Poly VideoOS Configuration Parameter Reference Guide 4.1.0 (G7500, Studio X70, Studio X52, Studio X50, and Studio X30)

SUMMARY

This guide provides the end-user with task-based user information for the featured product.

Table of contents

1   Before You Begin

This guide lists the available configuration parameters for provisioning your Poly G7500 and Studio X series system.

The information in this guide applies to all the following Poly video systems except where noted:

- Poly G7500

- Poly Studio X70

- Poly Studio X50

- Poly Studio X30

- Poly Studio X52

Audience, purpose, and required skills

This guide is written for a technical audience.

You must be familiar with the following concepts before beginning:

- Current telecommunications practices, protocols, and principles

- Telecommunication basics, video teleconferencing, and voice or data equipment

- OpenSIP networks and VoIP endpoint environments

Related Poly and Partner Resources

See the following sites for information related to this product.

- Poly Support is the entry point to online product, service, and solution support information. Find product-specific information such as Knowledge Base articles, Support Videos, Guide & Manuals, and Software Releases on the Products page, download software for desktop and mobile platforms from Downloads & Apps, and access additional services.

- The Poly Documentation Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.

- The Poly Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.

- The Poly Partner Network is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs, making it easy for you to communicate face-to-face using the applications and devices you use every day.

- Poly Services help your business succeed and get the most out of your investment through the benefits of collaboration. Enhance collaboration for your employees by accessing Poly service solutions, including Support Services, Managed Services, Professional Services, and Training Services.

- With Poly+ you get exclusive premium features, insights and management tools necessary to keep employee devices up, running, and ready for action.

- Poly Lens enables better collaboration for every user in every workspace. It is designed to spotlight the health and efficiency of your spaces and devices by providing actionable insights and simplifying device management.

2 Getting Started

You can use the configuration parameters described in this guide to provision single or multiple systems. Use the navigation on the left to find parameters grouped by Required, Recommended, and Optional.

Unless otherwise noted in the description, you can provision a parameter on systems in Poly Video Mode or Poly Partner Mode.

Understanding Parameter Lists

The following information describes the general convention for parameter list details. Parameter details vary depending on the complexity of the parameter.

`parameter.name`
A parameter's description, applicability, or dependencies.
The parameter's permitted values, default value, and the value's unit of measure (such as seconds, Hz, or dB).

A note that highlights critical information you need to know.

> 📝 **NOTE:** Some parameters use check boxes as value options on the provisioning server's web interface, where selected check boxes indicate true and cleared check boxes indicate false.

Automatic Provisioning with Poly Clariti Manager

By default, the Poly Clariti Manager system automatically provisions some G7500 and Studio X series system settings for you using a special configuration value (for example, `voIpProt.SIP.userName="${sip_alias}"`).

The following parameters support automatic configuration values:

```
device.local.deviceName="${device_name}"dir.ldap.server.address="$
{ldap_serveraddress}"dir.ldap.baseDN="$
{ldap_baseDN}"dir.ldap.defaultGroupDN="$
{ldap_defaultgroupDN}"voIpProt.H323.name="$
{h323_ID}"voIpProt.H323.e164="${h323_e164}"voIpProt.SIP.userName="$
{sip_alias}"
```

These parameters are provisioned by default, so you won't see them in the profiles provided by the Poly Clariti Manager system. You can overwrite these parameters with your own values (for example, `voIpProt.SIP.userName="meetingSpace"`).

You also can automatically generate new values by resetting these parameters with a special configuration value (for example, `voIpProt.H323.e164="${h323_e164}"`). However, you can't rename existing endpoints by setting `device.local.deviceName="${device_name}"` because that value is applied only to new endpoints.

For more information, see the [Poly Clariti Manager Administrator Guide](#) and see the Provisioning, Monitoring, and Upgrading UC Managed Video Endpoints section.

3   Required Parameters

The parameters in this section are required to successfully run your system.

Required Calendaring Parameters

These calendaring parameters are required to successfully run your system.

Using Provisioning Service Credentials to Register with a Calendaring Service

You can register your G7500 and Studio X series system with a calendaring service using the same credentials you used to register with your provisioning service.

To do this, set `exchange.auth.useLoginCredentials="True"`.

With this parameter, provisioning separate username, password, and domain parameters for the calendaring service isn't necessary. For example, if you set `exchange.auth.useLoginCredentials="True"`, you don't have to set `exchange.auth.userName`, `exchange.auth.password`, and `exchange.auth.domain`.

Calendaring Parameters

`exchange.auth.domain`
Specifies the domain for registering to the Microsoft Exchange Server in NETBIOS or DNS notation (e.g., company.local or COMPANY).
You can't provision this parameter if the system is in Partner Mode.

String

`exchange.auth.email`
Specifies the email address used when scheduling the system for a meeting (for instance, you could use your system as a mechanism for reserving a meeting space). This should match the Primary SMTP Address for the account on Microsoft Exchange Server, which displays as the value of the mail attribute in the account properties.
You can't provision this parameter if the system is in Partner Mode.

String

`exchange.auth.password`
Specifies the system password for registering with the Microsoft Exchange Server. This can be the system password or an individual's password.
If you want the calendaring service to use the calendar associated with an Office 365 account, enter the password for that account here.

You can't provision this parameter if the system is in Partner Mode.

String

exchange.auth.userName
Specifies the user name for registering to the Microsoft Exchange Server with no domain information included. This can be the system name or an individual's name (e.g., username@company.com).
If you want the calendaring service to use the calendar associated with an Office 365 account, enter the user name for that account here.

You can't provision this parameter if the system is in Partner Mode.

String (0-64)

exchange.enable
Enables or disables the ability to register with a calendaring service.
You can't provision this parameter if the system is in Partner Mode.

False (default)

True

exchange.meeting.reminderInterval
Specifies the number of minutes before the meeting that a reminder displays on the system.
You can't provision this parameter if the system is in Partner Mode.

5 (default)

None

1

10

15

30

exchange.meeting.reminderSound.enable
Specifies whether to play a sound along with the text reminder (when the system is not in a call).
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

exchange.server.url
Specifies the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Client Access server. If your organization has multiple servers behind a network load balancer, this is the FQDN of the server's virtual IP address. If required, an IP address can be used instead of an FQDN, but Poly recommends using the same FQDN for Outlook clients.
You can't provision this parameter if the system is in Partner Mode.

String

exchange.showPrivateMeeting
Specifies whether to display details about meetings marked private.
You can't provision this parameter if the system is in Partner Mode.

False (default)

True

exchange.auth.useLoginCredentials
Specifies if you want to register with a calendaring service using the same credentials you used for registering with a provisioning service.
With this parameter, provisioning separate username, password, and domain parameters for the calendaring service isn't necessary.

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

Required Call Control Parameters

These call control parameters are required to successfully run your system.

Configuring Dialing Preferences

Remember the following when provisioning dialing preferences for your G7500 and Studio X series system:

- To successfully provision a dialing preference, the corresponding call protocol (SIP or H.323) must be enabled. For example, you must configure `voIpProt.H323.enable="True"` to set `call.videoDialPreference.1="h323"`.

- To configure a secondary dialing preference, you must set `voIpProt.H323.enable` and `voIpProt.SIP.enable` to `"True"`.

- If you enable SIP and H.323, you must configure primary and secondary dialing preferences.

- You can't configure your primary and secondary dialing preferences with the same value.
  For example, `call.videoDialPreference.1` and `call.videoDialPreference.2` cannot both be set to `"sip"`.

- You can't configure `call.voiceDialPreference.1` or `call.voiceDialPreference.2` if `call.audioOnly.enable="False"`.

Call Control Parameters

call.autoAnswer.micMute
Specifies whether to mute incoming calls.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

call.conference.joinLeaveTone.enable
Plays an audible tone when someone joins or leaves a conference call.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.autoAnswer.answerP2PCall`

Sets whether the system answers an incoming call when not in a call.
If set to "Do_Not_Disturb", incoming calls are rejected without notification.

You can't provision this parameter if the system is in Partner Mode.

No (default)

Yes

Do_Not_Disturb

`call.displayIconsInCall`

Specifies whether to display onscreen graphics, including icons and help text, during calls.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.maxTimeInCall`

Sets the maximum number of hours allowed for a call.
When that time expires, you're prompted if you want to hang up. If you don't answer within one minute, the call automatically ends. If you choose to stay in the call, you aren't prompted again.

You can't provision this parameter if the system is in Partner Mode.

8_hours (default)

1_hour

2_hours

3_hours

4_hours

5_hours

6_hours

7_hours

9_hours

10_hours

11_hours

12_hours

24_hours

48_hours

`call.preferredPlaceACallNav`

Specifies the default options that display on the local interface place a call screen.
You can't provision this parameter if the system is in Partner Mode.

keypad (default) - Displays recently-dialed numbers and a dialpad.

globaldir - Displays a screen for searching a directory. The multitiered directory (LDAP) root entry displays at the top of the Contacts list, which combines your search results and favorites.

recentcalls - Lists previous calls in chronological order.

`call.audioOnly.enable`
Lets you place audio-only calls on the system.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.h239.enable`
Allows the use of a standards-based specification for parallel video streams (i.e., people and content). Enable if you know call participants support H.239.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.preferredSpeed.maxIncoming`
Calls are received at no higher than the speed set here.
You can't provision this parameter if the system is in Partner Mode.

128

256

384

512

768

1024

1472

1920

2048

3072

3840

4096

6144 (default)

`call.preferredSpeed.outgoing`
Determines the IP call speed your system uses when the call is placed from the directory.
You can't provision this parameter if the system is in Partner Mode.

128

256

384

512

768

1024 (default)

1472

1920

2048

3072

3840

4096

6144

> **NOTE:** If the far-site system does not support the selected speed, a lower speed is automatically negotiated.

`call.videoDialPreference.1`
Specifies your first preference for how the system places video calls to directory entries with more than one type of number.
You can't provision this parameter if the system is in Partner Mode.

sip (default)

h323

`call.videoDialPreference.2`
Specifies your second preference for how the system places video calls to directory entries with more than one type of number.
You can't provision this parameter if the system is in Partner Mode.

h323 (default)

sip

`call.voiceDialPreference.1`
Specifies your first preference for how the system places audio calls to directory entries with more than one type of number.
You can't provision this parameter if the system is in Partner Mode.

sip (default)

h323

`call.voiceDialPreference.2`
Specifies your second preference for how the system places audio calls to directory entries with more than one type of number.
You can't provision this parameter if the system is in Partner Mode.

h323 (default)

sip

`call.encryption.requireAES`
Specifies how you want to use AES encryption for calls.
You can't provision this parameter if the system is in Partner Mode.

When_Available (default) - AES encryption is used with systems that support it, but unencrypted calls also are allowed.

Required_Video - AES encryption is used in all video calls. Calls with systems that don't support fail.

Required_All - AES encryption is used in all types of calls. Calls with systems that don't support fail.

Off - AES encryption is disabled.

`call.cdr.enable`
Call detail records (CDRs) are included in the system logs. When disabled, the system does not write call information.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.recentCalls.enable`
Specifies whether to show recent calls on the local and system web interfaces.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.recentcalls.maxNumberToDisplay`
The maximum number of calls displayed in the recent calls list.
You can't provision this parameter if the system is in Partner Mode.

100 (default)

25

50

75

`call.escalate2MCU.enable`
If set to "True", a point-to-point call on your system can escalate to an impromptu conference call on an external Polycom MCU.
Calls converted through a Poly Clariti Core or Poly Clariti Edge system gateway (H.323 to SIP or vice versa) won't join an impromptu conference call.

To use this feature, make sure you set the relevant voIpProt.SIP.* parameters to register your system with a Poly Clariti Core or Poly Clariti Edge system. You also must set call..escalate2MCU.conferenceId.

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

`call.escalate2MCU.conferenceId`
Specifies the conference factory ID associated with the SIP conference factory on your Poly Clariti Core or Poly Clariti Edge system.
You can't provision this parameter if the system is in Partner Mode.

Integer (0-128)

NOTE: The conference factory ID should come from the same Poly Clariti Core or Poly Clariti Edge system your video-conferencing system uses for SIP registration. Calls won't escalate if the ID you provide isn't recognized by your RealPresence Poly Clariti Core or Poly Clariti Edge system.

Required System Display Parameters

These system display parameters are required to successfully run your system.

`device.local.datetime.date.format`
Specifies how the date displays.
mm_dd_yyyy (default)

dd_mm_yyyy

yyyy_mm_dd

`device.local.datetime.time.24HourClock`
Specifies how the time displays (12- or 24-hour format).
12_Hour (default)

24_Hour

`device.local.ntpServer.mode`
Specifies if you want to automatically or manually configure the system to use a time server.
Auto (default) - Your system tries to automatically connect with a time server.

Manual - Set device.local.ntpServer.address.1 and optionally device.local.ntpServer.address.2.

Off - Set the current date and time in the system web interface.

`device.local.timezone`
Specifies the time difference between GMT and your location.
CST6CDT (default)

Etc/GMT+12

Pacific/Midway

Pacific/Honolulu

America/Adak

America/Anchorag

Pacific/Pitcairn

PST8PDT

BAJA

America/Phoenix

America/Mazatlan

MST7MDT

America/Guatemala

America/Monterrey

America/Regina

America/Lima

EST5EDT

America/Indianapolis

Canada/Atlantic

America/La//Paz

America/Caracas

America/Santiago

Canada/Newfoundland

America/Sao//Paulo

America/Cordoba

America/Godthab

America/Noronha

Atlantic/Azores

Atlantic/Cape//Verde

Etc/Greenwich

Africa/Casablanca

Europe/London

Europe/Amsterdam

Europe/Belgrade

Europe/Paris

Europe/Warsaw

Africa/Bangui

Europe/Athens

Europe/Bucharest

Europe/Sofia

Egypt

Europe/Tirane

Africa/Harare

Europe/Helsinki

Asia/Jerusalem

Asia/Baghdad

Asia/Kuwait

Europe/Moscow

Africa/Nairobi

Africa/Dar//es//Salaam

Iran

Asia/Muscat

Asia/Baku

Asia/Kabul

Indian/Kerguelen

Asia/Yekaterinburg

Asia/Karachi

Asia/Calcutta

Asia/Mumbai

Asia/Katmandu

Asia/Novosibirsk

Asia/Dhaka

Indian/Chagos

Asia/Colombo

Asia/Rangoon

Asia/Bangkok

Asia/Krasnoyarsk

Asia/Hong//Kong

Asia/Ulaanbaatar

Asia/Singapore

Australia/Perth

Asia/Taipei

Japan

Asia/Seoul

Asia/Yakutsk

Australia/Adelaide

Australia/Darwin

Australia/Brisbane

Australia/Sydney

Pacific/Guam

Australia/Hobart

Asia/Vladivostok

Asia/Magadan

Pacific/Auckland

Pacific/Fiji

Pacific/Tongatapu

The Etc/GMT+12 value represents International Date Line West.

---

device.local.contact.country
Country where support is located.
String (0-64)

device.local.country
Country where your system is located.
Not set (default)

Afghanistan

Albania

Algeria

American Samoa

Andorra

Angola

Anguilla

Antarctica

Antigua

Argentina

Armenia

Aruba

Ascension Islands

Australia

Australian Ext. Territories

Austria

Azerbaijan

Bahamas

Bahrain

Bangladesh

Barbados

Barbuda

Belarus

Belgium

Belize

Benin Republic

Bermuda

Bhutan

Bolivia

Bosnia and Herzegovina

Botswana

Brazil

British Virgin Islands

British Indian Ocean Territory

Brunei

Bulgaria

Burkina Faso

Burma (Myanmar)

Burundi

Cambodia

Cameroon United Republic

Canada

Cape Verde Island

Cayman Islands

Central African Republic

Chad Republic

Chile

China

Christmas Island

Cocos Islands

Colombia

Comoros

Congo

Congo Democratic Republic

Cook Islands

Costa Rica

Croatia

Cuba

Curacao

Cyprus

Czech Republic

Denmark

Diego Garcia

Djibouti

Dominica

Dominican Republic

Easter Island

East Timor

Ecuador

Egypt

El Salvador

Equatorial Guinea

Eritrea

Estonia

Ethiopia

Faeroe Islands

Falkland Islands

Fiji Islands

Finland

France

French Antilles

French Guiana

French Polynesia

French Southern and Antarctic Lands

Gabon

Gambia

Georgia

Germany

Ghana

Gibraltar

Greece

Greenland

Grenada

Guadeloupe

Guam

Guantanamo Bay

Guatemala

Guinea

Guernsey

Guinea-Bissau

Guyana

Haiti

Honduras

Hong Kong

Hungary

Iceland

India

Indonesia

Inmarsat (Atlantic Ocean West)

Inmarsat (Atlantic Ocean East)

Inmarsat (Indian Ocean)

Inmarsat (Pacific Ocean)

Inmarsat (SNAC)

Iran

Iraq

Ireland

Israel

Italy

Ivory Coast

Jamaica

Japan

Jersey

Jordan

Kazakhstan

Kenya

Kiribati

Korea North

Korea South

Kosovo

Kuwait

Kyrgyzstan

Laos

Latvia

Lebanon

Lesotho

Liberia

Libya

Liechtenstein

Lithuania

Luxembourg

Macao

Macedonia

Madagascar

Malawi

Malaysia

Maldives

Mali

Malta

Man, Isle of

Mariana Islands

Marshall Islands

Martinique

Mauritania

Mauritius

Mayotte Island

Mexico

Micronesia

Midway Island

Moldova

Monaco

Mongolia

Montenegro

Montserrat

Morocco

Mozambique

Myanmar (Burma)

Namibia

Nauru

Nepal

Netherlands

Netherlands Antillies

Nevis

New Caledonia

New Zealand

Nicaragua

Niger

Nigeria

Niue

Norfolk Island

Norway

Oman

Pakistan

Palau

Palestine

Panama

Papua New Guinea

Paraguay

Peru

Philippines

Pitcairn

Poland

Portugal

Puerto Rico

Qatar

Reunion Island

Romania

Russia

Rwanda

St Helena

St Kitts

St Lucia

St Pierre and Miquelon

St Vincent

San Marino

Sao Tome and Principe

Saudi Arabia

Senegal

Serbia

Seychelles

Sierra Leone

Singapore

Slovakia

Slovenia

Solomon Islands

Somalia Republic

South Africa

Spain

Sri Lanka

Sudan

Suriname

Swaziland

Sweden

Switzerland

Syria

Taiwan

Tajikistan

Tanzania

Thailand

Togo

Tonga

Trinidad and Tobago

Tunisia

Turkey

Turkmenistan

Turks and Caicos

Tuvalu

Uganda

Ukraine

United Arab Emirates

United Kingdom

United States

Uruguay

US Minor Outlying Islands

US Virgin Islands

Uzbekistan

Vanuatu

Vatican City

Venezuela

Vietnam

Wake Island

Wallis And Futuna Islands

Western Samoa

Yemen

Zambia

Zanzibar

Zimbabwe

`device.local.language`
Sets the language displayed on the system.
ENGLISHUS (default)

ARABIC

ENGLISHUK

GERMAN

SPANISH

FRENCH

ITALIAN

JAPANESE

KOREAN

HUNGARIAN

NORWEGIAN

POLISH

PORTUGUESE

RUSSIAN

CHINESE

CHINESET

Required Network Parameters

Use the following parameters to configure some network settings for your system.

Provisioning Basic Wired LAN Properties

You can provision your G7500 and Studio X series system to automatically obtain some wired LAN properties—including IP address, subnet mask, default gateway, and DNS server(s)—by setting `device.net.mode="Automatically"`.

These LAN properties can also be provisioned individually by setting `device.net.mode="Manually"`. In this situation, you must set all of the following additional parameters or no LAN properties will provision successfully:

- `device.net.ipAddress`

- `device.net.subnetMask`

- `device.net.ipGateway`

📝 **NOTE:** Setting `device.net.dns.server.*` parameters is optional when `device.net.mode="Manually"`.

When your system obtains these LAN properties automatically, you can't then overwrite individual properties by setting `device.net.ipAddress="192.0.2.255"`, for example.

When provisioning a new IP address for your system, active sessions through the system web interface don't automatically refresh. You must enter the new IP address in your browser to re-establish access.

Provisioning Basic Wi-Fi Properties

You can provision your G7500 and Studio X series system to automatically obtain some Wi-Fi properties—including IP address, subnet mask, default gateway, and DNS server(s)—by setting `device.net.secondaryNetwork.mode="Automatically"`.

These Wi-Fi properties can also be provisioned individually by setting `device.net.secondaryNetwork.mode="Manually"`. In this situation, you must set all of the following additional parameters or no Wi-Fi properties will provision successfully:

- `device.net.secondaryNetwork.ipAddress`

- `device.net.secondaryNetwork.subnetMask`

- `device.net.secondaryNetwork.ipGateway`

📝 NOTE: Setting `device.net.secondaryNetwork.dns.server.*` parameters is optional when `device.net.secondaryNetwork.mode="Manually"`.

When your system obtains these Wi-Fi properties automatically, you can't then overwrite individual properties by setting `device.net.secondaryNetwork.ipAddress="192.0.2.255"`, for example.

When provisioning a new IP address for your system, active sessions through the system web interface don't automatically refresh. You must enter the new IP address in your browser to re-establish access.

Remember, to successfully provision any Wi-Fi setting, you must set `device.net.secondaryNetwork.type="WiFi"`.

Network Parameters

`device.net.dns.server.1`
If the system does not automatically obtain a DNS server address on the wired LAN, enter one here.
String

`device.net.dns.server.2`
(Optional) If the system does not automatically obtain a DNS server address on the wired LAN, enter one here.
String

`device.net.dns.server.3`
(Optional) If the system does not automatically obtain a DNS server address on the wired LAN, enter one here.
String

`device.net.dns.server.4`
(Optional) If the system does not automatically obtain a DNS server address on the wired LAN, enter one here.
String

`device.net.ipAddress`
Specifies the system IPv4 address on the wired LAN.
You don't need to set this if device.net.mode="Automatically".

String

0.0.0.0

device.net.ipGateway
Specifies the IP gateway on the wired LAN.
You don't need to set this if device.net.mode="Automatically".

String

0.0.0.0

device.net.mode
Specifies how you want to configure your system IPv4 address on the wired LAN.
If set to "Automatically", make sure you have a DHCP server in your environment.

Automatically (default)

Manually

device.wifi.enable
Enables or disables Wi-Fi wireless communication on your system.
Setting to "False" turns off screen mirroring with Miracast-certified devices and prevents the system from using Wi-Fi to connect to a secondary network.

True (default)

False

device.net.secondaryNetwork.type
Specifies if you want your system to connect to a secondary network over Wi-Fi so that guest users can share content to the system using an AirPlay-certified device or the Polycom Content App.
None (default)

WiFi

Caution: In Partner Mode, make sure you set this parameter to 'None'.

device.net.secondaryNetwork.wifi.ssid
Specifies the name of the Wi-Fi network you're connecting systems to.
String (0-32)

device.net.secondaryNetwork.wifi.securityType
Specifies the Wi-Fi network encryption protocol.
WPA_PSK (default)

None

WEP

802_1xEAP

device.net.secondaryNetwork.wifi.WEP.key
Specifies the WEP key.
You should set this if device.net.secondaryNetwork.wifi.securityType="WEP".

String

device.net.secondaryNetwork.wifi.dot1xEAP.method
Specifies the extensible authentication protocol (EAP) for WPA-Enterprise (802.1xEAP).
You should set this if device.net.secondaryNetwork.wifi.securityType="802_1xEAP".

PEAP (default)

TLS

TTLS

PWD

device.net.secondaryNetwork.wifi.dot1xEAP.phase2Auth
Specifies the Phase 2 authentication method.
You should set this if device.net.secondaryNetwork.wifi.securityType="802_1xEAP".

MSCHAPV2 (default)

GTC

device.net.secondaryNetwork.wifi.WPA.password
Specifies an encryption passphrase (like a password) for the Wi-Fi network. You must enter the
passphrase to connect to the Wi-Fi network.
You should set this if device.net.secondaryNetwork.wifi.securityType="WPA_PSK".

String

device.net.secondaryNetwork.wifi.dot1xEAP.identity
Specifies the login username for WPA-Enterprise (802.1xEAP).
You should set this if device.net.secondaryNetwork.wifi.securityType="802_1xEAP".

String

device.net.secondaryNetwork.wifi.dot1xEAP.password
Specifies the login password for WPA-Enterprise (802.1xEAP).
You should set this if device.net.secondaryNetwork.wifi.securityType="802_1xEAP".

String

device.net.secondaryNetwork.dns.server.1
Specifics the DNS server address on the Wi-Fi network.
String

device.net.secondaryNetwork.dns.server.2
Specifics the alternate DNS server address on the Wi-Fi network.
String

device.net.secondaryNetwork.ipAddress
Specifies the system IPv4 address on the Wi-Fi network.
String

0.0.0.0

device.net.secondaryNetwork.ipGateway
Specifies the IP gateway for the Wi-Fi network.
String

0.0.0.0

device.net.secondaryNetwork.mode
Specifies how you want to configure your system Wi-Fi network IP address.
If you set "Automatically", make sure you have a DHCP server in your environment.

Automatically (default)

Manually

device.net.secondaryNetwork.subnetMask
Specifies the subnet mask address for the Wi-Fi network.
String

255.255.255.0

device.net.subnetMask
Specifies the subnet mask address for the wired LAN.
You don't need to set this if device.net.mode="Automatically".

String

255.255.255.0

device.net.domain
Identifies the domain your system belongs to.
You can optionally set this if the system does not automatically obtain a domain name.

String

device.net.dot1x.enable
Specifies whether EAP/802.1X network access is enabled. The following authentication protocols are supported:
EAP-MD5

EAP-PEAPv0 (MSCHAPv2)

EAP-TTLS

EAP-TLS

False (default)

True

device.net.dot1x.identity
Specifies the system's identity used for 802.1X authentication.
String (0-64)

device.net.dot1x.password
Specifies the system's password used for 802.1X authentication. This setting is required when EAP-MD5, EAP-PEAPv0, or EAP-TTLS is used.
String

device.net.echo.enable
When enabled, your system sends an ICMP Echo Reply message in response to a broadcast or multicast Echo Request that isn't specifically addressed to the system.
False (default)

True

device.net.ethernet.autoNegotiation
Specifies whether the system should automatically negotiate the LAN speed and duplex mode per IEEE 802.3 autonegotiation procedures.
Poly recommends that you use autonegotiation to avoid network issues.

If enabled, you don't have to set device.net.ethernet.portSpeed or device.net.ethernet.duplexMode.

True (default)

False

device.net.ethernet.duplexMode
Specifies the duplex mode to use. Note that the speed you choose must be supported by the switch.
You don't need to set this if device.net.ethernet.autoNegotiation="True".

Half (default)

Full

device.net.ethernet.portSpeed
Specifies the wired LAN speed to use. Note that the speed you choose must be supported by the switch.
You don't need to set this if device.net.ethernet.autoNegotiation="True".

100Mbps (default)

10Mbps

1000Mbps

device.net.hostName
Indicates your system name. If the system discovers a valid name during setup or a software update, the system automatically creates the hostname. However, if an invalid name is found, such as a name with a space, the system creates a hostname using the following format: SystemType-xxxxxx, where xxxxxx is a set of random alphanumeric characters.
IPv4 networks: The system sends the host name to the DHCP server to attempt to register the name with the local DNS server or look up the domain where the system is registered (if supported).

String (0-36)

roomseries

device.net.icmp.txRateLimit
Specifies the minimum number of milliseconds between transmitted packets.
The default value of 1000 means the system sends 1 packet per second. If you enter 0, the transmission rate limit is disabled.

This setting applies only to "error" ICMP packets. This setting has no effect on "informational" ICMP packets, such as echo requests and replies.

1000 (default)

Integer (0-60000)

device.net.ignoreRedirect
Enables the system to ignore ICMP redirect messages.
Poly recommends you enable this setting in most circumstances.

True (default)

False

device.net.lldp.enable
Specifies if you want the system to advertise itself on the network using the Link Layer Discovery Protocol (LLDP).
Set to "True" if you want your system to operate on a virtual LAN (VLAN).

If set to "True", device.net.vlan.enable and device.net.vlanid should be automatically configured.

False (default)

True

`device.net.unreachableTx.enable`
Generates an ICMP Destination Unreachable message if a packet cannot be delivered to its destination for reasons other than network congestion.
True (default)

False

`device.net.vlan.audioPriority`
Sets the link layer priority of audio traffic on the wired LAN. Audio traffic is RTP traffic consisting of audio data and associated RTCP traffic.
Setting "6" or "7" isn't recommended.

To use this parameter, you should set device.net.lldp.enable="True".

You can't set this parameter in Partner Mode.

0 (default)

1

2

3

4

5

6

7

`device.net.vlan.controlPriority`
Sets the link layer priority of control traffic on the wired LAN. Control traffic is consists of control information associated with a call:
H.323: H.225.0 Call Signaling, H.225.0 RAS, H.245, Far-End Camera Control (FECC)

SIP: SIP Signaling, FECC, Binary Floor Control Protocol (BFCP)

Setting "6" or "7" isn't recommended.

To use this parameter, you should set device.net.lldp.enable="True".

You can't set this parameter in Partner Mode.

0 (default)

1

2

3

4

5

6

7

`device.net.vlan.enable`
Enable if you want to configure your system with a virtual LAN (VLAN) and and set link layer priorities.
False (default)

True

`device.net.vlan.videoPriority`
Sets the link layer priority of video traffic on the wired LAN. Video traffic is RTP traffic consisting of video data and associated RTCP traffic.
Setting "6" or "7" isn't recommended.

To use this parameter, you should set device.net.lldp.enable="True".

You can't set this parameter in Partner Mode.

0 (default)

1

2

3

4

5

6

7

`device.net.vlanid`
Identifies the VLAN you want your system to operate on.
To use this parameter, you should set device.net.vlan.enable="True".

1 (default)

Integer (1-4095)

`net.firewall.fixedPorts.enable`
If enabled, you can define which TCP and UDP ports your system uses for firewall traversal.
Enable if your firewall isn't H.323 compatible. Disable if your firewall is H.323 compatible or the system isn't behind a firewall.

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

For the fixed ports you configure, you must open the corresponding ports on your firewall. For H.323, open TCP port 1720. For SIP, open UDP port 5060, TCP 5060, or TCP 5061 depending on if you're using UDP, TCP, or TLS, respectively, as the SIP transport protocol.

net.firewall.fixedPorts.tcpStart
The starting value for the range of TCP ports used by the system. The system automatically
configures the range based on the beginning value you set here.
The system assigns a port range starting with the TCP and UDP ports you specify (port 3230 is where
the range begins by default).

To allow H.323 traffic, you need two TCP and eight UDP ports per connection. You must also open
TCP port 1720 on the firewall.

To allow SIP traffic, you need TCP port 5060 and eight UDP ports per connection.

Fixed ports range and filters: You might notice that the source port of a SIP signaling message is not
in the fixed ports range. When your firewall is filtering on source ports, in the system web interface,
set voIpProt.SIP.forceConnectionReuse="True". When enabled, the system uses port 5060 and 5061
for the source and destination port (these must be open on the firewall).

You can't provision this parameter if the system is in Partner Mode.

Integer (1024-65522)

3230 (default)

net.firewall.fixedPorts.udpStart
The starting value for the range of UDP ports used by the system. The system automatically
configures the range based on the beginning value you set here.
To allow H.323 traffic, you need two TCP and eight UDP ports per connection. You must also open
TCP port 1720 on the firewall.

To allow SIP traffic, you need TCP port 5060 and eight UDP ports per connection.

Because systems support ICE, the range of fixed UDP ports is 32. The system cycles through the
available ports from call to call.

Fixed ports range and filters: You might notice that the source port of a SIP signaling message is not
in the fixed ports range. When your firewall is filtering on source ports, in the system web interface,
set voIpProt.SIP.forceConnectionReuse="True". When enabled, the system uses port 5060 and 5061
for the source and destination port (these must be open on the firewall).

You can't provision this parameter if the system is in Partner Mode.

Integer (1024-65424)

3230 (default)

net.firewall.h460.enable
Allows the system to be configured for H.460 firewall/NAT traversal.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

net.firewall.nat.gabAddressDisplayed
Sets whether to display the system's public or private address in the global directory.
To use this parameter, make sure net.firewall.nat.useNatAddress is set to "Auto" or "Manual".

You can't provision this parameter if the system is in Partner Mode.

Public (default)

Private

net.firewall.nat.h323Compatible
Identifies whether the system is behind a NAT that can translate H.323 traffic.
To use this parameter, make sure net.firewall.nat.useNatAddress is set to "Auto" or "Manual".

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

net.firewall.nat.publicAddress
The address callers from outside the LAN use to call your system. If you configured the NAT manually (net.firewall.nat.useNatAddress="Manual"), set the NAT public address here.
You can't provision this parameter if the system is in Partner Mode.

String (0-255)

0.0.0.0 (default)

net.firewall.nat.useNatAddress
Specifies if the system should automatically determine the NAT public (WAN) address.
If the system is not behind a NAT or is connected to the network through a VPN, set to "Off".

If the system is behind a NAT that allows HTTP traffic, set to "Auto".

If the system is behind a NAT that does not allow HTTP traffic, set to "Manual".

You can't provision this parameter if the system is in Partner Mode.

Off (default)

Auto

Manual

net.proxy.address
The web proxy address.
You can't provision this parameter if the system is in Partner Mode.

Set this parameter if net.proxy.autoconf="False".

String (0-1024)

net.proxy.autoconf
Set to "True" for the following web proxy configuration methods:
Automatic: Your system obtains a URL for downloading a proxy auto-configuration (PAC) file through DHCP option 252. With this method, you may have to also set proxy credentials.

Semi-automatic: You specify the proxy credentials and URL for automatically downloading a PAC file.

Set to "False" for manual configuration. You must then specify the proxy address, port, and credentials. This method lets you configure your system with only one proxy.

You can't provision this parameter if the system is in Partner Mode.

True (default)

False

net.proxy.pacfile.url
The address from which your system downloads the PAC file.
You can't provision this parameter if the system is in Partner Mode.

String (0-1024)

net.proxy.port
The web proxy port.
Set this parameter if net.proxy.autoconf="False".

You can't provision this parameter if the system is in Partner Mode.

Integer (1-65535)

8080 (default)

net.proxy.webproxy.auth.password
The password for connecting your system with the web proxy.
You can't provision this parameter if the system is in Partner Mode.

String

Credentials may not be needed if your system is automatically configured with a proxy.

net.proxy.webproxy.auth.userName
The username for connecting your system with the web proxy.
You can't provision this parameter if the system is in Partner Mode.

String (0-64)

Credentials may not be needed if your system is automatically configured with a proxy.

net.proxy.webproxy.blockBasicAuth
Specifies if you want to allow your system to use basic authentication (disabled by default) when connecting with a web proxy.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

net.proxy.webproxy.enable
Enable to allow your system to be configured with web proxies.
You can't provision this parameter if the system is in Partner Mode.

False (default)

True

net.proxy.wpad.enable
Set to "True" if net.proxy.autoconf="True" and you prefer the automatic web proxy configuration method. Enabling the web proxy auto-discovery protocol (WPAD) helps your system automatically download the PAC file on your network using DHCP option 252.
Set to "False" if you prefer semi-automatic web proxy configuration, where you specify the proxy credentials and URL for automatically downloading a PAC file.

You can't provision this parameter if the system is in Partner Mode.

True (default)

False

Required System Conferencing Provider Parameter

This system conferencing provider parameter is required to successfully set the system's conferencing application.

`management.provider.select`
Specifies the system's conferencing provider.
Poly

Zoom Rooms

Microsoft Teams

GoToRoom

RingCentral Rooms

Device Mode

StarLeaf

BlueJeans Rooms (This is a beta feature only.)

Dialpad Conference Room

4   Recommended Parameters

These parameters are recommended to successfully run your system.

Recommended Software Update Parameters

Use the following parameters to update your software.

upgrade.auto.enable
Controls whether the software of your system and its connected peripheral devices automatically updates.
False (Teams and Zoom default)

True (All other conferencing providers default)

upgrade.auto.timeFrame.enable
If you've configured automatic software updates (upgrade.auto.enable="True"), you can restrict those updates to occur only during a maintenance window.
If set to "True", make sure you also configure upgrade.auto.timeFrame.startTime and upgrade.auto.timeFrame.stopTime.

False (Teams and Zoom default)

True (All other conferencing providers default)

upgrade.auto.timeFrame.startTime
Specifies when the maintenance window starts. Set a value using 24-hour clock format (HH:MM). For example, "23:30" is an acceptable value.
String

01:00 (default)

upgrade.auto.timeFrame.stopTime
Specifies when the maintenance window ends. Set a value using 24-hour clock format (HH:MM). For example, "05:30" is an acceptable value.
String

05:00 (default)

upgrade.auto.polling.interval
If you've configured automatic software updates (upgrade.auto.enable="True"), you can specify how often (in seconds) your system checks with Poly Clariti Manager to see if there's a new update to download. The default value "3600" means your system checks for updates once every hour.
Doing either of the following turns this feature off:

Disable provisioning (you can do this only in the system web interface).

Enable an automatic update maintenance window by setting upgrade.auto.timeFrame.enable="True". (The maintenance window takes priority over automatic polling.)

Integer > 300

3600 (default)

Recommended System Display Parameters

Provide a description of the parameters in this topic. Use the following parameters to configure a feature you might enjoy using for your products.
device.local.contact.email
Support email address.
String (0-64)

device.local.contact.fax
Support fax number.
String (0-64)

device.local.contact.organization
Name of organization where device is located.
String (0-64)

device.local.contact.person
Name of primary support contact.
String (0-64)

device.local.contact.phone
Phone number of primary support contact.
String (0-64)

device.local.contact.site
Site where device is located.
String (0-64)

device.local.contact.state
State where support is located.
String (0-64)

device.local.contact.techSupport
Additional support contact.
String (0-64)

device.local.roomName
Specifies the room where your system resides.
The room name displays on the screens of call participants.

String (1-40)

G7500 (default)

device.remoteControl.audioConfirm
Specifies whether to play a voice confirmation of numbers selected with the remote control or keypad.
True (default)

False

`device.remoteControl.numKeypadInCall`
Specifies whether pressing number buttons on the remote control or keypad moves the camera to presets or generates touch tones (DTMF tones).
If set to "Presets", you can generate DTMF tones by pressing the # key on the remote control while on a video screen.

Presets (default)

Tones

`device.remoteControl.poundButtonFunction`
Specifies the behavior of the # button on the remote control.
pound_then_at (default) - Pressing the # button once displays the hash symbol. Pressing the # button twice quickly displays the @ symbol.

at_then_pound - Pressing the # button once displays the @ symbol. Pressing the # button twice quickly displays the # symbol.

`device.remoteControl.starButtonFunction`
Specifies the behavior of the * button on the remote control.
period_then_star (default) - Pressing the * button once displays the * symbol. Pressing the * button twice quickly displays a period.

star_then_period - Pressing the * button once displays a period. Pressing the * button twice quickly displays the * symbol.

`device.screenSaver.mode`
Specifies if you want to display a black screen or no signal message when your system goes to sleep.
You can't provision this parameter if the system is in Partner Mode.

NoSignal (default)

Black

`device.sleepTimeout`
Specifies how many minutes the device can be idle before it goes to sleep.
0 (default)

1

3

15

30

45

60

120

240

480

`homeScreen.addressBar.primary`
Specifies the main element that displays on the home screen address bar.
You can't provision this parameter if the system is in Partner Mode.

LAN IP Address (default)

Wi-Fi IP Address

SIP Address

H.323 Extension

None

`homeScreen.addressBar.secondary`
Specifies the secondary element that displays on the home screen address bar.
You can't provision this parameter if the system is in Partner Mode.

SIP Address (default)

LAN IP Address

Wi-Fi IP Address

H.323 Extension

None

`homeScreen.backgroundImage`
Specify a background image for the home screen.
You can't provision this parameter if the system is in Partner Mode.

String

The image must have a 16:9 resolution between 1280x720 and 3840x2160 (Poly recommends 1920x1080, 2560x1440, or 3840x2160). JPEG and PNG formats with a file size of less than 10 MB are supported.

If the image requirements (resolution, format, and size) are not met, provisioning of this parameter fails.

The path to the image must be absolute; relative paths do not work.

NOTE: Setting this parameter with an empty string applies the default background image.

`homeScreen.topWidgetType`
Determines if meeting information or favorite contacts display on the local interface home screen. You also can hide this information by setting "none".
You can't provision this parameter if the system is in Partner Mode.

calendar (default)

favorites

Recommended Security Parameters

Use the following parameters to configure security settings on your system.

Provisioning Updated PKI Certificates and CRLs

During provisioning, your G7500 and Studio X series system checks if a new public key infrastructure (PKI) certificate is just an updated version of an installed certificate.

If the certificate contents have changed since it was last successfully provisioned or manually installed (for example, there's a new expiration date), the new certificate is applied and the older one is deleted. If the certificate hasn't changed, the new certificate is ignored.

This is not the case with certificate revocation lists (CRLs), which are replaced each time your system is provisioned even if the CRL hasn't changed.

Security Parameters

`cast.miracast.enforcepin`
For enhanced security, you can require that Windows users enter a security code each time they connect to the system with their Miracast-certified device.
You can't provision this parameter if the system is in Partner Mode.

False (default)

True

This feature applies only to Windows 10 version 1709 and later.

To use this feature, you must set sec.access.room.secCode.enable="True".

When you set content.miracast.enable="False", this parameter resets to its default value.

`sec.access.maxSessions`
Sets the maximum number of connected sessions through the system web interface and command-line API (SSH or telnet).
50 (default)

45

40

35

30

25

20

15

10

`sec.auth.portLockout.failedLoginWindow`
Specifies the number of hours, starting with the first failed login attempt, during which subsequent failed login attempts are counted against the maximum number allowed (sec.auth.portLockout.lockoutAttempts).
The counter resets when the set period of time expires or a user successfully logs in.

Off (default)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

sec.auth.portLockout.lockoutAttempts
The number of failed login attempts allowed before the web interface locks.
Off (default)

2

3

4

5

6

7

8

9

10

`sec.auth.portLockout.lockoutTime`
Specifies the number of minutes that the web interface remains locked due to failed login attempts.
When this period expires, the failed login attempts counter resets and you can try to log in again.
1 (default)

2

3

5

10

20

30

60

120

240

480

`sec.auth.portLockout.ssh.failedLoginWindow`
Specifies the number of hours, starting with the first failed login attempt, during which
subsequent failed login attempts are counted against the maximum number allowed
(sec.auth.portLockout.ssh.lockoutAttempts).
The counter resets when the set period of time expires or a user successfully logs in.

Off

1 (default)

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

`sec.auth.portLockout.ssh.lockoutAttempts`
Specifies the number of failed login attempts allowed before SSH access to the API locks.
Off

2

3 (default)

4

5

6

7

8

9

10

`sec.auth.portLockout.ssh.lockoutTime`
Specifies the amount of time that SSH access to the API remains locked due to failed login attempts.
When this period expires, the failed login attempts counter resets and you can try to log in again.
1 (default)

2

3

5

10

20

30

60

120

240

480

sec.nids.enable
When set to "True", the system creates security log entries when it detects a possible network intrusion.
False (default)

True

sec.telnet.apiPort
Specifies whether to use port 23 or 24 for command-line API access.
24 (default)

23

sec.telnet.apiPortIdleTimeout.enable
Specifies whether to allow the command-line API port to time out at the configured time interval or not.
The timeout is set using sec.web.idleSessionTimeout.

False (default)

True

sec.telnet.diagPortIdleTimeout.enable
Specifies whether to allow the diagnostics port to time out at the configured time interval or not.
The timeout is set using sec.web.idleSessionTimeout.

False (default)

True

sec.telnet.enable
Specifies whether you can access the system using telnet.
False (default)

True

sec.web.enable
Specifies whether you can access the system using its web interface.
True (default)

False

sec.web.idleSessionTimeout
Specifies the number of minutes a session can be idle before it times out.
1

3

5

10 (default)

15

20

30

45

60

120

240

480

sec.usb.disableAll
Set to "True" to prevent use of the system's USB ports.
Note: You can't completely turn off the USB-C port; it still provides power.

If you disable the system's USB ports, you can't use the system as an external camera, microphone, and speaker accessory (i.e., Poly Device Mode).

False (default)

True

sec.TLS.cert.sslVerificationDepth
Specifies how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host when a network connection is being established between the two systems.
0

1

2 (default)

3

4

5

6

7

8

9

10

11

12

sec.TLS.cert.validatePeer.enable
Determines whether your system requires a remote server to present a valid certificate when connecting to it for services, such as provisioning.
False (default)

True

sec.TLS.customCaCert.1
Specifies a CA-signed PKI certificate to install on your system.
Your system accepts the following certificate file formats: .pem, .der, and PKCS #7 (which typically has a .p7b filename extension).

String

sec.TLS.customCaCert.2
Specifies a CA-signed PKI certificate to install on your system.
Your system accepts the following certificate file formats: .pem, .der, and PKCS #7 (which typically has a .p7b filename extension).

String

sec.TLS.customCaCert.3
Specifies a CA-signed PKI certificate to install on your system.
Your system accepts the following certificate file formats: .pem, .der, and PKCS #7 (which typically has a .p7b filename extension).

String

sec.TLS.revocation.crl.1
Specifies a CRL to install on your system for certificate revocation checks.
Installing a CRL will fail unless you've installed all of the certificates in the issuing CA's chain of trust for that CRL.

To use this parameter, make sure to set sec.TLS.revocation.ocsp.enable="False".

String

sec.TLS.revocation.crl.2
Specifies a CRL to install on your system for certificate revocation checks.
Installing a CRL will fail unless you've installed all of the certificates in the issuing CA's chain of trust for that CRL.

To use this parameter, make sure to set sec.TLS.revocation.ocsp.enable="False".

String

sec.TLS.revocation.crl.3
Specifies a CRL to install on your system for certificate revocation checks.
Installing a CRL will fail unless you've installed all of the certificates in the issuing CA's chain of trust for that CRL.

To use this parameter, make sure to set sec.TLS.revocation.ocsp.enable="False".

String

sec.TLS.revocation.looseRevocation.enable
CRL method: When you enable this parameter, a certificate in the chain of trust validates without a revocation check if no corresponding CRL from the issuing CA is installed.

OCSP method: When you enable this parameter, your system considers a revocation check successful if there is no response or the OCSP responder indicates a certificate's status is unknown. Regardless of how you configure this paramter, the following statements apply:

If the OCSP responder indicates a known revoked status, your system treats it as a revocation check failure and doesn't allow the connection. If the OCSP responder indicates a known good status, your system treats it as a successful revocation check and allows the connection

False (default)

True

sec.TLS.revocation.ocsp.enable
Specifies the certificate revocation method you want to use.
False (default) - Set to use the CRL method of revocation.

True - Set to use the OCSP method of revocation.

sec.TLS.revocation.ocsp.responderAddress
Specifies the URI of the OCSP responder (e.g., http://responder.example.com/ocsp). The responder is used when sec.TLS.revocation.ocsp.useResponderInCert is disabled and sometimes even when it's enabled. Poly recommends you always include a URI in this field regardless of how sec.TLS.revocation.ocsp.useResponderInCert is configured.
To use this parameter, make sure to set sec.TLS.revocation.ocsp.enable="True".

String

sec.TLS.revocation.ocsp.useResponderInCert
Some certificates include the OCSP responder address. When this parameter is enabled, your system attempts to use this address (when present) instead of the global responder address you specified in sec.TLS.revocation.ocsp.responderAddress.
To use this parameter, make sure to set sec.TLS.revocation.ocsp.enable="True".

False (default)

True

NOTE: Only HTTP URLs in a certificate's AIA field are supported.

---

sec.ssh.enable
Specifies if you can access the command-line API using SSH (port 22).
False (default)

True

sec.auth.external.AD.adminGroup
Specifies the Active Directory group whose members should have administrator access to the system. This name must exactly match the name in the AD server for successful authentication.
String (0-512)

sec.auth.external.AD.enable
Specifies whether to authenticate users with Active Directory server. When AD authentication is enabled, users can log in to the system with their network credentials using this format: domain\user. With this format, users can have accounts on multiple domains.
False (default)

True

`sec.auth.external.AD.server.address`

Specifies the Active Directory server's fully qualified domain name (FQDN) or IP address. If you are using subdomains, append port number 3268 as follows: ad.domain.com:3268.
You can alternatively use Poly Clariti Manager as an AD server and enter its address here.

If sec.TLS.cert.validatePeer.enable="True", make sure this value matches what is in the AD server certificate. For example, if you enter the AD server IP address here, but the certificate only has the server's FQDN, external authentication will fail.

String (0-256)

`sec.auth.external.AD.userGroup`

Specifies the Active Directory group whose members should have user access to the system. This name must exactly match the name in the AD server for successful authentication.
String (0-512)

`sec.TLS.minimumVersion`

You can restrict your system from using earlier versions of TLS for secure communications.
For example: If you set this parameter to "tlsv1_1", you are disabling TLS 1.0.

tlsv1_2 (default)

tlsv1

tlsv1_1

`sec.auth.accountLockout.admin.failedLoginWindow`

Determines how many hours the failed login window lasts. The window is a period of time starting with the first failed login attempt and during which subsequent failed attempts are counted against the number allowed.
The counter resets to zero at the end of the window (if the account is not locked because of failed attempts) and after a successful login.

Off (default)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

sec.auth.accountLockout.admin.lockoutAttempts
Specifies the number of failed login attempts allowed before the system locks the account.
Off (default)

1

2

3

4

5

6

7

8

9

10

sec.auth.accountLockout.admin.lockoutTime
Specifies the amount of time an account is locked because of failed login attempts. After this period expires, the failed login attempts counter is reset to zero and users can again log in with that account.
1 (default)

2

3

5

sec.auth.admin.id
The local administrator account name.
String (can be a combination of letters and numbers)

admin (default)

sec.auth.admin.password
If set, this password must be entered to access the system through the web interface or command-line API (SSH or telnet).
To successfully provision this parameter, you must set sec.auth.admin.useRoomPassword="False".

String

sec.auth.admin.room.password
If set, this password (also referred to as the Room Password) must be entered to change administrator settings in the local interface.
String

sec.auth.admin.useRoomPassword
When set to "True", the password configured for sec.auth.admin.room.password is also used for accessing the system remotely.
True (default)

False

sec.auth.admin.room.password.canContainIdOrReverse
Specifies whether the associated ID or its reverse can be part of a password. If this setting is enabled and the ID is "admin", passwords "admin" and "nimda" are allowed.
True (default)

False

sec.auth.admin.room.password.expirationWarning
Specifies how many days in advance a warning displays indicating that the password will soon expire (if a maximum password age is set).
Off (default)

1

2

3

4

5

6

7

sec.auth.admin.room.password.lowercaseCount
The minimum number of lowercase letters required for a valid password.
Off (default)

1

2

All

sec.auth.admin.room.password.maxAge
The maximum number of days before the password must change.
Off (default)

30

60

90

100

110

120

130

140

150

160

170

180

`sec.auth.admin.room.password.maxRepeatedChars`
The maximum number of consecutive repeated characters in a password. For example, if set to "3", aaa123 is a valid password but aaaa123 is not.
Off (default)

1

2

3

4

`sec.auth.admin.room.password.minAge`
The minimum number of days before the password can change.
Off (default)

1

5

10

15

20

30

`sec.auth.admin.room.password.minChangedChars`
The number of characters that must be different or change position in a new password. For example, if set to "3", 123abc can change to 345cde but not to 234bcd.
Off (default)

1

2

3

4

All

sec.auth.admin.room.password.minLength
The minimum number of characters required for a valid password.
Off (default)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

32

sec.auth.admin.room.password.numCount
The minimum amount of numbers required for a valid password.
Off (default)

1

2

All

sec.auth.admin.room.password.rejectPrevPassword
The number of most recent passwords that cannot be reused. If set to "Off", all previous passwords
are valid.
Off (default)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

`sec.auth.admin.room.password.specialCharCount`
The minimum number of special characters required for a valid password. Supported characters
include: @ - _ ! ; $, \ / & . # *
Off (default)

1

2

All

`sec.auth.admin.room.password.uppercaseCount`
The minimum number of uppercase letters required for a valid password.
Off (default)

1

2

All

`sec.auth.remote.password.canContainIdOrReverse`
Specifies whether the associated ID or its reverse can be part of a password. If this setting is enabled
and the ID is "admin", passwords "admin" and "nimda" are allowed.
True (default)

False

`sec.auth.remote.password.expirationWarning`
Specifies how many days in advance a warning displays indicating that the password will soon expire
(if a maximum password age is set).

Off (default)

1

2

3

4

5

6

7

sec.auth.remote.password.lowercaseCount
The minimum number of lowercase letters required for a valid password.
Off (default)

1

2

All

sec.auth.remote.password.maxAge
The maximum number of days before the password must change.
Off (default)

30

60

90

100

110

120

130

140

150

160

170

180

sec.auth.remote.password.maxRepeatedChars
The maximum number of consecutive repeated characters in a password. For example, if set to "3", aaa123 is a valid password but aaaa123 is not.
Off (default)

1

2

3

4

`sec.auth.remote.password.minAge`
Required minimum age of the password (in days) before update is allowed.
Off (default)

1

5

10

15

20

30

`sec.auth.remote.password.minChangedChars`
The number of characters that must be different or change position in a new password. For example, if set to "3", 123abc can change to 345cde but not to 234bcd.
Off (default)

1

2

3

4

All

`sec.auth.remote.password.minLength`
The minimum number of characters required for a valid password.
Off (default)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

32

`sec.auth.remote.password.numCount`
The minimum amount of numbers required for a valid password.
Off (default)

1

2

All

`sec.auth.remote.password.rejectPrevPassword`
The number of most recent passwords that cannot be reused. If set to "Off", all previous passwords are valid.
Off (default)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

`sec.auth.remote.password.specialCharCount`
The minimum number of special characters required for a valid password. Supported characters
include: @ - _ ! ; $, \ / & . # *
Off (default)

1

2

All

`sec.auth.remote.password.uppercaseCount`
The minimum number of uppercase letters required for a valid password.
Off (default)

1

2

All

`sec.auth.snmp.password.canContainIdOrReverse`
Specifies whether the associated ID or its reverse can be part of a password. If this setting is enabled
and the ID is "admin", passwords "admin" and "nimda" are allowed.
False (default)

True

`sec.auth.snmp.password.lowercaseCount`
The minimum number of lowercase letters required for a valid password.
Off (default)

1

2

All

`sec.auth.snmp.password.maxRepeatedChars`
The maximum number of consecutive repeated characters in a password. For example, if set to "3",
aaa123 is a valid password but aaaa123 is not.
Off (default)

1

2

3

4

`sec.auth.snmp.password.minAge`
The minimum number of days before the password can change.
Off (default)

1

5

10

15

20

30

sec.auth.snmp.password.minLength
The minimum number of characters required for a valid password.
8 (default)

9

10

11

12

13

14

15

16

32

sec.auth.snmp.password.numCount
The minimum amount of numbers required for a valid password.
Off (default)

1

2

All

sec.auth.snmp.password.rejectPrevPassword
The number of most recent passwords that cannot be reused. If set to "Off", all previous passwords
are valid.
Off (default)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

sec.auth.snmp.password.specialCharCount
The minimum number of special characters required for a valid password. Supported characters include: @ - _ ! ; $, \ / & . # *
Off (default)

1

2

All

sec.auth.snmp.password.uppercaseCount
The minimum number of uppercase letters required for a valid password.
Off (default)

1

2

All

sec.access.room.secCode.enable
Enable or disable the security code required for connecting to the system and sharing content.
True (default)

False

sec.serialPort.login.mode
Specifies the credentials necessary for a control system to connect to the RS-232 port:
adminpassword (default) - Requires the administrator password, if one has been set, when the control system connects.

usernamepassword - Requires the username and administrator password, if one has been set, when the control system connects.

none - No username or password is required when the control system connects.

To successfully use this parameter, set device.serial.mode="Control".

Recommended Provisioning Parameters

Use the following parameters to configure provisioning settings on your G7500 and Studio X series system.

prov.polling.period
Specifies your system's provisioning polling interval in seconds.
For example, if you set this parameter to "120", your system is provisioned every 2 minutes.

Integer >= 60

prov.heartbeat.interval
Specifies how often (in seconds) your system indicates it's available to the provisioning server.

NOTE: To successfully provision this parameter with Poly Clariti Manager, you must set reports.enabled="True" and reports.server.URL=<IP/FQDN address of the Poly Clariti Manager provisioning server>.

This feature runs in the background and doesn't affect user experience.

600 (default)

Integer (120-600)

reports.enabled
Enables sending the heartbeat report to the Poly Clariti Manager provisioning server.
False - Your system doesn't send the heartbeat report to the provisioning server.

True - Your system sends the heartbeat report to the provisioning server.

reports.server.URL
Sets the IP/FQDN address of the Poly Clariti Manager provisioning server.
String

prov.softupdate.https.enable
Specifies whether your system gets software updates via HTTP or HTTPS.
False (default) - Your system gets software updates via HTTP.

True - Your system gets software updates via HTTPS.

If you're using private PKI certificates in your environment and want HTTPS downloads to work, you must install the trusted root certificate from your internal certificate authority (CA) on the system using one of the sec.TLS.customCaCert.* parameters.

Provisioning Server Redirect Parameters

Use the following parameters to redirect the provisioning of your system to another provisioning server. You must include all three parameters in your configuration file or the system ignores the redirect.

device.prov.serverName
Specifies the address of the system running the provisioning service.
String

device.prov.user
Specifies the user ID for registering with the provisioning service.
String

device.prov.password
Specifies the password for registering with the provisioning service.
String

Recommended Directory Parameters

The following parameters are recommended to configure directory settings on your system.

Using Provisioning Service Credentials to Register with an LDAP Directory

You can register your G7500 and Studio X series system with an LDAP directory using the same credentials you used to register with your provisioning service.

To do this, set `dir.ldap.auth.useLoginCredentials="True"`.

With this parameter, provisioning separate username, password, and domain parameters for the directory service isn't necessary. For example, if you set `dir.ldap.auth.useLoginCredentials="True"`, you don't have to set `dir.ldap.auth.userId`, `dir.ldap.auth.password`, and `dir.ldap.auth.domain`.

Directory Parameters

`dir.serverType`
Specifies the type of directory service you want to register with. (Your system's local directory is always enabled.)
You can't provision this parameter if the system is in Partner Mode.

Off (default) - Use only the system's local directory.

LDAP - Register with an LDAP directory.

Polycom GDS - Register with the Polycom Global Directory Server (GDS).

Recommended Logging Parameters

Use the following parameters to configure logging settings for your system.

`device.syslog.autoTransfer.customFolderName`
Lets you specify a folder name for manual log transfers.
Set if you configured device.syslog.autoTransfer.folderNameOption="Custom".

String (0-64)

Log_archive (default)

`device.syslog.autoTransfer.folderNameOption`
Specifies the folder name for log transfers.
SystemNameAndTimestamp (default) - Folder name is the system name and the timestamp of the log transfer. For example, if the system name is Marketing, the folder name might be marketing_<date_and_time>.

Timestamp - Folder name is the timestamp of the log transfer (e.g., <yyyyMMddhhmmssSSS>).

Custom - Lets you specify a folder name for manual log transfers. Set device.syslog.autoTransfer.customFolderName.

`device.syslog.autoTransfer.frequency`
Specifies when logs are transferred.
Manual (default) - The transfer starts when you select the Start Log Transfer button, which is visible only on the local interface. If the log fills before being transferred, new events overwrite the oldest events.

AutoAtThreshold - The transfer starts automatically when the limit set for
device.syslog.autoTransfer.threshold is reached.

device.syslog.autoTransfer.threshold
Reaching the log storage threshold percentage you configure here creates a
log entry and automatically transfers logs to an external storage device if
device.syslog.autoTransfer.frequency="AutoAtThreshold".
Off (default)

90

80

70

60

50

40

30

20

10

device.syslog.enable
Specifies whether remote logging is enabled. Enabling this causes the system to send each log
message to the specified server in addition to logging it locally.
Remote logging encryption is supported using TLS. If you're using UDP or TCP transport, Poly
recommends remote logging only on secure, local networks.

False (default)

True

device.syslog.level
Sets the minimum log level of messages stored in the system's flash memory. The level is the same
for local and remote logging.
"Debug" logs all messages, while "Critical" logs the fewest number of messages.

It's recommended you use the default value.

Debug (default)

Info

Warning

Error

Critical

device.syslog.serverName
Specifies the server address and port. If the port isn't specified, a default destination port is used. The
default port is determined by how device.syslog.transport is configured:
UDP: 514

TCP: 601

TLS: 6514

The address and port can be specified in the following formats:

IPv4 address: 192.0.2.0:<port>, where <port> is the elective destination port number in the 1-65535 range.

FQDN: logserverhost.company.com:<port>, where <por> is the elective destination port number in the 1-65535 range.

String

device.syslog.transport
Specifies the transport protocol for sending logs to a remote server.
UDP (default)

TCP

TLS

log.feature.h323Trace.enable
If set to "True", your system logs additional H.323 connectivity information.
You can't provision this parameter if the system is in Partner Mode.

False (default)

True

log.feature.sipTrace.enable
If set to "True", your system logs additional SIP connectivity information.
You can't provision this parameter if the system is in Partner Mode.

False (default)

True

Recommended SNMP Parameters

Use the following parameters to configure SNMP settings on your system.

snmp.enable
Allows administrators to monitor the system remotely using SNMP.
You must set this parameter to "True" to configure the other SNMP parameters.

False (default)

True

snmp.notification.enabled
Enables MIB notifications.
False (default)

True

snmp.version1.enable
Enables your system to use the SNMPv1 protocol.
Due to security issues, enabling this setting isn't recommended.

False (default)

True

snmp.version2.enable
Enables your system to use the SNMPv2c protocol.
Due to security issues, enabling this setting isn't recommended.

False (default)

True

snmp.version3.enable
Enables your system to use the SNMPv3 protocol.
True (default)

False

snmp.community
Specifies the SNMP community string for your system.
Poly does not support SNMP write operations for configuring or provisioning systems. The community string is for read operations and outgoing SNMP traps.

String (0-256)

public (default)

NOTE: For security reasons, do not use the default community string.

snmp.contactName
Specifies the name of the person responsible for remotely managing the system.
String (0-64)

IT Administrator (default)

snmp.locationName
Specifies the system location.
String (0-256)

snmp.systemDesc
Provides details about what kind of system it is.
String (0-256)

Videoconferencing Device (default)

snmp.auth.userId
Specifies the User Security Model (USM) account name for SNMPv3 message transactions.
You must set snmp.version3.enable="True" to configure this parameter.

String (0-64)

snmp.auth.algorithm
Specifies the type of SNMPv3 authentication algorithm used.
You must set snmp.version3.enable="True" to configure this parameter.

SHA (default)

MD5

snmp.auth.password
Specifies the SNMPv3 authentication password.

You must set snmp.version3.enable="True" to configure this parameter.

String (0-48)

snmp.privacyAlgorithm
Specifies the cryptographic privacy algorithm for SNMPv3 packets.
You must set snmp.version3.enable="True" to configure this parameter.

CFB-AES128 (default)

CBC-DES

snmp.privacyPassword
Specifies the SNMPv3 privacy (encryption) password.
You must set snmp.version3.enable="True" to configure this parameter.

String (0-48)

snmp.engineID
Specifies the unique ID of the SNMPv3 engine. This might be needed for matching the configuration of an SNMP console application. The ID is automatically generated, but you can create your own 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, :F: is equivalent to :0f:).

You must set snmp.version3.enable="True" to configure this parameter.

String

Must be between 10-32 hexadecimal digits.

Cannot be all zeros or Fs.

snmp.listeningPort
Specifies the port SNMP uses to listen for system messages.
161 (default)

Integer (1-65535)

snmp.transport
Specifies the transport protocol used.
UDP (default)

TCP

snmp.trapTarget.1.enable
Enable to send SNMP traps to an SNMP manager. You can send traps to up to three managers.
True (default)

False

snmp.trapTarget.1.address
Specifies the IP address of an SNMP manager where SNMP traps are sent.
String (0-255)

snmp.trapTarget.1.messageType
Specifies the type of SNMP message.
Trap (default)

Inform

snmp.trapTarget.1.protocolVersion
Specifies the SNMP version used by the SNMP manager.
v3 (default)

v2c

v1

snmp.trapTarget.1.port
Specifies the port where SNMP traps are sent.
162 (default)

String (1-65535)

snmp.trapTarget.2.enable
Enable to send SNMP traps to an SNMP manager. You can send traps to up to three managers.
True (default)

False

snmp.trapTarget.2.address
Specifies the IP address of an SNMP manager where SNMP traps are sent.
String (0-255)

snmp.trapTarget.2.messageType
Specifies the type of SNMP message.
Trap (default)

Inform

snmp.trapTarget.2.protocolVersion
Specifies the SNMP version used by the SNMP manager.
v3 (default)

v2c

v1

snmp.trapTarget.2.port
Specifies the port where SNMP traps are sent.
String (1-65535)

162 (default)

snmp.trapTarget.3.enable
Enable to send SNMP traps to an SNMP manager. You can send traps to up to three managers.
True (default)

False

snmp.trapTarget.3.address
Specifies the IP address of an SNMP manager where SNMP traps are sent.
String (0-255)

snmp.trapTarget.3.messageType
Specifies the type of SNMP message.
Trap (default)

Inform

snmp.trapTarget.3.protocolVersion
Specifies the SNMP version used by the SNMP manager.
v3 (default)

v2c

v3

snmp.trapTarget.3.port
Specifies the port where SNMP traps are sent.
162 (default)

String (1-65535)

5   Optional Parameters

These parameters are optional to run your system.

Optional Audio Parameters

Use the following parameters to configure audio settings on your system.

`voice.acousticFence.enable`
Specifies if you want to enable Polycom Acoustic Fence technology.
This setting is disabled if you set voice.stereo.enable="True".

False (default)

True

`voice.acousticFence.radius`
Specifies the width of the Polycom Acoustic Fence beam.
0-10 (default is 5) - Higher values increase the width of the audio fence beam between the primary and fence microphone(s). Use `0` for the narrowest beam (20 degrees) or `10` for the widest beam (120 degrees).

- **For Studio X Family systems**: Higher values increase the width of the audio fence beam. Use `1` for the narrowest beam (12 degrees) or `10` for the widest beam (120 degrees). The total angles is the setting number multiplied by 12.

  If **Acoustic Fence Sensitivity** is set to `0`, the system mutes the built in microphone and any supported echo canceling external microphone connected to the system. Setting the sensitivity level to `0` doesn't mute the 3.5 mm or USB audio in input.

- **For G7500 systems**: Higher values increase the width of the audio fence beam between the primary and fence microphone(s). Use `0` for the narrowest beam (20 degrees) or `10` for the widest beam (120 degrees).

`voice.alertTone`
Specifies the audible tone for user alerts.
You can't provision this parameter if the system is in Partner Mode.

Tone_1 (default)

voice.debutmicautoswitch.enable
(X50 only) Specifies whether to allow your system to automatically toggle the microphone input between the system's built-in microphones and a RealPresence Debut expansion microphone
True

False (default)

`voice.in.hdmi.level`
Sets levels for the left and right channels of the HDMI audio input.
You can't provision this parameter if the system is in Partner Mode.

0-10 (default is 5)

`voice.in.3p5.level`
(G7500 only) Sets levels for the left and right channels of the 3.5 mm stereo audio input.
You can't provision this parameter if the system is in Partner Mode.

0-10 (default is 5)

`voice.in.3p5.playbackOption`
(G7500 only) Specifies how audio from the 3.5 mm stereo audio input is routed and controlled.
You can't provision this parameter if the system is in Partner Mode.

Playback to All Locations (default) - Set this value if you're sending audio from a device.

- Near and far sites hear the 3.5 mm stereo input.

- You can't mute audio or control echo cancellation.

Playback to Far Sites - Set this value if you're using an external digital signal processor (DSP), such as Polycom SoundStructure, which provides mute controls and echo cancellation.

- Only far sites hear the 3.5 mm stereo input (there is no associated video content).

- You can't mute audio or control echo cancellation through the system.

Playback to Far Sites, Mute Controlled - Set this value if you want to perform activities like sharing music from a mobile phone to call participants.

- Only far sites hear the 3.5 mm stereo input (there is no associated video content).

- You can mute audio but can't control echo cancellation.

Playback to Far Sites, Mute Controlled, Echo Cancelled - Set this value if you're using a line-level microphone. (Note: The microphone must provide the line-level signal to work.)

- Only far sites hear the 3.5 mm stereo input (there is no associated video content).

- You can mute audio and control echo cancellation.

- Mic-level inputs aren't supported.

`voice.liveMusicMode.enable`
Specifies whether the system uses M-Mode, which transmits audio using a configuration that best reproduces interactive and live performance music picked up by microphones. This feature provides the highest-possible bandwidth for audio.
You can't provision this parameter if the system is in Partner Mode.

When M-Mode is enabled, even the faintest musical notes come through clearly.

False (default)

True

NOTE: Noise reduction features are disabled when M-Mode is enabled.

`voice.muteReminder.enable`
Specifies if a notification displays indicating microphones are muted when speaking is detected.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`voice.noiseSuppression.enable`
Enables Poly NoiseBlockAI, which during calls eliminates background and extraneous sounds in common working environments when no one is talking.
When you enable M-Mode (voice.liveMusicMode.enable="True"), this feature is disabled. If an external echo canceller is used, keyboard noise reduction is not available.

You can't provision this parameter if the system is in Partner Mode.

False

True (default)

`voice.out.line.mode`
Specifies how the volume for a device connected to the line out port is configured:
You can't provision this parameter if the system is in Partner Mode.

variable (default) - Allows users to change the volume.

fixed - Sets the volume to the audio level configured for the system.

`voice.ringTone`
Specifies the ringtone for incoming calls.
You can't provision this parameter if the system is in Partner Mode.

Tone_1 (default)

Tone_2

Tone_3

Tone_4

Tone_5

Tone_6

Tone_7

Tone_8

Tone_9

Tone_10

`voice.stereo.enable`
Enables Polycom StereoSurround software for all calls.
This setting is disabled if you set voice.acousticFence.enable="True".

You can't provision this parameter if the system is in Partner Mode.

This feature isn't available when using a Poly Microphone IP Adapter.

False (default)

True

voice.toneControl.bass
Sets the volume level for the low frequencies without changing the primary audio volume.
You can't provision this parameter if the system is in Partner Mode.

+6

+4

+2

0 (default)

-2

-4

-6

voice.toneControl.treble
Sets the volume level for the high frequencies without changing the primary audio volume.
You can't provision this parameter if the system is in Partner Mode.

+6

+4

+2

0 (default)

-2

-4

-6

voice.volume.soundEffects
Sets the volume level of the ringtone.
You can't provision this parameter if the system is in Partner Mode.

0-10 (default is 3)

voice.volume.speaker
Sets the main audio output volume level going to the speakers.
You can't provision this parameter if the system is in Partner Mode.

Even numbers from 0-100 (default is 50)

voice.volume.transmitLevel
Specifies the audio level, in decibels, at which to transmit sound. Unless otherwise advised, you should set this value to 0 dB.
You can't provision this parameter if the system is in Partner Mode.

-6-18 (default is 0)

voice.muteInSleep
If set to "True", microphones are muted when the system goes to sleep.
You can't provision this parameter if the system is in Partner Mode.

False (default)

True

Optional Call Control Parameters

Use the following optional parameters to configure call settings on your system.

`call.autoAnswer.answerP2PCall`
Sets whether the system answers an incoming call when not in a call.
If set to "Do_Not_Disturb", incoming calls are rejected without notification.

You can't provision this parameter if the system is in Partner Mode.

No (default)

Yes

Do_Not_Disturb

`call.displayIconsInCall`
Specifies whether to display onscreen graphics, including icons and help text, during calls.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.maxTimeInCall`
Sets the maximum number of hours allowed for a call.
When that time expires, you're prompted if you want to hang up. If you don't answer within one minute, the call automatically ends. If you choose to stay in the call, you aren't prompted again.

You can't provision this parameter if the system is in Partner Mode.

8_hours (default)

1_hour

2_hours

3_hours

4_hours

5_hours

6_hours

7_hours

9_hours

10_hours

11_hours

12_hours

24_hours

48_hours

`call.preferredPlaceACallNav`
Specifies the default options that display on the local interface place a call screen.
You can't provision this parameter if the system is in Partner Mode.

keypad (default) - Displays recently-dialed numbers and a dialpad.

globaldir - Displays a screen for searching a directory. The multitiered directory (LDAP) root entry displays at the top of the Contacts list, which combines your search results and favorites.

recentcalls - Lists previous calls in chronological order.

`call.cdr.enable`
Call detail records (CDRs) are included in the system logs. When disabled, the system does not write call information.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.recentCalls.enable`
Specifies whether to show recent calls on the local and system web interfaces.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`call.recentcalls.maxNumberToDisplay`
The maximum number of calls displayed in the recent calls list.
You can't provision this parameter if the system is in Partner Mode.

100 (default)

25

50

75

Optional Quality of Service Parameters

Use the following parameters to configure QoS settings on your G7500 and Studio X series system.

`qos.tosType`
Specifies the type of service (ToS), which lets you prioritize packets sent to your system for video, audio, Far End Camera Control (FECC), and OA&M
You can't provision this parameter if the system is in Partner Mode.

IP_Precedence (default) - Uses a priority level between 0 and 7.

DiffServ - Uses a priority level between 0 and 63.

`qos.diffServ.audio`
Specifies the DiffServ priority level for audio RTP and associated RTCP traffic.
You can't provision this parameter if the system is in Partner Mode.

0 (default)

Integer (0-63)

`qos.diffServ.video`
Specifies the DiffServ priority level for video RTP and associated RTCP traffic.
You can't provision this parameter if the system is in Partner Mode.

0 (default)

Integer (0-63)

`qos.diffServ.fecc`
Specifies the DiffServ priority level for control traffic on the following channels:
H.323: H.225.0 call signaling, H.225.0 RAS, H.245, and far-end camera control (FECC).

SIP: SIP signaling, FECC, and Binary Floor Control Protocol (BFCP).

You can't provision this parameter if the system is in Partner Mode.

40 (default)

Integer (0-63)

NOTE: FECC is enabled by video.camera.farControlNearCamera.

`qos.diffServ.oam`
Specifies the DiffServ value for traffic unrelated to video, audio, or FECC.
You can't provision this parameter if the system is in Partner Mode.

16 (default)

Integer (0-63)

`qos.dynamicBandwidth.enable`
Enable if you want the system to automatically determine the optimal call rate.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`qos.intServ.audio`
Specifies the IP Precedence priority level for audio RTP and associated RTCP traffic.
You can't provision this parameter if the system is in Partner Mode.

5 (default)

Integer (0-7)

`qos.intServ.fecc`
Specifies the IP precedence priority level for control traffic on the following channels:
H.323: H.225.0 call signaling, H.225.0 RAS, H.245, and far-end camera control (FECC).

SIP: SIP signaling, FECC, and Binary Floor Control Protocol (BFCP).

You can't provision this parameter if the system is in Partner Mode.

3 (default)

Integer (0-7)

FECC is enabled by video.camera.farControlNearCamera.

---

qos.intServ.oam
Specifies the IP Precedence value for traffic unrelated to video, audio, or FECC.
You can't provision this parameter if the system is in Partner Mode.

0 (default)

Integer (0-7)

qos.intServ.video
Specifies the IP Precedence priority level for video RTP and associated RTCP traffic.
You can't provision this parameter if the system is in Partner Mode.

4 (default)

Integer (0-7)

qos.LPR.enable
If enabled, the system uses the Lost Packet Recovery (LPR) protocol to help compensate for packet loss if it occurs.
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

qos.maxRxBandwidth
Specifies the maximum receive call rate between 64 kbps and the system's maximum line rate. This can be useful when the system is connected to the network using an access method with different transmit and receive bandwidth.

You can't provision this parameter if the system is in Partner Mode.

6144 (default)

64

128

192

256

320

384

448

512

576

640

704

768

832

896

960

1024

1088

1152

1216

1280

1344

1408

1472

1536

1600

1664

1728

1792

1856

1920

2048

3840

4096

`qos.maxTxBandwidth`
Specifies the maximum receive call rate between 64 kbps and the system's maximum line rate. This can be useful when the system is connected to the network using an access method with different transmit and receive bandwidth.

You can't provision this parameter if the system is in Partner Mode.

6144 (default)

64

128

192

256

320

384

448

512

576

640

704

768

832

896

960

1024

1088

1152

1216

1280

1344

1408

1472

1536

1600

1664

1728

1792

1856

1920

2048

3840

4096

`qos.mtuMode`
Determines whether to use the default Maximum Transmission Unit (MTU) size for calls or let you specify it.
You can't provision this parameter if the system is in Partner Mode.

Default (default)

Specify

qos.mtuSize
Specifies the MTU size (in bytes) used in calls.
Decrease the MTU if video quality is poor or network errors occur (packets might be too large).

Increase the MTU if the network is burdened with unnecessary overhead (packets might be too small).

You can't provision this parameter if the system is in Partner Mode.

1260 (default)

660

780

900

1020

1140

1500

qos.rsvp.enable
If enabled, the system can use the Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. (To use this feature, the near and far site must support RSVP.)
You can't provision this parameter if the system is in Partner Mode.

True (default)

False

Optional Feature Activation Parameters

Use the following parameters to unlock certain features or the ability to update software on your system.

For more information about feature activation and software update keys, see your system Administrator Guide .

license.optionKey
Set this parameter with your system feature activation key.
You can't provision this parameter if the system is in Partner Mode.

String

license.softupdateKey
Set this parameter with your system software activation key.
You can't provision this parameter if the system is in Partner Mode.

String

Optional Out of Office Parameters

Use the following parameters to configure out of office settings on your system.

`device.local.outofoffice.enabled`
Specifies if you want to enable/disable the out of office feature.
`device.local.outofoffice.offtime`
The stop time for the window in a day in 24 hr format (HH:MM format). Example: 23:30.
`device.local.outofoffice.starttime`
The start time for the window in a day in 24 hr format (HH:MM format). Example: 23:30.

Optional Peripheral Device Pairing Parameter

Use the following parameter to automatically pair some devices with your system.

`mr.primary.autoPair.enable`
Enables your system to automatically pair with some devices, such as a Poly IP Table Microphone.
For example, if mr.primary.autoPair.enable="True" and you connect a table microphone to a LAN port
on your system, it should automatically pair and be ready to use.

You can't provision this parameter if the system is in Partner Mode.

True (default)

False

Optional Poly IP Table and Ceiling Microphone Parameters

Use the following parameters to configure Poly IP Table Microphones and Poly IP Ceiling
Microphones connected to your system.

`log.level.change.xxx`
Controls the logging detail level. These are the input filters into the internal memory-based log
system.
Possible values for xxx are cfg, curl, mr, so, ss, ssps, and usb.
0-6 (default is 4)

`log.render.level`
Controls the logging level for the lowest severity of events to log.
For example, if you configure this parameter to "2", the log includes all events of an equal or greater
severity level.
0 or 1 - Severity Debug (7)

2 or 3 - Severity Informational (6)

4 Severity Error (3)

5 Severity Critical (2)

6 Severity Emergency (0)

0-6 (default is 1)

`log.render.stdout`
Enables or disables the logs print to standard out (serial and shell terminal).
False (default)
True

`mr.pair.tls.enabled`

Enables or disables TLS between paired devices.
True (default)
False

device.net.mikoTimeout.set
Allows you to set the device.net.mikoTime parameter.
False (default)
True

device.net.mikoTimeout
Timeout value for table microphone DHCP in seconds.
30-60 (default is 30)
feature.usbdevice.enable
Enables or disables USB device access.
True (default)
False

Optional Poly Microphone IP Adapter Parameters

device.syslog.renderLevel
Controls the logging details level.
Debug (default)

Info

Warning

Error

Critical

call.encryption.requireAES
Controls when to use the audio encryption.
You can't provision this parameter if the system is in Partner Mode.

Off

When_Available (default)

Required_Video

Required_All

sec.TLS.disableVersion1
Enables or disables TLS1.0.
True

False (default)

device.local.deviceName
The name of your system.
String

Optional Serial Port Hardware Parameters

Use the following parameters to configure serial port settings on your system.

device.serial.mode
Specifies the mode used for the RS-232 serial port.
Control (default) - Receives control signals from a touch-panel control. Allows any device connected to the RS-232 port to control the system using API commands.

Off - Disables the serial port.

device.serial.baud
Set this to the same value configured on the serial device.
9600 (default)

19200

38400

57600

115200

device.serial.flowControl
Specifies if you want to use hardware flow control between the connected device and your system.
none (default)

hardware

device.serial.parity
Set this to the same value configured on the serial device.
none (default)

even

odd

device.serial.stopBits
Set this to the same value configured on the serial device.
1 (default)

2

Optional System Usage Data Parameter

Use the following parameter to configure the system usage data collection setting.

cloud.polycom.analytics.enable
Specifies if you want your system to send usage data to Poly to help improve its products and services.
True (default)

False

For information about the data that Poly collects, see the system Privacy Guide on the Poly Support website.

Optional Video and Camera Parameters

Use the following parameters to configure video settings on your system.

Provisioning Camera Parameters

Using the `video.camera.[index].type` parameter, you can configure parameters differently for the following cameras supported by your system:

- Poly EagleEye Cube USB

- Polycom EagleEye IV 4x

- Polycom EagleEye IV 12x

- Polycom EagleEye IV USB

- Polycom EagleEye Director II

- Polycom EagleEye Producer

- Poly Studio X70, Poly Studio X50, and Studio X30 (which use built-in cameras)

- Poly Studio USB video bar

- Polycom EagleEye Mini

- Poly Studio E70

IMPORTANT: If you provision USB cameras, you must disable provisioning on your system to change out that USB camera for a different camera. If you don't disable provisioning when changing cameras, the previously provisioned settings may carry over to the new camera and you won't be able to modify them.

The following examples show you how to configure cameras based on type.

Table 5-1 **Per-Camera Configuration Examples**

Camera Type Configuration	Per-Camera Configuration
`video.camera.1.type=EagleEyeIV12x`	`video.camera.1.brightness="14"` `video.camera.1.backlightCompensation="True"`
`video.camera.2.type=EagleEyeDirectorII`	`video.camera.2.trackingMode="FrameSpeaker"` `video.camera.2.trackingSpeed="Normal"`

You also can configure common parameters that apply to all camera types.

Configure Common and Per-Camera Parameters

You can configure parameters that apply to all cameras along with parameters that apply only to a specific type of camera. The following example shows how you might configure a mix of common and per-camera parameters.

1. Set some common configurations for any type of camera.

```
video.camera.backlightCompensation="False"video.camera.brightness="13"video.camer
Energy"video.camera.groupViewSize="Medium"
```

2. Assign an index to a specific camera model for per-camera configurations.

```
video.camera.1.type="EagleEyeDirectorII"
```

3. Set a per-camera configuration.

```
video.camera.1.trackingMode="FrameSpeaker"
```

Video and Camera Parameters

> **NOTE:** Per-camera configurations override common camera configurations. For example, if you set `video.camera.[index].videoQuality` for a specific camera, the `video.camera.videoQuality` parameter is overridden.

video.layout.contentMirror
Specifies your content layout preference during an active call when using dual monitors.
False (default) - Content displays only on the secondary monitor.

True - Content displays on the primary and secondary monitors.

video.layout.selfviewPIP
Specifies your Self View layout preference during an active call when using dual monitors.
False (default) - Self View displays on the entire screen of the secondary monitor.
True - Self View displays in the corner of the secondary monitor.

video.monitor.1.display
Specifies how you want to configure the primary monitor.
auto (default) - The highest-supported resolution of the primary monitor is detected.
manual - Lets you set the monitor resolution with video.monitor.1.resolution.

video.monitor.1.resolution
Specifies the primary monitor resolution.
Monitor resolution is automatically configured if you set video.monitor.1.display="auto".

3840x2160p 25Hz

3840x2160p 30Hz

3840x2160p 50Hz

3840x2160p 60Hz

1920x1080p 50Hz

1920x1080p 60Hz (default)

video.monitor.2.display
Specifies how you want to configure the secondary monitor.
off - Disables the secondary monitor.

auto (default) - The highest-supported resolution of the secondary monitor is detected.

video.monitor.cec.enable
Enable or disable the system's Consumer Electronics Control (CEC) feature for HDMI-connected monitors that support the CEC protocol.
With CEC enabled, connected monitors switch to standby mode when the system goes to sleep. You can also wake monitors with your remote control.

False (default)

True

video.camera.[index].type
Choose a camera type that corresponds to [index], where [index] can be 1-4.
The value set for [index] in this parameter and related parameters determines the configuration settings for the camera type you specify.

For example, setting video.camera.1.type="EagleEyeDirectorII" gives you a reference index of 1 to configure your Polycom EagleEye Director II camera settings.

EagleEyeIV4x

EagleEyeIV12x

EagleEyeProducer

EagleEyeDirectorII

EagleEyeCubeUSB

BuiltInCamera (Use this parameter for Studio X30 and Studio X50.)

PolyStudio

EagleEyeIVUSB

EagleEyeMini

PolyStudioE70

video.camera.[index].backlightCompensation
Specifies if the camera automatically adjusts for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.
Use this to configure the camera type identified with the video.camera.[index].type parameter.

True

False (default)

video.camera.[index].brightness
Specifies how bright the video is.
Use this to configure the camera type identified with the video.camera.[index].type parameter.

11 (default)

Integer (0-21)

video.camera.[index].groupViewSize
Specifies the group framing size used by the EagleEye Cub USB, EagleEye Director II, or EagleEye Producer camera.
Use this to configure the camera type identified with the video.camera.[index].type parameter.

Medium (default) - Average-sized frame.

Wide - Most expansive frame.

Tight - Close-up frame.

`video.camera.[index].name`
Specifies a name for the camera.
Use this to configure the camera type identified with the video.camera.[index].type parameter.

String (0-32)

`video.camera.[index].orientation`
Specifies whether to invert the camera display for a Studio X30 system that's mounted below a monitor upside down.
Use this to configure the camera type identified with the video.camera.[index].type parameter.

You can't provision this parameter if the system is in Partner Mode.

Normal (default)

Inverted

`video.camera.[index].roomViewPIP`
When enabled, a Picture-in-Picture window displays showing a wide angle of the room in addition to the main window showing the primary speaker(s).
This parameter is supported when using a camera with tracking features, such as the EagleEye Director II.

True (default)

False

`video.camera.[index].saturation`
Specifies the intensity of the video color.
Use this to configure the camera type identified with the video.camera.[index].type parameter.

6 (default)

Integer (0-14)

`video.camera.[index].sharpness`
Adjusts the video's overall clarity.
Use this to configure the camera type identified with the video.camera.[index].type parameter.

11 (default)

Integer (1-11)

`video.camera.[index].skinEnhancement`
Enables or disables natural skin color enhancements for participants.
This parameter applies only to the EagleEye Cube USB camera.

True (default)

False

`video.camera.[index].trackingMode`

NOTE: In Partner Mode, the partner application controls the camera settings and framing behavior. Provisioning this parameter may interfere with the partner application features.

Specifies the tracking mode used by the EagleEye Cube USB, EagleEye Director II, EagleEye Producer, Studio E70, Studio X70, Studio X50, or Studio X30 camera.

Use this to configure the camera type identified with the video.camera.[index].type parameter.

FrameGroup (default) - The camera automatically locates and frames all the people in the room.

FrameSpeaker - This option behaves a little differently depending on your system. Note that when you mute your microphone, the camera tracking mode automatically switches to "FrameGroup".

- Studio X70, Studio X50 and Studio X30 systems: The camera includes everyone in the current conversation. For example:

  – The camera focuses on people actively talking to each other.

  – When someone is talking for a prolonged period of time, the camera assumes that this person is presenting and only focuses on them.

  – If there's a period in which no one has said anything or the far side is doing most of the talking, the camera frames everyone in the room.

- G7500 systems: The camera automatically locates and frames the active speaker. When someone else starts speaking, the camera switches to that person.

FrameGroupWithTransition - (EagleEye Producer camera only) The camera automatically locates and frames people in the room while displaying camera motion. For example, if someone enters the room, you might see the camera pan until that person is in view.

Off - Disables automatic tracking. All camera control must be handled manually.

`video.camera.[index].videoQuality`
Sharpness - Gives preference to resolution over frames per second. With this setting, moderate-to-heavy motion at low call rates can cause some frames to drop.
Motion - Gives preference to frames per second over resolution.

Use this to configure the camera type identified with the video.camera.[index].type parameter.

Sharpness (default)

Motion

`video.camera.[index].whiteBalanceMode`
Specifies how the camera compensates for light source variations in the room. Use this to configure the camera type identified with the video.camera.[index].type parameter.
Auto (default) - Setting this value is recommended for most situations. It calculates the best white balance setting based on lighting conditions in the room.

The following color temperatures are available with the EagleEye Director II camera (measured in Kelvin): 3200k, 3680k, 4160k, 5120k, and 5600k.

The following color temperatures are available with the EagleEye IV and EagleEye Producer cameras (measured in Kelvin): 2300k, 2856k, 3450k, 4230k, 5200k, and 6504k.

The following color temperatures are available with the EagleEye Cube USB camera (measured in Kelvin): 2300k, 2856k, 3200k, 3450k, 3680k, 4160k, 4230k, 4640k, 5120k, 5200k, 5600k, and 6504k.

The following color temperatures are available with the Studio X Family system cameras: incandescent, fluorescent, warm_fluorescent, daylight, cloudy_daylight, twilight, and shade.

Manual - Setting this value may be necessary for rooms where the "Auto" and fixed values don't provide acceptable color reproduction. Remember, however, you must manually white balance the camera. (This value is not supported by the EagleEye Cube USB or Studio X Family cameras.)

video.camera.[index].wideDynamicRange
Enables or disables re-exposure according to the framed area instead of full view.
This parameter applies only to the EagleEye Cube USB camera.

True (default)

False

video.camera.autoUpdate.enable
Enable or disable automatic software updates to your HDCI-connected Polycom camera.
If newer software than what the camera has is detected, the camera updates automatically when the system isn't in a call. (However, if during a call you connect a camera that isn't running the latest software, the call ends and the update starts.)

True

False (default)

video.camera.backlightCompensation
Specifies whether to have the camera automatically adjust for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.
You can't provision this parameter if the system is in Partner Mode.

True

False (default)

video.camera.brightness
Specifies how bright the video is.
You can't provision this parameter if the system is in Partner Mode.
11 (default)

Integer (0-21)

video.camera.digitalzoomfactor
Specifies the maximum digital zoom factor for the camera.
3x (default)
String (1x-5x)

video.camera.farControlNearCamera
Specifies whether the far site can pan, tilt, or zoom the near-site camera. When you enable this setting, a user at the far site can control the framing and angle of the camera for the best view of the near site. This is also called Far End Camera Control (FECC).
True (default)
False

video.camera.groupViewSize
Specifies the framing size used by the EagleEye Cube USB, EagleEye Director II, or EagleEye Producer camera.
Medium (default) - Average-sized frame.

Wide - Most expansive frame.

Tight - Close-up frame.

video.camera.name
Specifies a name for the camera.
String (0-32)
video.camera.orientation

Specifies whether to invert the camera display for a Studio X30 system that's mounted below a monitor upside down.

You can't provision this parameter if the system is in Partner Mode.

Normal (default)

Inverted

video.camera.powerFrequency

Specifies the power-line frequency for your system. In most cases, this should be the same as your display frequency.

Your system typically defaults to the correct power-line frequency based on the video standard used in the country where it's located. This parameter helps you adapt the system to areas where the frequency doesn't match the video standard. You might also need to change this configuration to avoid flicker from fluorescent lights in the room.

60 (default)

50

video.camera.preset.snapshot.enable

Enables or disables the use of snapshot icons that represent camera presets.

To see a preset icon, you must enable this setting before configuring the preset.

True (default)

False

video.camera.roomViewPIP

When enabled, a Picture-in-Picture window displays showing a wide angle of the room in addition to the main window showing the primary speaker(s).

This parameter is supported only with G7500 systems using an EagleEye Director II camera.

True (default)

False

video.camera.saturation

Specifies the intensity of the video color.

You can't provision this parameter if the system is in Partner Mode.

6 (default)

Integer (0-14)

video.camera.sharpness

Adjusts the video's overall clarity.

11 (default)

Integer (1-11)

video.camera.skinEnhancement

Enables or disables natural skin color enhancements for participants.

This parameter applies only to the EagleEye Cube USB camera.

True (default)

False

`video.camera.sleepMode`

Specifies a sleep mode for your camera.

Save Energy (default) - Puts the camera into standby mode to save power (the camera spins to the rear and faces down). Remember the following when setting this value in conjunction with device.screenSaver.mode:

When device.screenSaver.mode="Black", it takes a few seconds for the camera to send an image.

When device.screenSaver.mode="NoSignal", the camera is sending an image by the time the display synchronizes with the system.

Fast Wake Up - The camera provides an image as soon as the monitor wakes. While asleep, the camera faces forward. Remember the following when setting this value in conjunction with device.screenSaver.mode:

When device.screenSaver.mode="Black", an image displays more quickly, but be aware that this uses maximum power.

When device.screenSaver.mode="NoSignal", the display synchronizes with the system. This can take a few seconds but may conserve energy depending on the monitor.

`video.camera.trackingMode`

NOTE: In Partner Mode, the partner application controls the camera settings and framing behavior. Provisioning this parameter may interfere with the partner application features.

Specifies the tracking mode used by the EagleEye Cube USB, EagleEye Director II, EagleEye Producer, Studio E70, Studio X70, Studio X50, and Studio X30 camera.

FrameGroup (default) - The camera automatically locates and frames all the people in the room.

FrameSpeaker - This option behaves a little differently depending on your system. Note that when you mute your microphone, the camera tracking mode automatically switches to "FrameGroup".

- Studio X70, Studio X50, and Studio X30 systems: The camera includes everyone in the current conversation. For example:

    - The camera focuses on people actively talking to each other.

    - When someone is talking for a prolonged period of time, the camera assumes that this person is presenting and only focuses on them.

    - If there's a period in which no one has said anything or the far side is doing most of the talking, the camera frames everyone in the room.

- G7500 systems: The camera automatically locates and frames the active speaker. When someone else starts speaking, the camera switches to that person.

FrameGroupWithTransition - (EagleEye Producer camera only) The camera automatically locates and frames people in the room while displaying camera motion. For example, if someone enters the room, you might see the camera pan until that person is in view.

Off - Disables automatic tracking. All camera control must be handled manually.

`video.camera.videoQuality`

Specifies your camera video quality preference.

Sharpness (default) - Gives preference to resolution over frames per second. With this setting, moderate-to-heavy motion at low call rates can cause some frames to drop.

Motion - Gives preference to frames per second over resolution.

`video.camera.whiteBalanceMode`
Specifies how the camera compensates for light source variations in the room.
You can't provision this parameter if the system is in Partner Mode.

Auto (default) - Setting this value is recommended for most situations. It calculates the best white balance setting based on lighting conditions in the room.

The following color temperatures are available with the EagleEye Director II camera (measured in Kelvin): 3200k, 3680k, 4160k, 5120k, and 5600k.

The following color temperatures are available with the EagleEye IV and EagleEye Producer cameras (measured in Kelvin): 2300k, 2856k, 3450k, 4230k, 5200k, and 6504k.

The following color temperatures are available with the EagleEye Cube USB camera (measured in Kelvin): 2300k, 2856k, 3200k, 3450k, 3680k, 4160k, 4230k, 4640k, 5120k, 5200k, 5600k, and 6504k.

The following color temperatures are available with the Studio X Family system cameras: incandescent, fluorescent, warm_fluorescent, daylight, cloudy_daylight, twilight, and shade.

Manual - Setting this value may be necessary for rooms where the "Auto" and fixed values don't provide acceptable color reproduction. Remember, however, you must manually white balance the camera. (This value is not supported by the EagleEye Cube USB or Studio X Family cameras.)

`video.camera.wideDynamicRange`
Enables or disables re-exposure according to the framed area instead of full view.
This parameter applies only to the EagleEye Cube USB camera.

True (default)

False

`video.content.name`
Specifies a name for the device connected to your system using HDMI. This device is typically used to share content.
String (0-32)

`video.camera.perimeterEnabled`
Enable or disable the Poly Perimeter feature.
Level value= "1"

`video.camera.perimeterWidth`
Specifies width of the room to be included when calculating the perimeter.
Level value= "1"

`video.camera.perimeterFront`
Specifies offset from camera or front exclusion distance when calculating the perimeter.
Level value= "1"

`video.camera.perimeterDepth`
Specifies maximum distance from camera OR room depth to be included when calculating the perimeter.
Level value= "1"

`video.camera.perimeterMetric`
Specifies metric for Poly Perimeter configurations.
Level value= "1"

device.scheduledreboot.enabled
Enable or disable a scheduled reboot.
False (default)

True

device.scheduledreboot.frequency
Specifies the frequency of a scheduled reboot.
WEEKLY (default)

DAILY

device.scheduledreboot.dayofweek
Specifies the day of the week on which a scheduled reboot should occur.
SATURDAY (default)

Type one of SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY

device.scheduledreboot.time
(Optional if device.scheduledreboot.frequency is set to DAILY)Specifies the time of day for the scheduled reboot in 24 hr format (HH:MM format. Example: 08:00
00.00 (default)

Type one of SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY

Optional VoIP Parameters

Use the following parameters to configure VoIP settings on your system.

Using Provisioning Service Credentials to Register with SIP

You can register your G7500 and Studio X series system with a SIP service using the same credentials you used to register with your provisioning service.

To do this, set `voIpProt.SIP.auth.useLoginCredentials="True"`.

With this parameter, provisioning separate username, password, and domain parameters for the SIP service isn't necessary. For example, if you set `voIpProt.SIP.auth.useLoginCredentials="True"`, you don't have to set `voIpProt.SIP.auth.userId`, `voIpProt.SIP.auth.password`, and `voIpProt.SIP.auth.domain`.

VoIP Parameters

voIpProt.SIP.auth.domain
Specifies the domain that your SIP username belongs to.
You can't provision this parameter if the system is in Partner Mode.

String

voIpProt.SIP.sbcKeepAlive.enable
Specifies whether to regularly transmit keep-alive messages on the SIP signaling channel and on RTP sessions part of SIP calls. Keep-alive messages maintain connections through firewall/NAT devices that are often used at network edges.
If your system is in an Avaya SIP environment, it's recommended that you disable this setting to allow calls to fully connect.

You can't provision this parameter if the system is in Partner Mode.

True (default)

False

`voIpProt.H323.e164`

You can place point-to-point calls using this extension if both systems are registered with a gatekeeper. The extension is also used by gatekeepers and gateways use to identify your system. Your organization's dial plan might define the extensions you can use.

You can't provision this parameter if the system is in Partner Mode.

String (0-128)

${h323_e164} - Poly Clariti Manager accepts this value to automatically configure the parameter.

`voIpProt.H323.enable`

Enables or disables the ability for your system to use the H.323 protocol.
You must set to "True" to use other voIpProt.H323.* parameters.

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

If set to "False", you can't also set voIpProt.SIP.enable="False".

`voIpProt.H323.gk.auth.enable`

Enables support for H.235 Annex D Authentication.
When H.235 Annex D Authentication is enabled, the H.323 gatekeeper ensures that only trusted H.323 endpoints can access the gatekeeper.

To use this parameter, you should set voIpProt.H323.gk.mode="Specify".

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

`voIpProt.H323.gk.auth.password`

Specifies a password if authentication is required for registering with the gatekeeper.
To use this parameter, you should set voIpProt.H323.gk.mode="Specify" and voIpProt.H323.gk.auth.enable="True".

You can't provision this parameter if the system is in Partner Mode.

String

`voIpProt.H323.gk.auth.userId`

Specifies a username if authentication is required for registering with the gatekeeper.
To use this parameter, you should set voIpProt.H323.gk.mode="Specify" and voIpProt.H323.gk.auth.enable="True".

You can't provision this parameter if the system is in Partner Mode.

String (0-62)

voIpProt.H323.gk.ipAddress
The gatekeeper IPv4 address the system registers with.
As part of the registration process, the gatekeeper might return alternate gatekeepers. If communication with the primary gatekeeper is lost, your system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system re-establishes communication with the primary gatekeeper, it unregisters from the alternate gatekeeper.

You can't provision this parameter if the system is in Partner Mode.

What you can set here is determined by how you've configured voIpProt.H323.gk.mode:

Off - Setting the gatekeeper IP address isn't needed.

Auto - Setting the gatekeeper IP address isn't needed.

Specify - Enter the gatekeeper IP address or name (e.g., 10.11.12.13 or gatekeeper.companyname.usa.com).

String (0-255)

voIpProt.H323.gk.mode
Specifies if you want to use a gatekeeper for H.323 services.
You can't provision this parameter if the system is in Partner Mode.

Off (default) - Calls do not use a gatekeeper.

Auto - System tries to automatically find an available gatekeeper.

Specify - Calls use the specified gatekeeper. Set this value if if you want to use voIpProt.H323.gk.auth.enable.

voIpProt.H323.name
How gatekeepers and gateways identify your system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper.
The value here is the same set for device.local.deviceName unless you change it. (Your organization's dial plan might define the name you can use.)

You can't provision this parameter if the system is in Partner Mode.

String (0-36)

${h323_ID} - Poly Clariti Manager accepts this value to automatically configure the parameter.

voIpProt.SIP.auth.useLoginCredentials
Specifies if you want to register with a SIP service using the same credentials you used for registering with a provisioning service.
With this parameter, provisioning separate username, password, and domain parameters for the SIP service isn't necessary.

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

voIpProt.SIP.auth.password
The password associated with the username for authenticating your system with a SIP registrar server.
You can't provision this parameter if the system is in Partner Mode.

String

`voIpProt.SIP.bfcpTransportPreference`
Controls content sharing negotiation behavior. Using the Binary Floor Control Protocol (BFCP), a relationship is established between the floor control server and its clients. What you set here determines how network traffic flows between the server and clients.
You can't provision this parameter if the system is in Partner Mode.

Prefer_UDP (default) - Starts resource sharing using UDP but falls back to TCP if needed.

Prefer_TCP - Starts resource sharing using TCP but falls back to UDP if needed.

UDP_ONLY - Shares resources only using UDP. If UDP is unavailable, content sharing in a separate video stream isn't available.

TCP_ONLY - Shares resources only through TCP. If TCP is unavailable, content sharing in a separate video stream isn't available.

TCP is typically known as slightly slower but more reliable than UDP. It is not supported under some circumstances, such as with session border controllers (SBCs).

`voIpProt.SIP.enable`
Enables or disables the ability for your system to use the SIP protocol.
You must set to "True" to use other voIpProt.SIP.* parameters.

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

If set to "False", you can't also set voIpProt.H323.enable="False".

`voIpProt.SIP.forceConnectionReuse`
When disabled (recommended), the system uses an ephemeral source port for outgoing SIP messages.
When enabled, the system uses the active SIP listening port as the source port (5060 or 5061, depending on the negotiated SIP transport protocol in use). This can be useful to establish correct operation with remote SIP peer devices, which require that the source port match the contact port in SIP messages.

You can't provision this parameter if the system is in Partner Mode.

False (default)

True

`voIpProt.SIP.proxyServer`
The IP address or fully qualified domain name (FQDN) of the SIP proxy server. If you don't set this, the registrar server address is used. If you also leave voIpProt.SIP.registrarServer blank, there is no SIP proxy server.
SIP signaling by default is sent to ports 5060 (TCP) and 5061 (TLS) on the proxy server.

The syntax for this is the same as voIpProt.SIP.registrarServer.

You can't provision this parameter if the system is in Partner Mode.

String (0-255)

voIpProt.SIP.registrarServer
The IP address or fully qualified domain name (FQDN) of the SIP registrar server. If registering a remote system with an edge server, use that server's FQDN.
SIP signaling by default is sent to ports 5060 (TCP) and 5061 (TLS) on the registrar server.

Enter the address and port using the following format: IP_Address:Port.

The IP_Address can be an IPv4 address or an FQDN (e.g., servername.company.com:6050).

You can't provision this parameter if the system is in Partner Mode.

String (0-255)

voIpProt.SIP.registrarServerType
Specifies the type of SIP registrar server you're using.
You can't provision this parameter if the system is in Partner Mode.

Standard SIP (default) - For standard SIP registrar servers.

voIpProt.SIP.serverType
Specifies whether to automatically or manually set the SIP server's IP address.
If set to "Auto", you don't have to set voIpProt.SIP.transport, voIpProt.SIP.registrarServer, or voIpProt.SIP.proxyServer.

You can't provision this parameter if the system is in Partner Mode.

Specify (default)

Auto

voIpProt.SIP.transport
Sets the protocol your system uses for SIP signaling (your SIP network determines which protocol is required).
Auto (default) - Enables automatic negotiation of protocols in the following order: TLS, TCP, and UDP. This is the recommended setting for most environments.

You can't provision this parameter if the system is in Partner Mode.

TLS - Provides secure SIP signaling. TLS is available only when your system is registered with a SIP server that supports it. If you set this, your system ignores TCP/UDP port 5060.

TCP - Provides reliable transport via TCP.

UDP - Provides best-effort transport via UDP.

voIpProt.SIP.auth.userId
Specifices the username for connecting your system with a SIP registrar server (e.g., marySmith).
If the SIP proxy requires authentication, this parameter and voIpProt.SIP.auth.password cannot be blank.
You can't provision this parameter if the system is in Partner Mode.

String

voIpProt.SIP.userName
Specifies the SIP address or name of the system (e.g., mary.smith@department.company.com). If you leave this blank, the system IP address is used for authentication.
You can't provision this parameter if the system is in Partner Mode.

String

${sip_alias} - Poly Clariti Manager accepts this value to automatically configure the parameter.