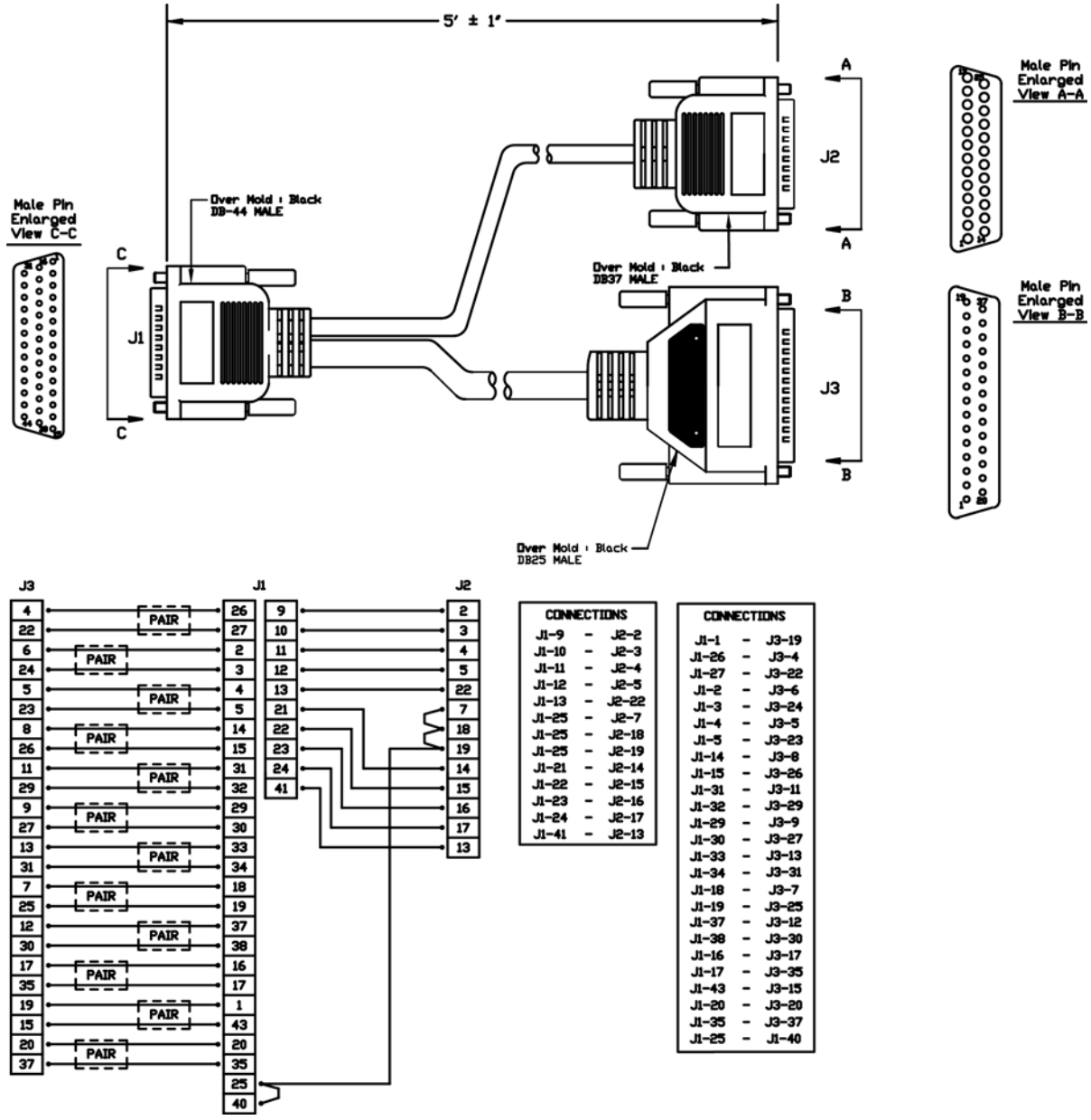
**Note:** Drawings and part numbers are provided for reference only. Polycom claims no responsibility or liability for the quality, performance, or reliability of cables based on these reference drawings, other than cables provided by Polycom. Contact your Polycom distributor or Polycom Custom/Vertical Products to order cables that meet the appropriate manufacturing tolerances, quality, and performance parameters for your application.

## RS-449 and RS-366 Serial Cable



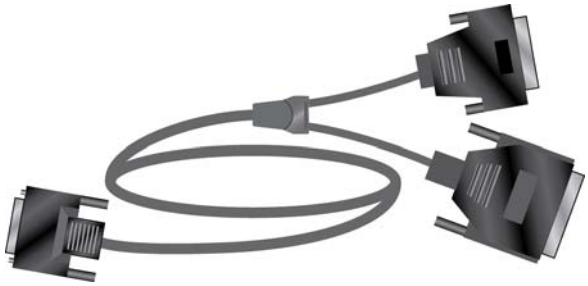
This cable connects the Polycom ISDN Gateway to third-party network equipment. It is used with the V.35/RS-449/RS-530 serial adapter to connect to network equipment that has an RS-449/RS-366 interface. It is HD-44 M to “Y” RS-449 DB-37M/RS-366 DB-25M and is used with ISDN systems.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 5 ft (1.65 m) | 2457-10610-200 | Yes |



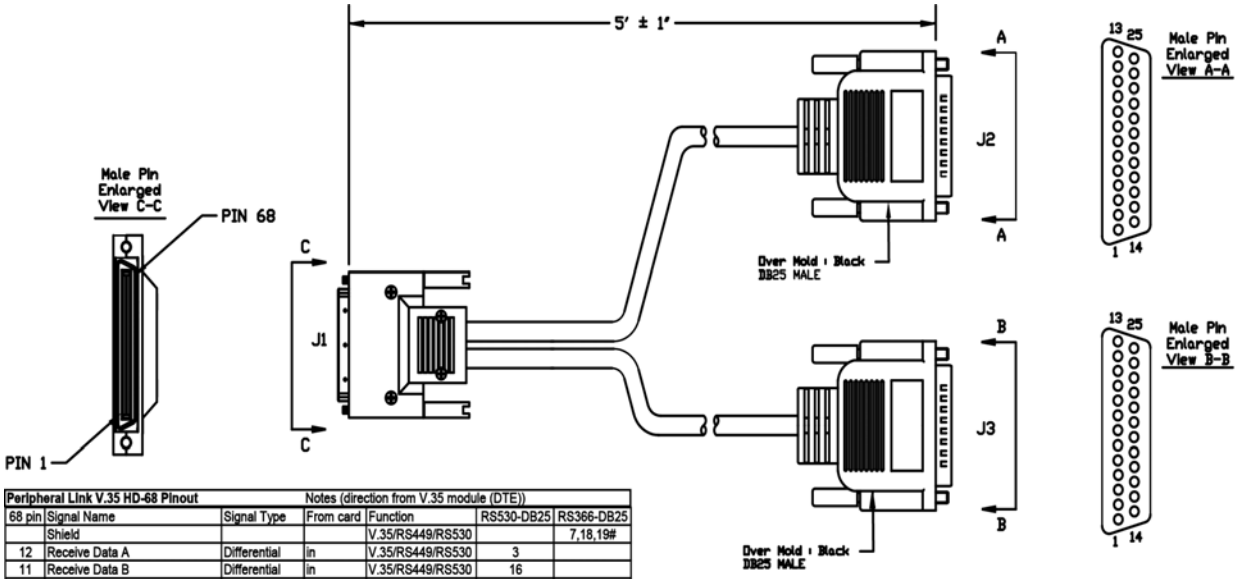

**Note:** Drawings and part numbers are provided for reference only. Polycom claims no responsibility or liability for the quality, performance, or reliability of cables based on these reference drawings, other than cables provided by Polycom. Contact your Polycom distributor or Polycom Custom/Vertical Products to order cables that meet the appropriate manufacturing tolerances, quality, and performance parameters for your application.

## RS-530 with RS-366 Serial Cable



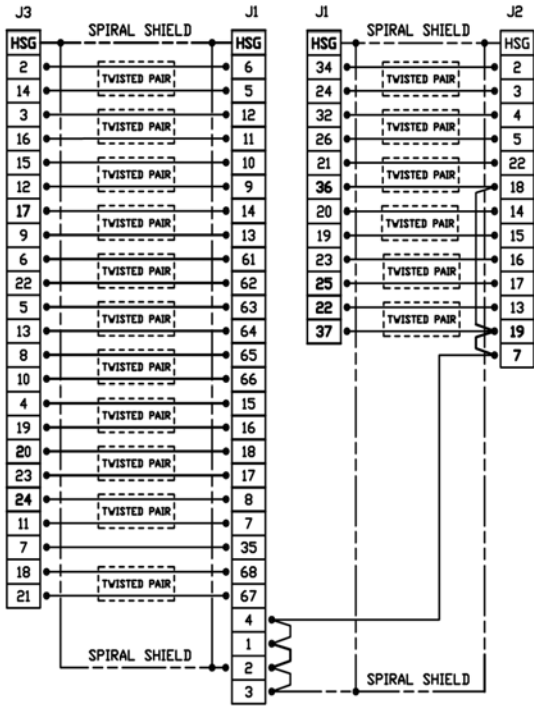
This cable connects the Polycom ISDN Gateway to third-party network equipment. It is used to connect to network equipment that has an RS-530/RS-366 interface. It is HD-68M to “Y” DB-25M and is used with ISDN systems.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 5 ft (1.65 m) | 2457-21263-200 | Yes |




| Peripheral Link V.35 HD-68 Pinout | | | Notes (direction from V.35 module (DTE)) | | | |
|---|---|---|---|---|---|---|
| 68 pin | Signal Name | Signal Type | From card | Function | RS530-DB25 | RS366-DB25 |
| | Shield | | | V.35/RS449/RS530 | | 7,18,19# |
| 12 | Receive Data A | Differential | in | V.35/RS449/RS530 | 3 | |
| 11 | Receive Data B | Differential | in | V.35/RS449/RS530 | 16 | |
| 10 | Send Timing A | Differential | in | V.35/RS449/RS530 | 15 | |
| 9 | Send Timing B | Differential | in | V.35/RS449/RS530 | 12 | |
| 29 | Data Set Ready (DSR) | Single Ended | in | V.35 | | |
| 28 | Request To Send (RTS) | Single Ended | out | V.35 | | |
| 27 | Data Terminal Ready (DTR) | Single Ended | out | V.35 | | |
| 34 | Digit Present (DPR) | Single Ended | out | RS366 | | 2 |
| 24 | Abandon Call/Retry (ACR) | Single Ended | in | RS366 | | 3 |
| 32 | Call Request (CRQ) | Single Ended | out | RS366 | | 4 |
| 26 | Present Next Digit (PND) | Single Ended | in | RS366 | | 5 |
| 21 | Data Line Occupied (DLO) | Single Ended | in | RS366 | | 22 |
| 14 | Receive Timing A | Differential | in | V.35/RS449/RS530 | 17 | |
| 13 | Receive Timing B | Differential | in | V.35/RS449/RS530 | 9 | |
| 8 | Terminal Timing A | Differential | out | V.35/RS449/RS530 | 24 | |
| 7 | Terminal Timing B | Differential | out | V.35/RS449/RS530 | 11 | |
| 15 | Request To Send (RTS) A | Differential | out | RS449/RS530 | 4 | |
| 16 | Request To Send (RTS) B | Differential | out | RS449/RS530 | 19 | |
| 35** | Receive Common | Gnd | | RS449 | | |
| 20 | BCD Dial Digit Bit 1 (NB1) | Single Ended | out | RS366 | | 14 |
| 19 | BCD Dial Digit Bit 2 (NB2) | Single Ended | out | RS366 | | 15 |
| 23 | BCD Dial Digit Bit 4 (NB4) | Single Ended | out | RS366 | | 16 |
| 25 | BCD Dial Digit Bit 8 (NB8) | Single Ended | out | RS366 | | 17 |
| 2** | Signal Ground | Gnd | | V.35/RS366 | | 7,18,19 |
| 6 | Send Data A | Differential | out | V.35/RS449/RS530 | 2 | |
| 5 | Send Data B | Differential | out | V.35/RS449/RS530 | 14 | |
| | reserved (Ascend select line) | | | | | |
| 63 | Clear To Send (CTS) A | Differential | in | RS449/RS530 | 5 | |
| 64 | Clear To Send (CTS) B | Differential | in | RS449/RS530 | 13 | |
| 61 | Data Mode (DM-DSR) A | Differential | in | RS449/RS530 | 6 | |
| 62 | Data Mode (DM-DSR) B | Differential | in | RS449/RS530 | 22 | |
| 65 | Receiver Ready (RR-DCD) A | Differential | in | RS449/RS530 | 8 | |
| 66 | Receiver Ready (RR-DCD) B | Differential | in | RS449/RS530 | 10 | |
| 4** | Send Common | Gnd | | RS530 | 7 | |
| 33 | Data Carrier Detect (DCD) | Single Ended | in | V.35 | | |
| 18 | Terminal Ready (TR-DTR) A | Differential | out | RS449/RS530 | 20 | |
| 17 | Terminal Ready (TR-DTR) B | Differential | out | RS449/RS530 | 23 | |
| 3 | V.35 Cable Connected | | ground to indicate a V.35 cable is attached | | | 7,18,19* |
| 1 | RS449 Cable Connected | | ground to indicate a RS449 cable is attached | | | 7,18,19^# |
| 22 | Distant Station Connected (DSC) | Single Ended | in | RS366 | | 13 |
| 30 | Clear To Send (CTS) | Single Ended | in | V.35 | | |
| 31 | Ring Indicate (RI) (Incoming Call | Single Ended | in | V.35/RS449 | | |
| | reserved (Ascend select line) | | | | | |
| 68 | LOS A | Differential | out | RS530 crypto | 18 | |
| 67 | LOS B | Differential | out | RS530 crypto | 21 | |

* For V.35, connect pin 3 of 68 pin connector to ground
^For RS449, connect pin 1 of 68 pin connector to ground
#For RS530, connect pins 1 and 3 of 68 pin connector to ground
** Gnd pins are 2,4, 35-60



# Serial Cables

The available serial cables include the following:

- Straight-Through Cable
- Null Modem Adapter

## Straight-Through Cable

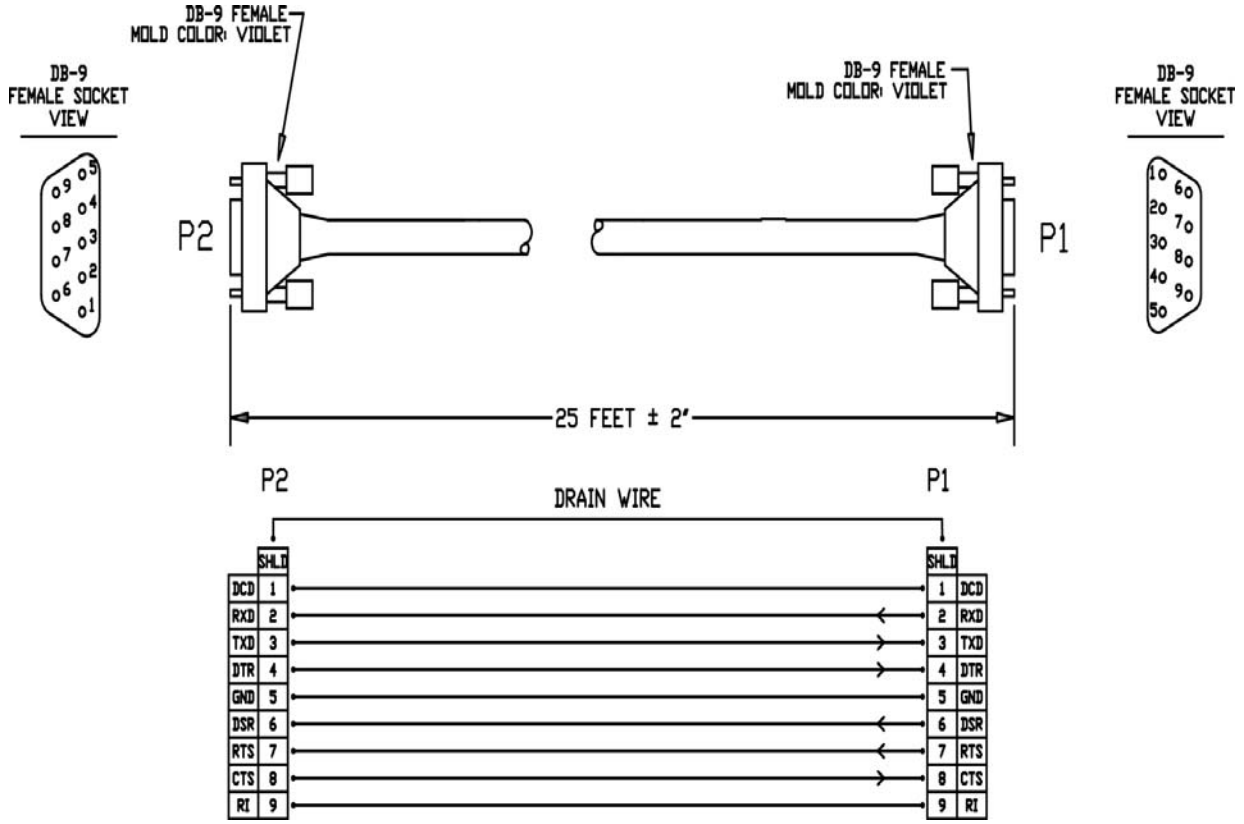
This cable connects the Polycom ISDN Gateway to a serial device. It has a DB-9 connector on each end. The maximum approved length for this cable is 4.92 ft (1.5 m).

### Recommendations for Use

Polycom does not recommend using this straight-through serial cable for RS-232 communication from a computer, Crestron system, or AMX device. Instead, for RS-232 communication, Polycom recommends using a cross-over cable with pin 2 wired to pin 3, pin 3 wired to pin 2, and pin 5 wired to pin 5. The other pins are not used.

If you choose to use this straight-through serial cable for RS-232 communication from a computer or Crestron system, the Null Modem Adapter is required. However, the null modem adapter does not work for RS-232 communication from AMX devices and causes problems if you try to use it.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| 25 ft (7.6 m) | 2457-09172-001 | — |


DB-9 FEMALE
MOLD COLOR: VIOLET
DB-9
FEMALE SOCKET
VIEW
P2
DB-9 FEMALE
MOLD COLOR: VIOLET
DB-9
FEMALE SOCKET
VIEW
P1
25 FEET ± 2"
P2
P1
DRAIN WIRE
SHLD 1
DCD 2
RXD 3
TXD 4
DTR 5
GND 6
DSR 7
RTS 8
CTS 9
RI
SHLD 1
1 DCD
2 RXD
3 TXD
4 DTR
5 GND
6 DSR
7 RTS
8 CTS
9 RI

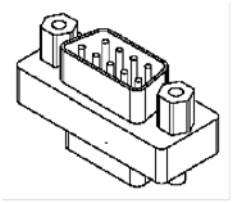
# Null Modem Adapter

This adapter is used when connecting the Polycom ISDN Gateway to a serial device that transmits on pin 3 such as Crestron Pro2 processor. It is a male to female DB-9 adapter plug.

**Note:** Do not use this adapter with an AMX device. AMAX systems support both RS-232 and RS-422. Therefore, for RS-232 support, use a null modem cross-over cable that carries only pins 2, 3, and 5, with pins 2 and 3 crossed.

| Length | Part Number | RoHS Compliant |
|---|---|---|
| — | 1517-61577-001 | Yes |

| DB9F | DB9M |
|---|---|
| PIN 1&6 | PIN 4 |
| PIN 2 | PIN 3 |
| PIN 3 | PIN 2 |
| PIN 4 | PIN 1&6 |
| PIN 5 | PIN 5 |
| PIN 7 | PIN 8 |
| PIN 8 | PIN 7 |
| PIN 9 | N/C |



**Note:** Drawings and part numbers are provided for reference only. Polycom claims no responsibility or liability for the quality, performance, or reliability of cables based on these reference drawings, other than cables provided by Polycom. Contact your Polycom distributor or Polycom Custom/Vertical Products to order cables that meet the appropriate manufacturing tolerances, quality, and performance parameters for your application.

## Crossover cable

You can use an RS-232 crossover cable to connect to the Polycom ISDN Gateway. Polycom recommends a crossover cable with any one of the following specifications:

- RS232 Male (DB9) to RS232 Female (DB9)
- RS232 Male (DB9) to USB converter cable

This crossover cable is not provided with the Polycom ISDN Gateway.

# Appendix B: Port Usage

You might need port usage information when you configure your network equipment for video conferencing. The following tables show IP port usage to and from Polycom ISDN Gateway.

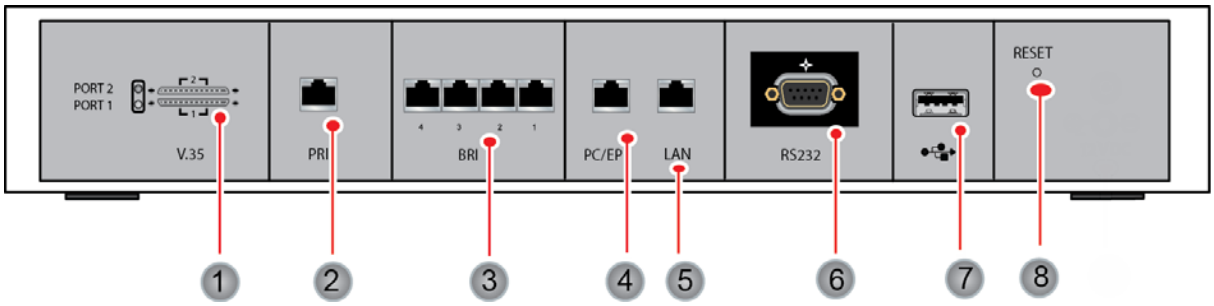
## Connections to the Polycom ISDN Gateway

| Inbound Port | Type | Protocol | Function | Configuration | | |
|---|---|---|---|---|---|---|
| | | | | On By Default ? (Low Security Profile) | Enable/Disable? | Configurable Port Number |
| 23 | Static | TCP | Telnet Diagnostics | No | Admin Settings > Security > Global Security > Access > Enable Telnet Access | No |
| 161 | Static | UDP | SNMP | No | Admin Settings > Security > Global Security > Access > Enable SNMP Access<br>Admin Settings > Servers > SNMP > Enable SNMP | Admin Settings > Servers > SNMP > Listening Port |
| 443 | Static | TLS | Web interface of Polycom ISDN Gateway HTTPS | Yes | Admin Settings > Security > Global Security > Access > Enable Web Access | No |
| 1719 | Static | UDP | H.225.0 RAS | No | Admin Settings > Network > IP Network > H.323 > Use Gatekeeper | No |
| 1720 | Static | TCP | H.225.0 Call Signaling | Yes | Admin Settings > Network > IP Network > H.323 > Enable IP H.323 | No |

| Inbound Port | Type | Protocol | Function | Configuration | | |
|---|---|---|---|---|---|---|
| | | | | On By Default ? (Low Security Profile) | Enable/Disable? | Configurable Port Number |
| 49152-65535 | Dynamic | TCP | H.245 | Yes | Admin Settings > Network > IP Network > H.323 > Enable IP H.323 | Admin Settings > Network > IP Network > Firewall > Fixed Ports > TCP Ports (1024-65535) |
| 16384-32764 (Default) | Dynamic | UDP | RTP/RTCP Video and Audio | Yes | Admin Settings > Network > IP Network > H.323 > Enable IP H.323 | Admin Settings > Network > IP Network > Firewall > Fixed Ports > UDP Ports (1024-65535) |

# Appendix C: Back Panel View

**Polycom ISDN Gateway Back Panel**




| Ref. Number | Location in Web Interface: Admin Settings > | Input/ Output | Supported Formats | Description |
|---|---|---|---|---|
| 1 | Network > ISDN | V.35 port | V.35/RS449/ RS530 | Connectivity with inverse multiplexer |
| 2 | Network > ISDN | ISDN Port for PRI | E1/T1 | Connectivity for ISDN network |
| 3 | Network > ISDN | ISDN Port for Quad BRI | S/T | Connectivity for ISDN network |
| 4 | Network > LAN Properties | LAN Port | Ethernet | • Connectivity for IP network, for example, Polycom ISDN Gateway web interface, telnet interface and H.323<br>• Connectivity for endpoints |
| 5 | Network > LAN Properties | LAN Port | Ethernet, 36V-56V DC, 600mA POE+ | Connectivity for IP and power input |
| 6 | General Settings > Serial Ports | Serial Port | RS-232 | Serial port |

| Ref. Number | Location in Web Interface: Admin Settings > | Input/ Output | Supported Formats | Description |
|---|---|---|---|---|
| 7 | N/A | USB Connector | USB 2.0 | USB for software update |
| 8 | N/A | Reset Button | N/A | • Restores the Polycom ISDN Gateway to the default configuration stored in its factory partition<br>• Reinstalls the Polycom ISDN Gateway's software |

# Appendix D: Security Profile Settings

Polycom ISDN Gateway security profiles provide varying levels of secure access to your Polycom ISDN Gateway. The default settings are different for each security profile.

- Maximum Security Profile Default Settings
- High Security Profile Default Settings
- Medium Security Profile Default Settings
- Low Security Profile Default Settings

To learn how to enable a security profile, refer to Configure Security Profiles .

## Maximum Security Profile Default Settings

The following table shows the default values for specific settings when you use the **Maximum** security profile.

| Admin Settings Area | | Maximum | | |
|---|---|---|---|---|
| | | Range | Default Value | Configurable? |
| **General Settings** | | | | |
| **System Settings** | | | | |
| **Recent Calls** | | | | |
| | Call Detail Report | Checkbox | Enabled | No |
| **Serial Ports** | | | | |
| **Mode** | | | | |
| | RS-232 Mode | Off<br>Control | Control | Yes |
| **Security** | | | | |
| **Global Security** | | | | |
| **Security Profile** | | | | |
| | Security Profile | Maximum<br>High<br>Medium<br>Low | Maximum | Yes |

| Admin Settings Area | | | Maximum Range | Default Value | Configurable? |
|---|---|---|---|---|---|
| | **Remote Access** | | | | |
| | | Enable Network Intrusion Detection System (NIDS) | Checkbox | Enabled | Yes |
| | | Enable Remote Access: Telnet | Checkbox | Disabled | Read-only |
| | | Enable Remote Access: SNMP | Checkbox | Disabled | Yes |
| | | API Port | 23, 24 | 23 | Yes |
| | | Enable SSH Access | Checkbox | Enabled | Yes |
| | | Lock Port after Failed Logins | Off, 2-10 | Off | Yes |
| | | Port Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | | Reset Port Lock Count After | Off, [1...24] hours | Off | Yes |
| | | Enable Whitelist | Checkbox | Disabled | Yes |
| | | Idle Session Timeout | 1, 3, 5, 10, 15, 20, 30, 45, 60 minutes | 10 | Yes |
| | | Maximum Number of Active Sessions | 10-50 | 25 | Yes |
| **Global Security** | | | | | |
| | **Account Lockout** | | | | |
| | | Lock Admin Account After Failed Logins | Off, 2-10 | 3 | Yes |
| | | Admin Account Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 | Yes |
| | | Reset Admin Account Lock Counter After | Off, [1...24] hours | 1 | Yes |
| | | Lock User Account After Failed Logins | Off, 2-10 | 3 | Yes |
| | | User Account Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |

| Admin Settings Area | | | Maximum Range | Default Value | Configurable? |
|---|---|---|---|---|---|
| | | Reset User Account Lock Counter After | Off, [1...24] hours | 1 | Yes |
| | | Lock Auditor Account After Failed Logins | Off, 2-10 | 3 | Yes |
| | | Auditor Account Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | | Reset Auditor Account Lock Counter After | Off, [1...24] hours | 1 | Yes |
| | **Password Requirements** | | | | |
| **Admin (Room, Auditor), User (Room, Auditor)** | | | | | |
| | | Reject Previous Passwords | 8-16 | 10 | Yes |
| | | Minimum Password Age in Days | Off, 1, 5, 10, 15, 20, 30 | Off | Yes |
| | | Maximum Password Age in Days | 30, 60, 90, 100, 110, 120, 130, 140, 150,160, 170, 180 | 60 | Yes |
| | | Minimum Changed Characters | 1-4 | 4 | Yes |
| | | Password Expiration Warning | 1-7 | 7 | Yes |
| | | Minimum Length | 6-16, 32 | 9 | Yes |
| | | Require Lowercase | Off, 1, 2, All | Off | Yes |
| | | Require Uppercase | Off, 1, 2, All | Off | Yes |
| | | Require Numbers | Off, 1, 2, All | Off | Yes |
| | | Require Special Characters | Off, 1, 2, All | Off | Yes |
| | | Maximum Consecutive Repeated Characters | 1-4 | 2 | Yes |
| | | Can contain ID or Its Reverse Form | Checkbox | Disabled | Read-only |
| | **SNMP**<br>**Note:** SNMP Passwords are applicable only when the system uses SNMP v3 | | | | |
| | | Minimum Length | 8-16, 32 | 12 | Yes |

| Admin Settings Area | | | Maximum Range | Default Value | Configurable? |
|---|---|---|---|---|---|
| | | Require Lowercase | Off, 1, 2, All | 1 | Yes |
| | | Require Uppercase | Off, 1, 2, All | 1 | Yes |
| | | Require Numbers | Off, 1, 2, All | 1 | Yes |
| | | Require Special Characters | Off, 1, 2, All | 1 | Yes |
| | | Reject Previous Passwords | 8-16 | 10 | Yes |
| | | Minimum Password Age in Days | Off, 1, 5, 10, 15, 20, 30 | Off | Yes |
| | | Maximum Consecutive Repeated Characters | 1-4 | 2 | Yes |
| | | Can contain ID or its Reverse Form | Checkbox | Disabled | Read-only |
| **Security Banner** | | | | | |
| | | Enable Security Banner | Off<br>DoD<br>Custom | DoD | Yes |
| | | Remote System Banner Text | Unicode characters, 2048 bytes max | DoD Banner Text | Yes |
| **Certificates** | | | | | |
| | **Certificate Options** | | | | |
| | | Certificate Validation (Web Server) | Checkbox | Enabled | Yes |
| | | Certificate Validation (Client Apps) | Checkbox | Enabled | Yes |
| | **Revocation** | | | | |
| | | Revocation Method | OCSP<br>CRL | OCSP | Yes |
| | | Allow Incomplete Revocation Checks | Checkbox | Enabled | Yes |
| **Servers** | | | | | |
| | **SNMP** | | | | |
| | | Version1 | Checkbox | Disabled | Yes |

| Admin Settings Area | | Maximum Range | Default Value | Configurable? |
|---|---|---|---|---|
| | Version2c | Checkbox | Disabled | Yes |
| | Version3 | Checkbox | Enabled | Yes |

| Diagnostics Area | | Maximum Range | Default Value | Configurable? |
|---|---|---|---|---|
| **System** | | | | |
| **System Log Settings** | | | | |
| | Enable Remote Logging | Checkbox | Disabled | Yes |
| | Transport Protocol | UDP | UDP | Read-only |

## High Security Profile Default Settings

The following table shows the default values for specific Admin settings when you use the High security profile.

| Admin Settings Area | | High Range | Default Value | Configurable? |
|---|---|---|---|---|
| **General Settings** | | | | |
| **System Settings** | | | | |
| **Recent Calls** | | | | |
| | Call Detail Report | Checkbox | Enabled | Yes |
| **Serial Port** | | | | |
| **Mode** | | | | |
| | RS-232 Mode | Off<br>Control | Control | Yes |
| **Security** | | | | |
| **Global Security** | | | | |
| **Security Profile** | | | | |
| | Security Profile | Maximum<br>High<br>Medium<br>Low | High | Yes |

| Admin Settings Area | | | High | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | **Access** | | | | |
| | | Enable Network Intrusion Detection System (NIDS) | Checkbox | Enabled | Yes |
| | | Enable Remote Access: Telnet | Checkbox | Disabled | Read-only |
| | | Enable Remote Access: SNMP | Checkbox | Disabled | Yes |
| | | API Port | 23, 24 | 23 | Yes |
| | | Enable SSH Access | Checkbox | Enabled | Yes |
| | | Lock Port after Failed Logins | Off, 2-10 | Off | Yes |
| | | Port Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes | 1 minute | Yes |
| | | Reset Port Lock Count After | Off, [1...24] hours | Off | Yes |
| | | Enable Whitelist | Checkbox | Disabled | Yes |
| | | Idle Session Timeout | 1, 3, 5, 10, 15, 20, 30, 45 minutes<br>1, 2, 4, 8 hours | 10 | Yes |
| | | Maximum Number of Active Web Sessions | 10-50 | 25 | Yes |
| **Global Security** | | | | | |
| | **Account Lockout** | | | | |
| | | Lock Admin Account after failed logins | 2-10 | 3 | Yes |
| | | Admin Account Lock Duration | 1, 2, 3, 5 minutes | 1 minute | Yes |
| | | Reset Admin Account Lock Counter After | Off, [1...24] hours | Off | Yes |
| | | Lock User Account After Failed Logins | 2-10 | 3 | Yes |
| | | User Account Lock Duration | 1, 3, 5, 10, 15, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |

| Admin Settings Area | | | High | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | | Reset User Account Lock Counter After | Off, [1...24] hours | Off | Yes |
| | | Lock Auditor Account After Failed Logins | 2-10 | 3 | Yes |
| | | Auditor Account Lock Duration | 1, 3, 5, 10, 15, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | | Reset Auditor Account Lock Counter After | Off, [1...24] hours | Off | Yes |
| | **Password Requirements** | | | | |
| | **Admin (Room), User (Room), Auditor** | | | | |
| | | Reject Previous Passwords | Off, 1-16 | 10 | Yes |
| | | Minimum Password Age in Days | Off, 1, 5, 10, 15, 20, 30 | Off | Yes |
| | | Maximum Password Age in Days | Off, 30, 60, 90, 100, 110, 120, 130, 140, 150,160, 170, 180 | 90 | Yes |
| | | Minimum Changed Characters | 1-4 | 4 | Yes |
| | | Password Expiration Warning | 1-7 | 4 | Yes |
| | | Minimum Length | 6-16, 32 | 6 | Yes |
| | | Require Lowercase | Off, 1, 2, All | Off | Yes |
| | | Require Uppercase | Off, 1, 2, All | Off | Yes |
| | | Require Numbers | Off, 1, 2, All | Off | Yes |
| | | Require Special Characters | Off, 1, 2, All | Off | Yes |
| | | Maximum Consecutive Repeated Characters | Off, 1-4 | Off | Yes |
| | | Can contain ID or Its Reverse Form | Checkbox | Disabled | Read-only |
| | **SNMP**<br>**Note:** SNMP Passwords are applicable only when the system uses SNMP v3 | | | | |

| Admin Settings Area | | | High | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | | Minimum Length | 8-16, 32 | 8 | Yes |
| | | Require Lowercase | Off, 1, 2, All | 1 | Yes |
| | | Require Uppercase | Off, 1, 2, All | 1 | Yes |
| | | Require Numbers | Off, 1, 2, All | 1 | Yes |
| | | Require Special Characters | Off, 1, 2, All | 1 | Yes |
| | | Reject Previous Passwords | Off, 1-16 | 5 | Yes |
| | | Minimum Password Age in Days | Off, 1,5, 10, 15, 20, 30 | Off | Yes |
| | | Maximum Consecutive Repeated Characters | Off, 1-4 | Off | Yes |
| | | Can contain ID or its reverse form | Checkbox | Disabled | Read-only |
| **Security Banner** | | | | | |
| | | Enable Security Banner | Off<br>DoD<br>Custom | Off | Yes |
| | | Remote System Banner Text | Unicode characters, 2048 bytes max | Null (No text) | Yes |
| **Certificates** | | | | | |
| | **Certificate Options** | | | | |
| | | Certificate Validation (Web Server) | Checkbox | Enabled | Yes |
| | | Certificate Validation (Client Apps) | Checkbox | Enabled | Yes |
| | **Revocation** | | | | |
| | | Revocation Method | OCSP<br>CRL | OCSP | Yes |
| | | Allow Incomplete Revocation Checks | Checkbox | Enabled | Yes |
| **Servers** | | | | | |
| | **SNMP** | | | | |

| Admin Settings Area | | High | | |
|---|---|---|---|---|
| | | Range | Default Value | Configurable? |
| | Version1 | Checkbox | Disabled | Yes |
| | Version2c | Checkbox | Disabled | Yes |
| | Version3 | Checkbox | Enabled | Yes |

| Diagnostics Area | | High | | |
|---|---|---|---|---|
| | | Range | Default Value | Configurable? |
| **System** | | | | |
| **System Log Settings** | | | | |
| | Enable Remote Logging | Checkbox | Disabled | Yes |
| | Transport Protocol | UDP | UDP | Read-only |

## Medium Security Profile Default Settings

The following table shows the default values for specific Admin settings when you use the Medium security profile.

| Admin Settings Area | | Medium | | |
|---|---|---|---|---|
| | | Range | Default Value | Configurable? |
| **General Settings** | | | | |
| **System Settings** | | | | |
| **Recent Calls** | | | | |
| | Call Detail Report | Checkbox | Enabled | Yes |
| **Serial Ports** | | | | |
| **Mode** | | | | |
| | RS-232 Mode | Off<br>Control | Control | Yes |
| **Security** | | | | |
| **Global Security** | | | | |
| **Security Profile** | | | | |

| Admin Settings Area | | | Medium | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | | Security Profile | Maximum<br>High<br>Medium<br>Low | Medium | Yes |
| | **Access** | | | | |
| | | Enable Network Intrusion Detection System (NIDS) | Checkbox | Enabled | Yes |
| | | Enable Remote Access: Telnet | Checkbox | Disabled | Read-only |
| | | Enable Remote Access: SNMP | Checkbox | Disabled | Yes |
| | | API Port | 23, 24 | 23 | Yes |
| | | Enable SSH Access | Checkbox | Enabled | Yes |
| | | Lock Port after Failed Logins | Off, 2-10 | Off | Yes |
| | | Port Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | | Reset Port Lock Count After | Off, [1...24] hours | Off | Yes |
| | | Enable Whitelist | Checkbox | Disabled | Yes |
| | | Idle Session Timeout in Minutes | 1, 2, 3, 5, 10, 20, 30, 45 minutes<br>1, 2, 4, 8 hours | 10 | Yes |
| | | Maximum Number of Active Web Sessions | 10-50 | 25 | Yes |
| **Global Security** | | | | | |
| | **Account Lockout** | | | | |
| | | Lock Admin Account After Failed Logins | Off, 2-10 | 3 | Yes |
| | | Admin Account Lock Duration | 1, 2, 3, 5 minutes | 1 | Yes |
| | | Reset Admin Account Lock Count After | Off, [1...24] hours | Off | Yes |

| Admin Settings Area | | Medium | | |
|---|---|---|---|---|
| | | **Range** | **Default Value** | **Configurable?** |
| | Lock User Account After Failed Logins | Off, 2-10 | 3 | Yes |
| | User Account Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | Reset User Account Lock Count After | Off, [1...24] hours | Off | Yes |
| | Lock Auditor Account After Failed Logins | Off, 2-10 | 3 | Yes |
| | Auditor Account Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | Reset Auditor Account Lock Count After | Off, [1..24] hours | Off | Yes |
| **Password Requirements** | | | | |
| **Admin (Room), User (Room), Auditor** | | | | |
| | Reject Previous Passwords | Off, 1-16 | Off | Yes |
| | Minimum Password Age in Days | Off, 1, 5, 10, 15, 20, 30 | Off | Yes |
| | Maximum Password Age in Days | Off, 30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180 | Off | Yes |
| | Minimum Changed Characters | Off, 1-4 All | Off | Yes |
| | Password Expiration Warning | Off, 1-7 | Off | Yes |
| | Minimum Length | 3-16, 32 | 3 | Yes |
| | Require Lowercase | Off, 1, 2, All | Off | Yes |
| | Require Uppercase | Off, 1, 2, All | Off | Yes |
| | Require Numbers | Off, 1, 2, All | Off | Yes |
| | Require Special Characters | Off, 1, 2, All | Off | Yes |
| | Maximum Consecutive Repeated Characters | Off, 1-4 | Off | Yes |

| Admin Settings Area | | Medium | | |
|---|---|---|---|---|
| | | **Range** | **Default Value** | **Configurable?** |
| | Can contain ID or Its reverse form | Checkbox | Disabled | Yes |
| **SNMP**<br>**Note**: SNMP passwords are applicable only when the system uses SNMP v3. | | | | |
| | Minimum Length | 8-16, 32 | 8 | Yes |
| | Require Lowercase | Off, 1, 2, All | Off | Yes |
| | Require Uppercase | Off, 1, 2, All | Off | Yes |
| | Require Numbers | Off, 1, 2, All | Off | Yes |
| | Require Special Characters | Off, 1, 2, All | Off | Yes |
| | Reject Previous Passwords | Off, 1-16 | Off | Yes |
| | Minimum Password Age in Days | Off, 1, 5, 10, 15, 20, 30 | Off | Yes |
| | Maximum Consecutive Repeated Characters | Off, 1-4 | Off | Yes |
| | Can contain ID or its reverse form | Checkbox | Disabled | Read-only |
| **Security Banner** | | | | |
| | Enable Security Banner | Off<br>DoD<br>Custom | Off | Yes |
| | Remote system Banner text | Unicode characters, 2048 bytes max | Null (No text) | Yes |
| **Certificates** | | | | |
| | **Certificate Options** | | | |
| | Certificate Validation (Web Server) | Checkbox | Disabled | Yes |
| | Certificate Validation (Client Apps) | Checkbox | Disabled | Yes |
| | **Revocation** | | | |
| | Revocation Method | OCSP<br>CRL<br>Checkbox | OCSP | Yes |

| Admin Settings Area | | | Medium | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | | Allow incomplete Revocation checks | Checkbox | Enabled | Yes |
| **Servers** | | | | | |
| | **SNMP** | | | | |
| | | Version1 | Checkbox | Disabled | Yes |
| | | Version2c | Checkbox | Disabled | Yes |
| | | Version3 | Checkbox | Enabled | Yes |

| Diagnostics Area | | | Medium | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| **System** | | | | | |
| **System Log Settings** | | | | | |
| | | Enable Remote Logging | Checkbox | Disabled | Yes |
| | | Transport Protocol | UDP | UDP | Read-only |

## Low Security Profile Default Settings

The following table shows the default values for specific Admin settings when you use the Low security profile.

| Admin Settings Area | | | Low | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| **General Settings** | | | | | |
| **System Settings** | | | | | |
| **Recent Calls** | | | | | |
| | | Call Detail Report | Checkbox | Enabled | Yes |
| **Serial Ports** | | | | | |
| **Mode** | | | | | |
| | | RS-232 Mode | Off<br>Control | Control | Yes |
| **Security** | | | | | |
| **Global Security** | | | | | |

| Admin Settings Area | | | Low | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | **Security Profile** | | | | |
| | | Security Profile | Maximum<br>High<br>Medium<br>Low | Low | Yes |
| | **Access** | | | | |
| | | Enable Network Intrusion Detection System (NIDS) | Checkbox | Disabled | Yes |
| | | Enable Remote Access: Telnet | Checkbox | Disabled | Yes |
| | | Enable Remote Access: SNMP | Checkbox | Disabled | Yes |
| | | API Port | 23, 24 | 23 | Yes |
| | | Enable SSH Access | Checkbox | Enabled | Yes |
| | | Lock Port after Failed Logins | Off, 2-10 | Off | Yes |
| | | Port Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | | Reset Port Lock Count After | Off, [1...24] hours | Off | Yes |
| | | Enable Whitelist | Checkbox | Disabled | Yes |
| | | Idle Session Timeout | 1, 2, 3, 5, 10, 20, 30, 45 minutes<br>1, 2, 4, 8 hours | 10 | Yes |
| | | Maximum Number of Active Web Sessions | 10-50 | 25 | Yes |
| **Global Security** | | | | | |
| | **Account Lockout** | | | | |
| | | Lock Admin Account After Failed Logins | Off, 2-10 | Off | Yes |
| | | Admin Account Lock Duration | 1, 2, 3, 5 minutes | 1 | Yes |

| Admin Settings Area | | | Low | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | | Reset Admin Account Lock Counter After | Off, [1...24] hours | Off | Yes |
| | | Lock User Account After Failed Logins | Off, 2-10 | Off | Yes |
| | | User Account Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | | Reset User Account Lock Counter After | Off, [1...24] hours | Off | Yes |
| | | Lock Auditor Account After Failed Logins | Off, 2-10 | Off | Yes |
| | | Auditor Account Lock Duration | 1, 2, 3, 5, 10, 20, 30 minutes<br>1, 2, 4, 8 hours | 1 minute | Yes |
| | | Reset Auditor Account Lock Counter After | Off, [1...24] hours | Off | Yes |
| | **Password Requirements** | | | | |
| | **Admin (Room), User (Room), Auditor** | | | | |
| | | Reject Previous Passwords | Off, 1-16 | Off | Yes |
| | | Minimum Password Age in Days | Off, 1, 5, 10, 15, 20, 30 | Off | Yes |
| | | Maximum Password Age in Days | Off, 30, 60, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180 | Off | Yes |
| | | Minimum Changed Characters | Off, 1-4, All | Off | Yes |
| | | Password Expiration Warning | Off, 1-7 | Off | Yes |
| | **SNMP**<br>**Note**: SNMP passwords are applicable only when the system uses SNMP v3. | | | | |
| | | Minimum Length | 8-16, 32 | 8 | Yes |
| | | Require Lowercase | Off, 1, 2, All | Off | Yes |
| | | Require Uppercase | Off, 1, 2, All | Off | Yes |
| | | Require Numbers | Off, 1, 2, All | Off | Yes |

| Admin Settings Area | | | Low | | |
|---|---|---|---|---|---|
| | | | Range | Default Value | Configurable? |
| | | Require Special Characters | Off, 1, 2, All | Off | Yes |
| | | Reject Previous Passwords | Off, 1-16 | Off | Yes |
| | | Minimum Password Age in Days | Off, 1, 5, 10, 15, 20, 30 | Off | Yes |
| | | Maximum Consecutive Repeated Characters | Off, 1-4 | Off | Yes |
| | | Can contain ID or its reverse form | Checkbox | Disabled | Yes |
| **Security Banner** | | | | | |
| | | Enable Security Banner | Off<br>DoD<br>Custom | Off | Yes |
| | | Remote system Banner text | Unicode characters, 2048 bytes max | Null (text) | Yes |
| **Certificates** | | | | | |
| | **Certificate Options** | | | | |
| | | Certification Validation (Web Server) | Checkbox | Disabled | Yes |
| | | Certification Validation (Client Apps) | Checkbox | Disabled | Yes |
| | **Revocation** | | | | |
| | | Revocation Method | OCSP<br>CRL | OCSP | Yes |
| | | Allow incomplete Revocation checks | Checkbox | Enabled | Yes |
| **Servers** | | | | | |
| **SNMP** | | | | | |
| | | Version 1 | Checkbox | Disabled | Yes |
| | | Version 2c | Checkbox | Disabled | Yes |
| | | Version 3 | Checkbox | Enabled | Yes |

| Admin Settings Area | | Low | | |
|---|---|---|---|---|
| | | Range | Default Value | Configurable? |
| **Diagnostics Area** | | **Low** | | |
| | | **Range** | **Default Value** | **Configurable?** |
| **System** | | | | |
| **System Log Settings** | | | | |
| | Enable Remote Logging | Checkbox | Disabled | Yes |
| | Transport Protocol | UDP | UDP | Read-only |