Genesys Application Note

Polycom SIP Phones With Genesys SIP Server

Document version 1.8

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

About Genesys

Every year, Genesys® delivers more than 70 billion remarkable customer experiences for organizations in over 100 countries. Through the power of the cloud and AI, our technology connects every customer moment across marketing, sales and service on any channel, while also improving employee experiences. Genesys pioneered Experience as a Service℠ so organizations of any size can provide true personalization at scale, interact with empathy, and foster customer trust and loyalty. This is enabled by Genesys Cloud™, an all-in-one solution and the world's leading public cloud contact center platform, designed for rapid innovation, scalability and flexibility. Go to www.genesys.com for more information.

Each product has its own documentation for online viewing at the Genesys Customer Care website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc. cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Genesys and the Genesys logo are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other company names and logos may be trademarks or registered trademarks of their respective holders.

Table of Contents

1 Summary

Polycom SoundPoint IP and VVX phones are highly recommended as SIP "hard phones" to be integrated and used with the Genesys SIP solution. All voice features, from simple calls to voicemail integration to agent-login, have been successfully validated during extensive testing.

This application note details the supported features, and includes reference configuration examples.

Polycom phones run common firmware across the entire model line. As such, all SoundPoint IP phones with v4.0 firmware (4.0.3.7562 and later) are supported.

The following Polycom VVX phones were tested and supported:

- Polycom VVX phones (VVX 300, VVX 400, VVX 500, VVX 600) with v5.2 firmware (5.2.0.8330 and later) and with v.5.5 firmware (5.5.1.15880 and later).

- Polycom VVX 350 (firmware 5.9.6.2996 and later).

- Polycom VVX phones (VVX 501, VVX 601) with Polycom EagleEye Mini Camera (5.9.1.0615 and later) are supported with video calls.

The supporting versions of Genesys components include SIP Server 8.1.x (8.1.1 recommended), SIP Feature Server 8.1.x (8.1.2 recommended), Media Server (8.5.x and 9.0.x), and SIP Proxy (8.1.x).

Note: Polycom SoundPoint IP and VVX phones support only IPv4.

2 SIP Endpoint Features

2.1 Feature Chart

Feature Name	
General Features Supported By Phone (1pcc)	**Supported**
Agent Login from the Phone	Yes
Agent State Control from the Phone	Yes
Auto-Answer	Yes
Alternate Ringtones	Yes
Caller ID	Yes
Call Forward	Yes
Do Not Disturb	Yes
DNS-based redundancy (using SIP Proxy)	Yes
DTMF tones generation	Yes
IPv6 support	No
Multiple calls on one extension	Yes
Message Waiting Indicator	Yes
Shared Call Appearance (SCA)	Yes
SIP authentication	Yes
TLS/SRTP	Yes
Call Control Using Phone (1pcc)	**Supported**
Basic calling (incoming and outgoing calls)	Yes
Conference	Yes *
Hold/Retrieve	Yes
Unattended transfer	Yes
Semi-attended transfer	Yes
Attended transfer	Yes
Call Control Using Desktop Client (3pcc)	**Supported**
Answer Incoming Call	Yes
Make Outgoing Call	Yes
Hold/Retrieve	Yes
Conference	Yes
Remote Auto-Answer (based on SIP header)	Yes
Unattended transfer (Genesys Single-Step Transfer)	Yes
Semi-attended transfer (Genesys Blind Transfer)	Yes
Attended transfer (Genesys Two-Step Transfer)	Yes
DTMF tone generation	No
Video Support	**Supported**
Basic Video Calls	Yes
Push Video	Yes
Video Call on Hold/Retrieve	Yes
Video Call Transfer	Yes
Video Conference	Yes
Support of Genesys Solutions	**Supported**
Genesys Business Continuity	Yes
Genesys Voice Mail Solution	Yes

* See section 6 for known limitations.

2.2 Feature Chart Glossary

2.2.1 General Features Supported By Phone

1pcc: First-Party Call Control is a method to handle calls using the phone keypad.

3pcc: Third-Party Call Control is a method to handle calls using T-Library desktop connected to SIP Server.

Agent Login from the Phone: Agent sets login/logout from the phone. Agent state ready/not ready can be set from the phone or it can be pushed from the server to the phone after agent logs in from the phone. Functionality is supported based on RFC3863 using presence states open/closed.

Agent State Control from the Phone: This feature enables an agent to perform agent-related operations from the phone: login/logout, change of the state to ready/not ready/ACW, reason code for not ready state. Available for phones that support BroadSoft's Application Server Feature Event Package and Hoteling Event Package.

Alternate Ringtones: Phone provides distinctive ringtones requested by SIP Server. Functionality is supported based on RFC3261 using the Alert-Info header.

Auto-Answer: Phone can be configured to answer all calls automatically.

Caller ID: Phone is able to display the number and name of the calling party.

Call Forward: Phone can forward calls unconditionally or based on internal state (e.g. 'busy').

Do Not Disturb: Phone can reject all incoming calls.

DNS-based redundancy: Phone can toggle between SIP Servers provisioned by single FQDN if current SIP Server becomes unavailable. This functionality is required to deploy a phone with Genesys SIP Proxy. It also may be used for Genesys Business Continuity.

DTMF tones generation: Phone can pass DTMF tones in-band (RFC2833, RFC4733) or using SIP INFO messages.

IPv6 support: Phone can support the IPv6 protocol.

Message Waiting Indicator: SIP MWI support (RFC3842).

Multiple calls on one line: Phone can process multiple incoming/outgoing calls simultaneously on the same line.

Shared Call Appearance (SCA): This feature enables a group of SIP phones to receive inbound calls directed to a single destination (shared line); that way, any phone from this group can answer the call, barge-in to the active call, or retrieve the call placed on hold. The shared line has sub-lines called appearances.

SIP authentication: Phone can authenticate with SIP Server using the HTTP Digest algorithm (RFC3261 and RFC2617).

TLS/SRTP: Phone supports secure SIP environment that uses TLS and SRTP.

2.2.2 Call Control Using Phone (1pcc)

Basic calling: Incoming and outgoing calls.

Conference: Phone can bridge two or more calls without using MCU.

Hold/Retrieve: Phone can put a call on hold and then retrieve it.

Transfer:

- **Unattended transfer**: Call transfer using REFER.
- **Semi-attended transfer**: Completing the transfer when one party is on hold and the other party is ringing, using REFER with Replaces.
- **Attended transfer**: Completing the transfer using REFER with Replaces when one party is on hold and the other party has answered the call.

2.2.3 Call Control Using Desktop Client (3pcc)

Answer Incoming Call: Phone can answer the call using the BroadSoft extension 'talk' passed in SIP NOTIFY.

Make Outgoing Call: Phone can make an outgoing call initiated by SIP Server through the Genesys T-Library interface.

Conference: Phone supports server side single-step or two-step conference.

Hold/Retrieve: Phone can put a call on hold and retrieve it using the BroadSoft extensions 'hold' and 'talk' passed in SIP NOTIFY.

Remote Auto-Answer: Phone can answer a call automatically based on Auto-Answer (RFC5373) or Alert-Info headers.

Transfer:

- **Unattended transfer (Genesys Single-Step Transfer)**: Phone supports unattended transfer initiated by SIP Server using REFER or re-INVITE.
- **Semi-attended transfer (Genesys Blind Transfer)**: Phone supports completion of two-step transfer initiated by SIP Server when one party is on hold and the other party is ringing.
- **Attended transfer (Genesys Two-Step Transfer)**: Phone supports completion of two-step transfer initiated by SIP Server when one party is on hold and the other party has answered the call.

DTMF tone generation: Phone can generate DTMF tones through RTP when the tone generation is requested by SIP Server through the Genesys T-Library interface.

2.2.4 Video Support

Basic Video Calls: Incoming and outgoing video calls.

Push Video: Agent can show a video clip to the customer.

Video Hold/Treatment: Playing a video file when a call is put on hold or a treatment is applied from the routing strategy.

Video Call Transfer: Transferring video calls.

Video Conference: Video Conference with active speaker detection using Genesys Media Server.

2.2.5 Support of Genesys Solutions

Genesys Business Continuity: Phone is certified to be used in Genesys Business Continuity environment in one of two modes. It can switch between the two geo-redundant sites, or it can stay connected to both of them at the same time.

Genesys Voice Mail Solution: Phone is certified with Genesys Voice Mail solution, optionally with advanced features to support group Voice Mail Boxes, work with multiple Voice Mail Boxes configured for one line, and provide easy access to all configured Voice Mail Boxes.

3 Software and Hardware Versions Validated

The following Genesys components and Polycom phones were validated for reference configuration examples.

3.1 Genesys Components

Genesys Components		
Component	**Version**	**Notes**
SIP Server	8.1.1	Call switching and control is performed by Genesys SIP Server. SIP Server communicates via SIP with SIP Endpoints.
Genesys Media Server	8.5.1/9.0.x	Used to handle media interactions such as call treatments (ring back, busy tones and music on hold); also used as MCU.
Genesys Media Server: Media Control Platform	9.0.019.68	Required for video support.
SIP Feature Server	8.1.2	Used as a SIP Voicemail server.
SIP Proxy	8.1.1	Used for HA deployment.

3.2 Polycom SoundPoint IP/VVX phones

3rd Party Hardware Components		
Model	**Version**	**Notes**
Polycom SoundPoint IP Model 335	4.0.3.7562	4.0.3.7562 or later supported
Polycom VVX 300	4.1.3.7864	4.1.3.7864 or later supported
Polycom VVX 300/500/600	5.2.0.8330	5.2.0.8330 or later supported
Polycom VVX 600	5.5.1.15880	5.5.1.15880 or later supported
Polycom VVX 501/601	5.9.1.0615	5.9.1.0615 or later supported
Polycom VVX 350	5.9.6.2996	5.9.6.2996 or later supported

For a full listing of 3rd party hardware/software supported by Genesys, see the Genesys Supported Media Interface Guide (SMI).

4 Features Configuration in Genesys Configuration Environment

This section describes how to configure features represented in Feature Chart (Section 2.1, above) within a Genesys configuration environment.

Features can be configured in the SIP Server Switch on a DN object with type Extension (or ACD Position) representing SIP Endpoint devices, and/or on an Agent Login object, and/or in a SIP Server Application.

Note: It is assumed that the reader has Genesys knowledge and is familiar with deploying a basic Genesys environment.

Features Configuration In Genesys Configuration Environment	
General Features Supported By Phone (1pcc)	
Feature	**Key Actions and Procedures**
Agent Login from the Phone	1. Enable SIP Server mapping of agent-status from SUBSCRIBE or NOTIFY messages from a SIP Endpoint into T-Library Events. In the TServer section of the DN object, configure: **enable-agentlogin-subscribe=true** 2. If required, configure the password used for User authorization during the ACD login operation on the phone. Enter the password in the "Enter password" field on the Advanced tab of the Agent Login object. **Notes:** • The name of the Agent Login object must match the User ID value entered from the phone when you enter Login credentials. • The value of the password field on the Advanced tab must match the password value entered on the phone when you enter Login credentials.
Agent State Control from the Phone	If required, configure the password used for User authorization during the ACD login operation on the phone. Enter the password in the "Enter password" field on the Advanced tab of the Agent Login object. The name of the Agent Login object must match the User ID value entered from the phone when you enter Login credentials. The value of the password field on the Advanced tab must match the password value entered on the phone when you enter Login credentials.
Auto-Answer	No configuration is required.

<table>
<tr><td>Alternate Ringtones</td><td>

If required, specify the ring type for an incoming external call. For an external call, SIP Server will add the specified value to the Alert-Info header of the INVITE message that it sends to the SIP Endpoint. In the TServer section of the DN object, configure:
sip-alert-info-external=external
If required, specify the ring type for a consultation call. For a consultation call, SIP Server will add the specified value to the Alert-Info header of the INVITE message that it sends to the SIP Endpoint. In the TServer section of the DN object, configure:
sip-alert-info-consult=directory
If required, specify the ring type for any type of call. SIP Server will add the specified value to the Alert-Info header of the INVITE message that it sends to the SIP Endpoint. In the TServer section of the DN object, configure:
sip-alert-info=internal

Notes:

Settings in the sip-alert-info-external or sip-alert-info-consult options take precedence over sip-alert-info settings.
The values of these options must match the values set in the phone configuration (.cfg) file:
voIpProt.SIP.alertInfo.1.value="internal"
voIpProt.SIP.alertInfo.2.value="external"
voIpProt.SIP.alertInfo.3.value="directory"

</td></tr>
<tr><td>Caller ID</td><td>No configuration is required.</td></tr>
<tr><td>Call Forward</td><td>No configuration is required.</td></tr>
<tr><td>Do Not Disturb</td><td>No configuration is required.</td></tr>
<tr><td>DNS-based redundancy (using SIP Proxy)</td><td>Requires HA deployment using SIP Proxy deployment. SIP Proxy can be used in SIP Server standalone deployment or Genesys Business Continuity with SIP Proxy deployment. Refer to the Genesys SIP Proxy Deployment Guide and Genesys SIP Server High-Availability Deployment Guide.</td></tr>
<tr><td>DTMF tones generation</td><td>No configuration is required.</td></tr>
<tr><td>Multiple calls on one extension</td><td>See Call Control using desktop client -> Attended transfer feature.</td></tr>
</table>

Message Waiting Indicator	Configure a voice mail box for an Extension. In the TServer section of the DN object, configure: **gvm_mailbox=<voice mail box number>** For example: gvm_mailbox=12003, where 12003 is a mailbox number. **Note:** The voice mail box number must match the number configured in phone Web server as a username in the Subscription Address field: Settings -> Lines -> Line1 -> Message Center.
Shared Call Appearance (SCA)	1. Configure a Primary Shared Line DN: • Create a DN of type Extension with the number where all incoming calls will be delivered. • Specify that this DN is used as a Primary Shared Line number. In the TServer section of the DN object, configure: **shared-line=true** • Specify a number of shared line appearances. In the TServer section of the DN object, configure: **shared-line-capacity=<maximum number of simultaneous calls per shared line>** • If required, configure SIP authentication. (See SIP authentication in this table.) 2. Configure Secondary Shared Line DNs: • Create a DN of type Extension with the number to be used as a Secondary DN. • Specify a number of the Primary DN. In the TServer section of the DN object, configure: **shared-line-number=<number of Primary Shared Line DN>**

Shared Call Appearance (SCA) in Business Continuity (BC) Environment	**Note:** The phone should be configured to use single registration as described in the Genesys Business Continuity section of this document. 1. Configure a Primary shared Line DN: • In the TServer section of the SIP Server application, configure: **dr-peer-location=<specify the name of the other SIP Server DR Peer Switch in the pair>** • Create a DN of type Extension with the number where all incoming calls will be delivered. • In the TServer section of the DN object, configure: **dr-forward=oos** • Specify that this DN is used as a Primary Shared Line number. In the TServer section of the DN object, configure: **shared-line=true** • Specify a number of shared line appearances. In the TServer section of the DN object, configure: **shared-line-capacity=<maximum number of simultaneous calls per shared line>** • If required, configure SIP authentication. (See SIP authentication in this table.) • In the TServer section of the DN object, configure: **sca-preferred-site=<specify the name of the SIP Server DR Peer Switch corresponding to the preferred SCA site>** This option must be configured only for the DN with the option **shared-line=true**. 2. Configure Secondary shared Line DNs: • Create a DN of type Extension with the number to be used as a Secondary DN. • In the TServer section of the DN object, configure: **dr-forward=oos** • Specify the number of the Primary DN. In the TServer section of the DN object, configure: **shared-line-number=<number of Primary shared line DN>**
SIP authentication	1. Specify SIP requests (REGISTER, INVITE) which are sent by the phone to be authenticated by SIP Server. In the TServer section of the DN object, configure: **authenticate-requests=register,invite** 2. If required, configure the password used for authentication of incoming REGISTER or INVITE messages to SIP Server. In the TServer section of the DN object, configure: **password=<Any alphanumerical string>** **Note:** String must match the phone setting in Settings -> Lines -> Line1 -> Authentication/Password.
TLS/SRTP	See the Transport Layer Security for SIP Traffic chapter in the Genesys 8.1 SIP Server Deployment Guide for details.

Video Support	1. Enable all INFO messages to be sent to the peer connection. In the TServer section of the DN object, configure: **info-pass-through=*** 2. Refer to the Video Support chapter in the Genesys 8.1 SIP Server Deployment Guide for more detailed instructions.
Call Control Using Phone (1pcc)	
Feature	**Key Actions and Procedures**
Basic calling (Incoming and outgoing calls)	See the Make Outgoing call feature.
Conference	No configuration is required.
Hold/Retrieve	No configuration is required.
Unattended transfer	No configuration is required.
Semi-attended transfer	No configuration is required.
Attended transfer	No configuration is required.
Call Control Using Desktop Client (3pcc)	
Feature	**Key Actions and Procedures**
Answer Incoming Call	Enable SIP Server to send the SIP NOTIFY (event talk) message when desktop client requests to answer the incoming call. In the TServer section of the DN object, configure: **sip-cti-control=talk** **Note:** The "talk" value affects the Retrieve feature. See Hold/Retrieve feature for information about setting the sip-cti-control option.
Conference	Deploy Genesys Media Server with MCU capabilities. See the Genesys 8.1 SIP Server Deployment Guide for details.
Hold/Retrieve	Enable SIP Server to send the SIP NOTIFY (event hold) message when desktop client requests to hold the call, and the SIP NOTIFY (event talk) message when desktop client requests to retrieve the call. In the TServer section of the DN object, configure: **sip-cti-control=talk,hold**

Make Outgoing Call	1. Create a DN object with type Extension or ACD Position in the Genesys configuration environment under Switch object and DNs folders. This object represents the SIP phone. 2. To activate required features described in this Table, configure options in the DN object > TServer section. 3. Configure a phone to make basic calls (incoming, outgoing) with SIP Server. 4. Restart the phone. 5. After successful SIP registration the phone is ready for making outgoing calls and receiving incoming calls. 6. Run your desktop client to make a test call.
Remote Auto-Answer (based on SIP header)	1. If required, specify the string that SIP Server will add to the Alert-Info header of the INVITE message that it sends to the SIP Endpoint (originator of a call). The string must be known to a phone to automatically answer a call. In the TServer section of the SIP Server Application, configure: **make-call-alert-info= info=alert-autoanswer** 2. If required, specify the string that SIP Server will add to the Alert-Info header of the INVITE message that it sends to the SIP Endpoint (destination of a call). The string must be known to a phone to automatically answer a call. In the TServer section of the DN object, configure: **sip-alert-info= info=alert-autoanswer** **Note:** The specified "info=alert-autoanswer" value must match the settings in the Polycom phone sip.cfg file (alertInfo voIpProt.SIP.alertInfo.x.value parameter). For example: alertInfo voIpProt.SIP.alertInfo.1.value="info=alert-autoanswer"
Unattended transfer (Genesys Single-Step Transfer)	1. If an unattended transfer is to be processed by the SIP REFER method, in the TServer section of the DN object, configure: **refer-enabled=true** 2. If an unattended transfer is to be processed by the SIP re-INVITE method, in the TServer section of the DN object, configure: **refer-enabled=false** **Note:** This option must be set on the DN object that represents a party to be transferred.
Semi-attended transfer (Genesys Blind Transfer)	Enable completion of transfer when the destination is in alerting state. In the TServer section of the DN object (transfer target DN), configure: **blind-transfer-enabled=true** **Note:** This option must be set on the DN object that represents a transfer destination party.

Attended transfer (Genesys Two-Step Transfer)	1. Enable dual dialog to be supported on a DN for an attended transfer operation requested from a desktop client. In the TServer section of the DN object, configure: **dual-dialog-enabled=true** 2. Specify the call flow to process a make call/initiate consultative call operation initiated from a desktop client. In the TServer section of the DN object, configure: **make-call-rfc3725-flow=2** **Note:** A value of 1 or 2 is sufficient for the phone. 3. If an attended transfer is to be completed by the SIP REFER method, in the TServer section of the DN object, configure: **refer-enabled=true** **transfer-complete-by-refer=true** **Note:** These options must be set on the DN object which represents the party to be transferred.
Video Support	3. Enable all INFO messages to be sent to the peer connection. In the TServer section of the DN object, configure: **info-pass-through=*** 4. Refer to the Video Support chapter in the Genesys 8.1 SIP Server Deployment Guide for more detailed instructions.

Example of the DN .cfg file:

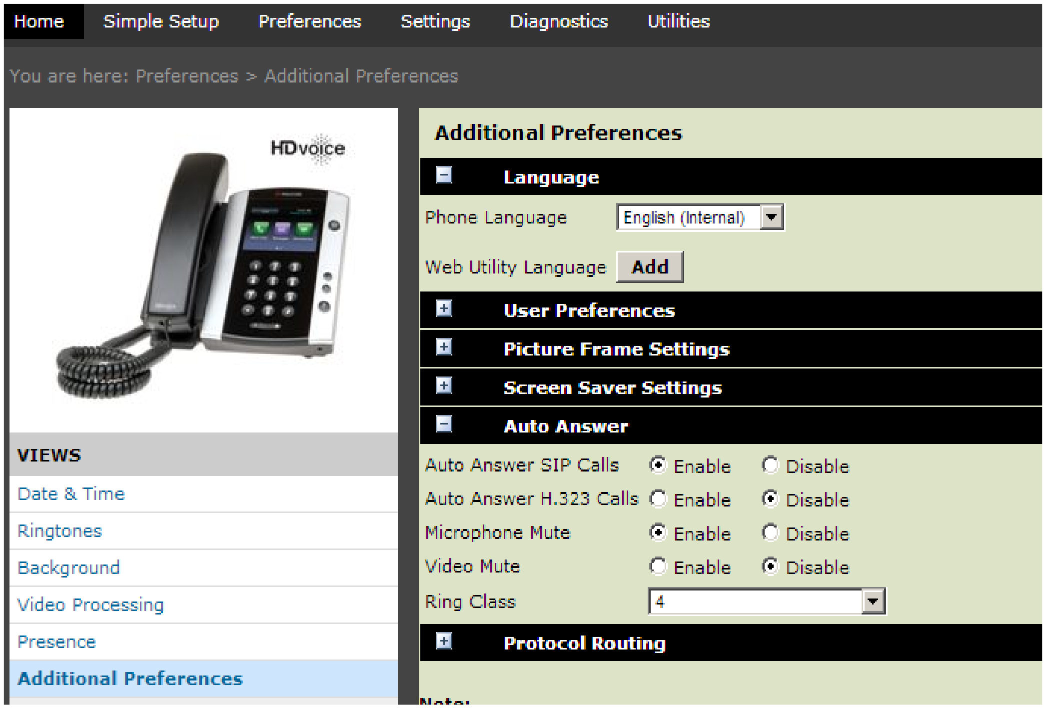
```
[TServer]
authenticate-requests=register,invite
blind-transfer-enabled=true
contact=sip:1669@172.21.83.101
dual-dialog-enabled=true
enable-agentlogin-subscribe=true
make-call-rfc3725-flow=1
refer-enabled=true
sip-alert-info=internal
sip-alert-info-consult=directory
sip-alert-info-external=external
sip-cti-control=talk,hold
transfer-complete-by-refer=true
info-pass-through=*
```

5 Polycom Phone Configuration

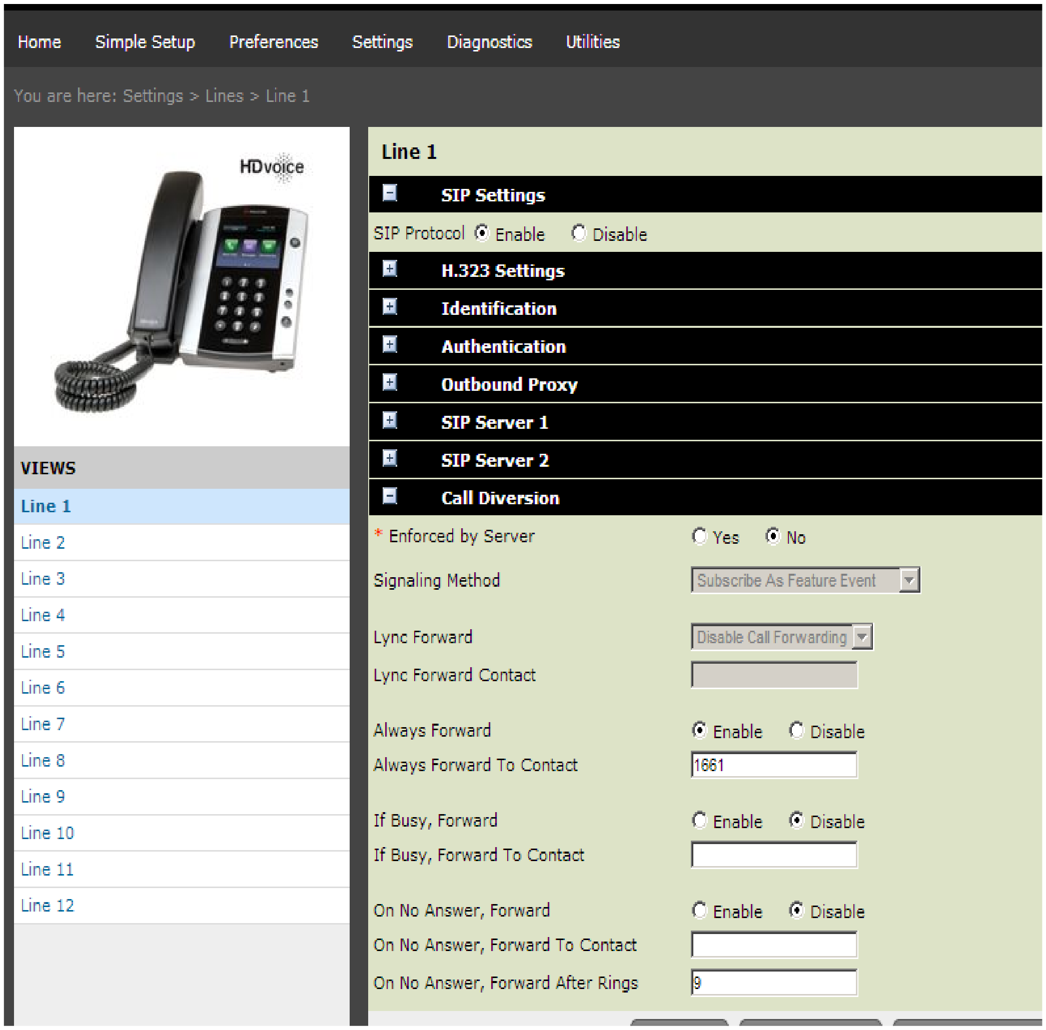
This section describes how to configure features represented in the Feature Chart (Section 2.1, above) using the phone Web interface or using the Polycom configuration file.

The following table displays screenshots of the Web interface of the Polycom VVX 500.

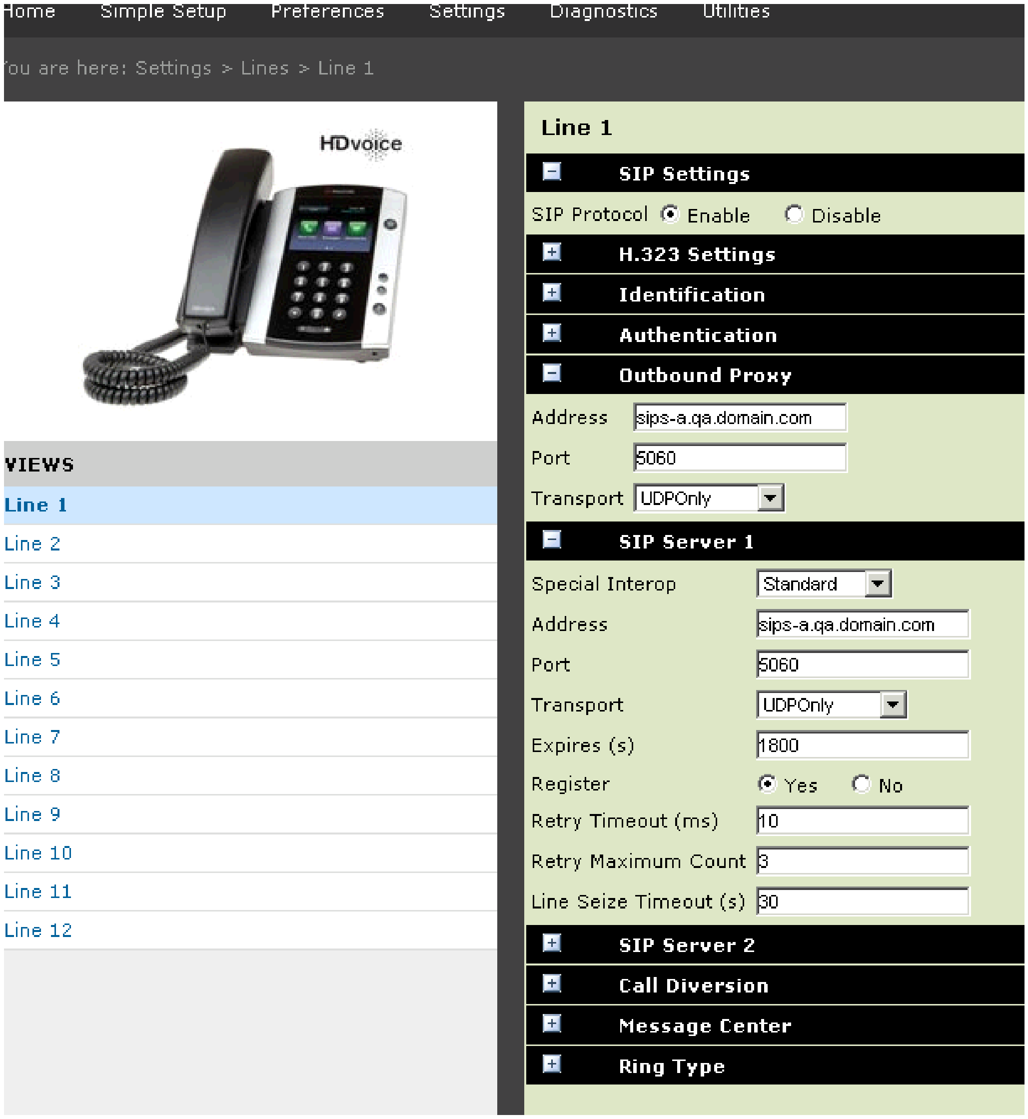
Polycom Phone Configuration	
General Features Supported By Phone	
Feature	**Key Actions and Procedures**
Agent Login from the Phone	1. Using the phone configuration file (.cfg), specify parameters: **feature.acdAgentAvailability.enabled="1"** **feature.acdLoginLogout.enabled="1"** 2. Enter Login Credentials (User ID and Password) from the phone touch screen: User ID and Password.
Agent State Control from the Phone	Using the phone configuration file (.cfg), specify parameters to enable **ACD agent Availability** and **Hoteling Enhancement** features on the phone: feature.acdAgentAvailable.enabled="1" feature.acdLoginLogout.enabled="1" feature.acdPremiumUnavailability.enabled="1" feature.enhancedFeaturekeys.enabled="1" feature.hoteling.enabled="1" feature.acdServiceControlUri.enabled="1" reg.**1**.acd-agent-available="1" ← the underlined digit is the configured line number where the feature is enabled reg.**1**.acd-login-logout="1" ← the underlined digit is the configured line number where the feature is enabled **hoteling.reg="1"** ← the line number where the feature is enabled **acd.reg="1"** ← the line number where the feature is enabled voIpProt.SIP.acd.signalingMethod="1" acd.stateAtSignIn="1" acd.1.unavailreason.active="1" acd.2.unavailreason.active="1" acd.3.unavailreason.active="1" acd.1.unavailreason.codeName="OutToLunch" acd.2.unavailreason.codeName="OutOfOffice" acd.3.unavailreason.codeName="OnVacation" acd.1.unavailreason.codeValue="1" acd.2.unavailreason.codeValue="2" acd.3.unavailreason.codeValue="3"

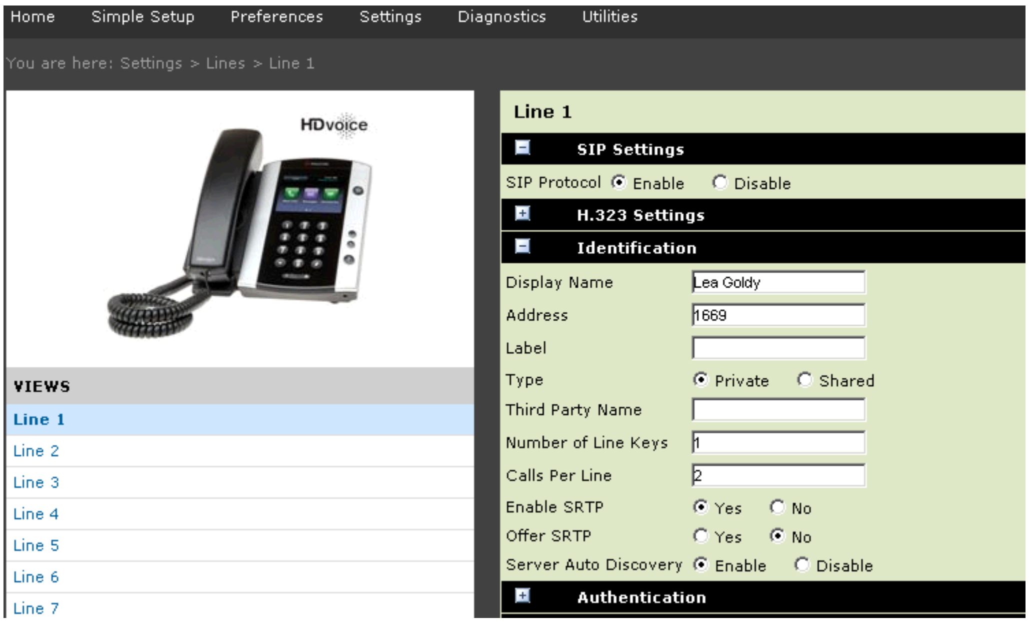
Auto-Answer	Using the Web interface, enable **Auto Answer SIP Calls** for all SIP calls.  Or, In the phone configuration file (.cfg), specify the following parameter: **call.autoAnswer.SIP="1"** **Note**: This feature applies only to the Polycom VVX 500.
Alternate Ringtones	In the phone configuration file (.cfg), specify the following parameters: **se.rt.custom1.name="Low Double Trill"** **se.rt.custom1.ringer="ringer3"** **se.rt.custom2.name="Medium Trill"** **se.rt.custom2.ringer="ringer4"** **se.rt.custom3.name="Triplet"** **se.rt.custom3.ringer="ringer11"** **voIpProt.SIP.alertInfo.1.class="custom1"** **voIpProt.SIP.alertInfo.2.class="custom2"** **voIpProt.SIP.alertInfo.3.class="custom3"** **voIpProt.SIP.alertInfo.1.value="internal"** **voIpProt.SIP.alertInfo.2.value="external"** **voIpProt.SIP.alertInfo.3.value="directory**" **Note:** SIP Server must include the Alert-Info header with the value configured in the **voIpProt.SIP.alertInfo.N.value** parameter. See Alternate Ringtone configuration in Section 4.
Caller ID	No configuration is required.

<table>
<tr>
<td>Call Forward</td>
<td>
Using the Web interface, configure call forward.



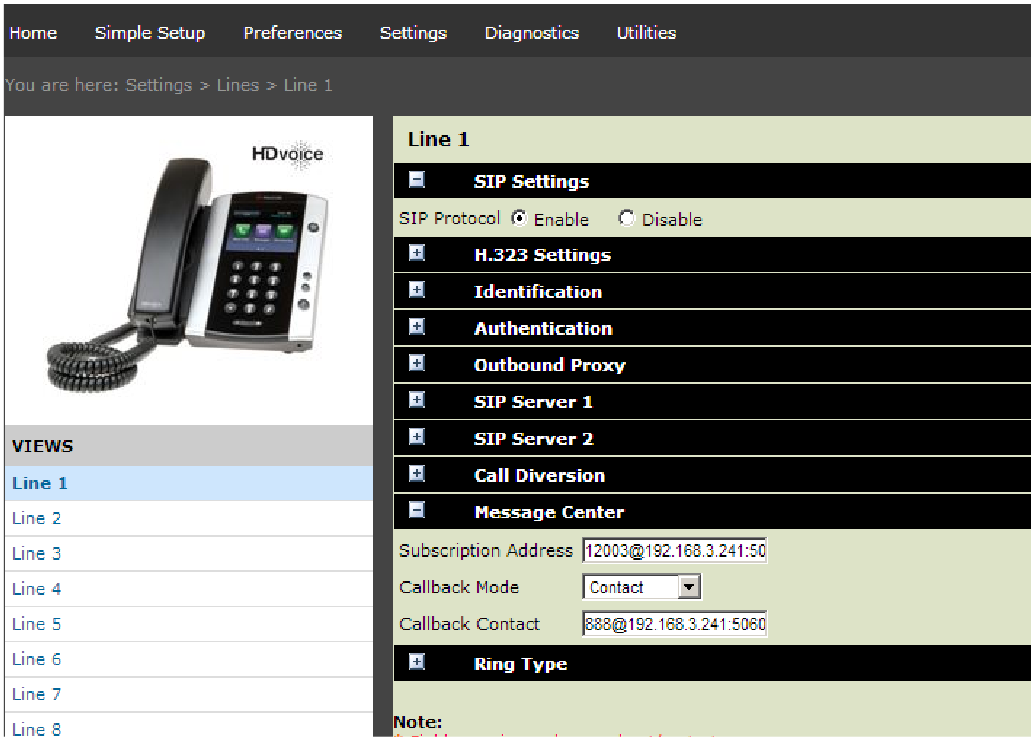
Or,
Using the phone, enable Forward from the phone by pressing the Forward button, then selecting Forwarding type (Forward -> Forwarding).
</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Using the phone, enable DND by pressing the DND button.</td>
</tr>
</table>

DNS-based redundancy (using SIP Proxy)	Using the Web interface, configure **Address** (FQDN of SIP Proxy pool) and **Port** in the **Outbound Proxy** and **SIP Server 1** sections.  **Note:** The Address field has the FQDN (sips-a.qa.domain.com) of a SIP Proxy pool that must be resolved in multiple a-records. Each SIP Proxy in the pool has the same SIP port configured in the Genesys configuration environment. Or, Using the phone configuration file (.cfg), configure the following parameters: **reg.1.server.1.address="sips-a.qa.domain.com"** **reg.1.server.1.expires="1800"** **reg.1.server.1.port="5060"** **reg.1.server.1.retryTimeOut="10"** **reg.1.outboundProxy.address=" sips-a.qa.domain.com "** **reg.1.outboundProxy.port="5060"**

DTMF tones generation	Using the phone configuration file (.cfg), specify the following parameters, as required: **tone.dtmf.viaRtp=”1”** **tone.dtmf.rfc2833Control**="1 **tone.dtmf.rfc2833Payload=”127”** **Note:** The settings above reflect default values.
Multiple calls on one extension	Using the Web interface, for each registration, specify the number of calls that can be active or on hold (**Calls Per Line**). Genesys recommends that **Calls Per Line** be set to 2. The **Display Name** can also be configured using the Web interface.  Or, Using the phone configuration file (.cfg), specify the following parameters: **reg.1.callsPerLineKey="2"** **reg.1.displayName="Lea Goldy"**

<table>
<tr>
<td>Message Waiting Indicator</td>
<td>
Using the Web interface, specify the following information:

- In the **Subscription Address** field, enter a mailbox number, in the format **<mailboxnumber>@<sipserver_host:port>**
- In the **Callback Contact** field, enter the value in the format **<value>@<sipserver_host:port>**. This allows you to access the mailbox by pressing the voicemail button on the phone.



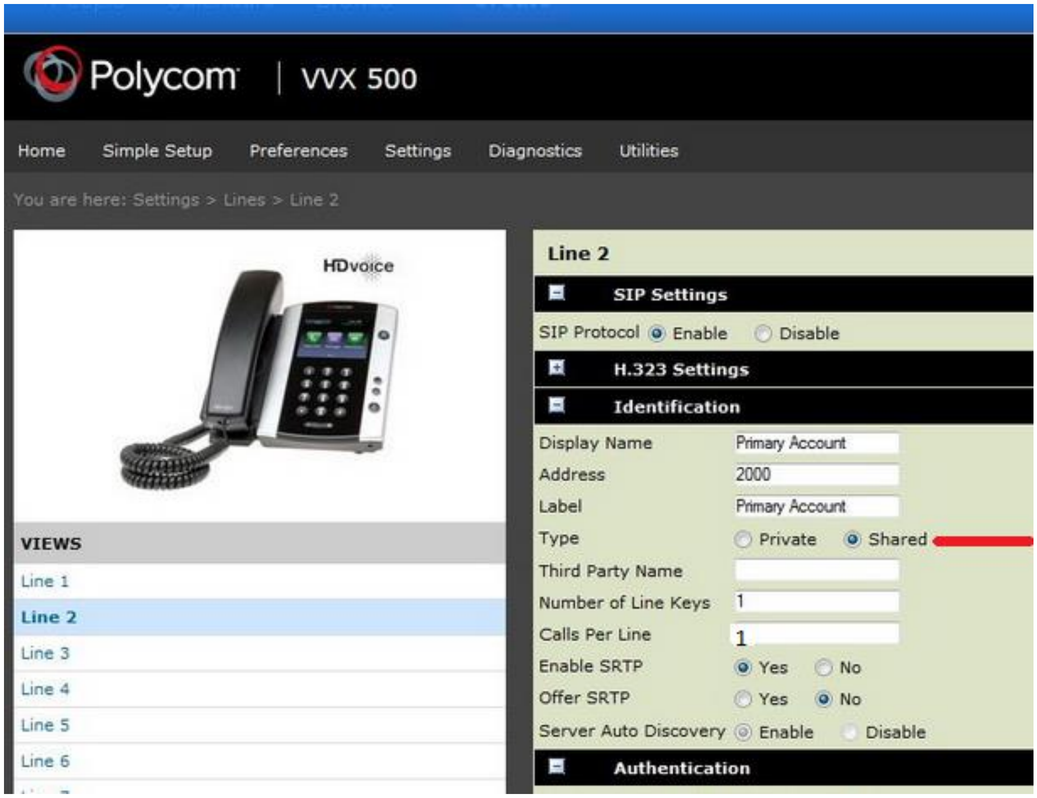
For example:
In the diagram above, the Subscription Address is **12003@192.168.3.241:5060**, where 12003 is a mailbox number.

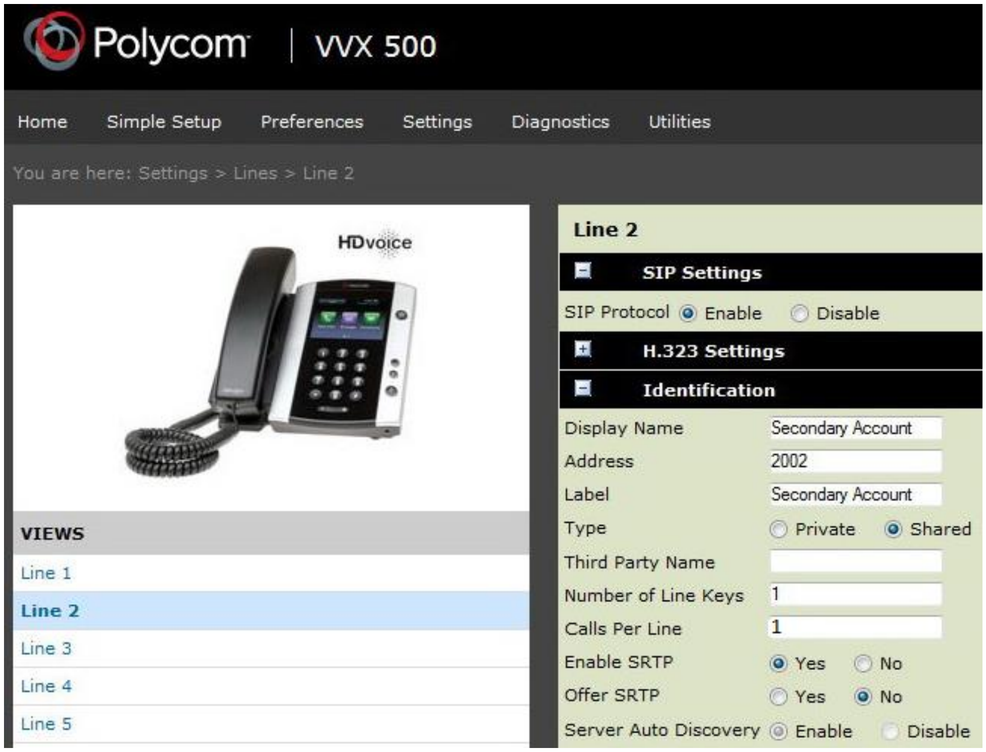
The Callback Contact is **888@192.168.3.241:5060**, where 888 is 888=>gcti::voicemail

Or,

Using the phone configuration file (.cfg), specify the following parameters:

msg.mwi.1.callBack="888@192.168.3.241:5060"
msg.mwi.1.callBackMode="contact"
msg.mwi.1.subscribe="12003@192.168.3.241:5060"
</td>
</tr>
</table>

Shared Call Appearance (SCA)	1. Using the Web interface, configure the Primary Shared Line for Shared Call Appearance: a. Select **Shared** as the line type.  b. If required, configure SIP authentication for the Primary Shared Line. (See SIP authentication in this table.) c. Configure basic calling for the Primary Shared Line. See Call Control Using Phone -> Basic calling (Incoming and outgoing calls). 2. Using the Web interface, configure another phone as the Secondary Shared Line for Shared Call Appearance: a. Select **Shared** as the line type. b. If required, configure SIP authentication for the Shared Line. (See SIP authentication in this table.) **Note:** The Primary User ID must be used in the Authentication when you configure the Secondary Shared Line. c. Configure basic calling for the Secondary Shared Line. See Call Control Using Phone -> Basic calling (Incoming and outgoing calls).



Or,

1. Using the phone configuration file (.cfg), specify the following parameters for the Primary Shared Line:

   reg.2.address="2000"
   reg.2.auth.domain="mydomain.com"
   reg.2.auth.userId="2000"
   reg.2.auth.password="1234"
   reg.2.displayName="Primary Account"
   reg.2.label="Primary Account"
   reg.2.server.1.address="192.168.3.241"
   reg.2.server.1.port="5060"
   reg.2.type="shared"
   reg.2.bargeInEnabled="1"

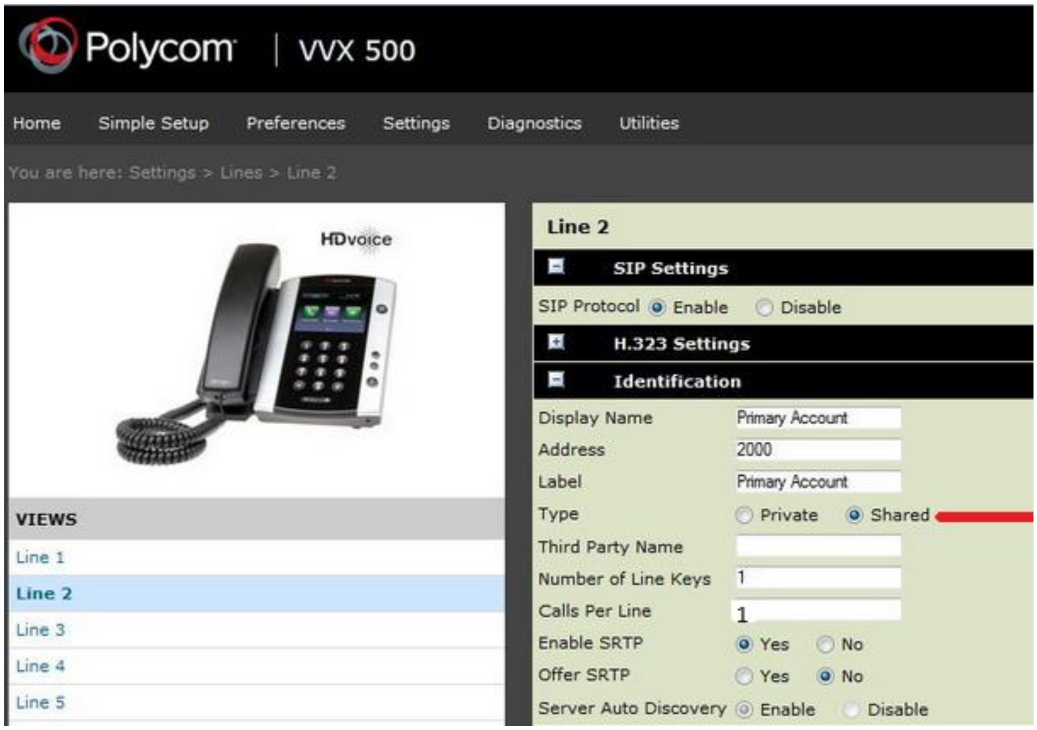
2. Using the phone configuration file (.cfg), specify the following parameters for the Secondary Shared Line:

   reg.2.address="2002"
   reg.2.auth.domain="mydomain.com"
   reg.2.auth.userId="2000"
   reg.2.auth.password="1234"
   reg.2.displayName="Secondary Account"
   reg.2.label="Secondary Account"
   reg.2.server.1.address="192.168.3.240"
   reg.2.server.1.port="5060"
   reg.2.type="shared"
   reg.2.bargeInEnabled="1"

<table>
<tr>
<td>Shared Call Appearance (SCA) in Business Continuity Environment</td>
<td>

1. Using the Web interface, configure the Primary Shared Line for Shared Call Appearance:

   a. Select **Shared** as the line type.



   b. If required, configure SIP authentication for the Primary Shared Line. (See SIP authentication in this table.)

   c. Configure basic calling for the Primary Shared Line. See Call Control Using Phone -> Basic calling (Incoming and outgoing calls).

2. Using the Web interface, configure another phone as the Secondary Shared Line for Shared Call Appearance:

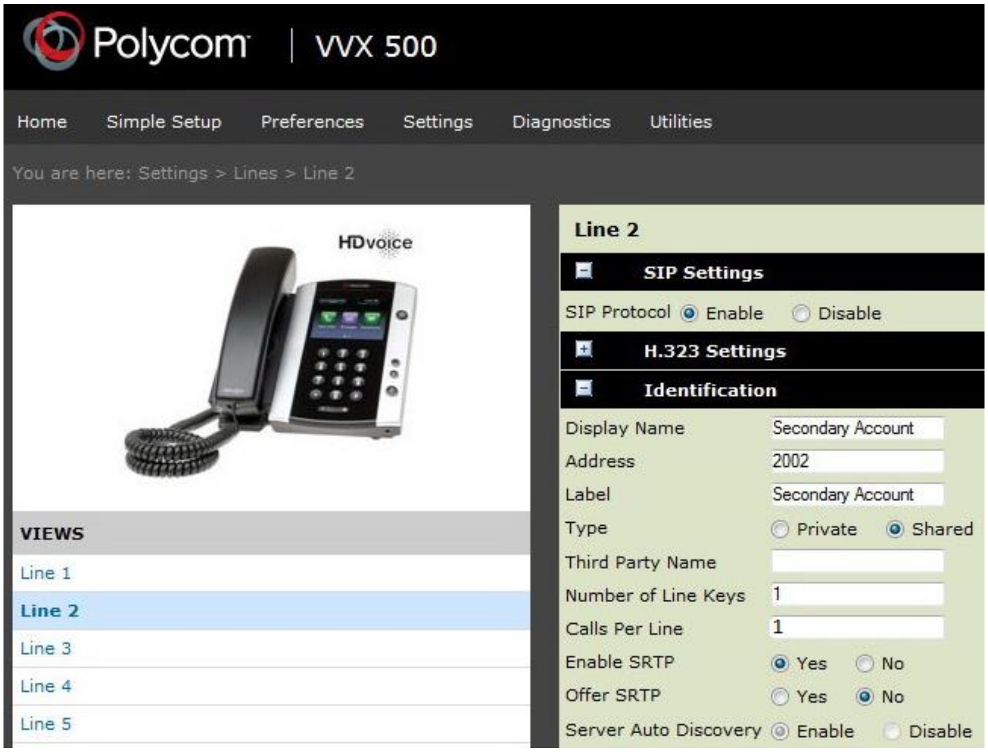
   a. Select **Shared** as the line type.

   b. If required, configure SIP authentication for the Shared Line. (See SIP authentication in this table.)

   Note: The Primary User ID must be used in the Authentication when you configure the Secondary Shared Line.

   c. Configure basic calling for the Secondary Shared Line. See Call Control Using Phone -> Basic calling (Incoming and outgoing calls).

</td>
</tr>
</table>



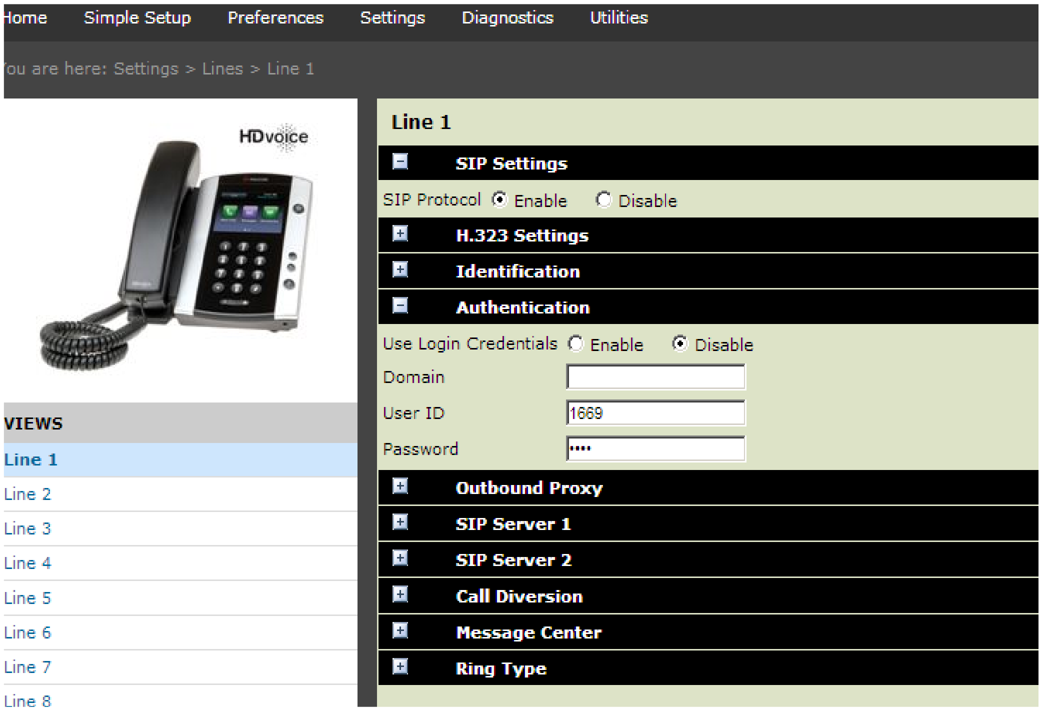
3. Using the phone configuration file (.cfg), specify the following parameters for the Primary Shared Line:

dns.cache.A.1.address="10.10.10.100"
dns.cache.A.2.address="10.10.10.101"
dns.cache.A.1.name="SIPS-811-BC.genesyslab.com"
dns.cache.A.2.name="SIPS-811-BC.genesyslab.com"
dns.cache.A.1.ttl="3600"
dns.cache.A.2.ttl="3600"
reg.2.address="2000"
reg.2.auth.domain="mydomain.com"
reg.2.auth.userId="2000"
reg.2.auth.password="1234"
reg.2.displayName="Primary Account"
reg.2.label="Primary Account"
reg.2.server.1.address="SIPS-811-BC.genesyslab.com"
reg.2.server.1.expires="120"
reg.2.server.1.failOver.failBack.mode="duration"
reg.2.server.1.failOver.failBack.timeout="60"
reg.2.server.1.port="5060"
reg.2.server.1.transport="UDPOnly"
reg.2.auth.loginCredentialType="usernameAndPassword"
reg.2.type="shared"
reg.2.bargeInEnabled="1"

4. Using the phone configuration file (.cfg), specify the following parameters for the Secondary Shared Line:

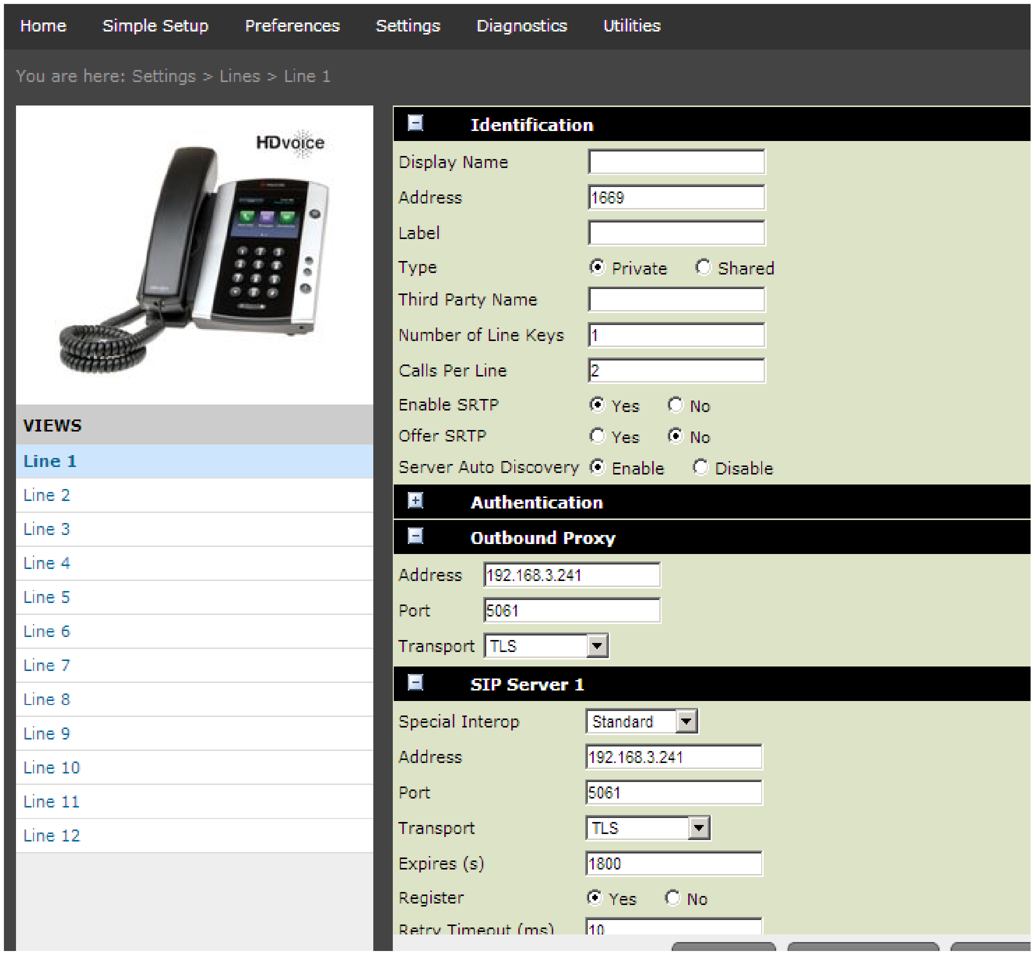
dns.cache.A.1.address="10.10.10.100"
dns.cache.A.2.address="10.10.10.101"
dns.cache.A.1.name="SIPS-811-BC.genesyslab.com"
dns.cache.A.2.name="SIPS-811-BC.genesyslab.com"

	dns.cache.A.1.ttl="3600" dns.cache.A.2.ttl="3600" reg.2.address="2002" reg.2.auth.domain="mydomain.com" reg.2.auth.userId="2000" reg.2.auth.password="1234" reg.2.displayName="Primary Account" reg.2.label="Primary Account" reg.2.server.1.address="SIPS-811-BC.genesyslab.com" reg.2.server.1.expires="120" reg.2.server.1.failOver.failBack.mode="duration" reg.2.server.1.failOver.failBack.timeout="60" reg.2.server.1.port="5060" reg.2.server.1.transport="UDPOnly" reg.2.auth.loginCredentialType="usernameAndPassword" reg.2.type="shared" reg.2.bargeInEnabled="1″

SIP authentication	Using the Web interface, specify login credentials (**User ID** and **Password**) for SIP authentication.  Or, Using the phone configuration file (.cfg), specify the following parameters: **reg.1.auth.password="xxxx"** **reg.1.auth.userId="xxxx"** The Password parameter should have the same value as that of the password option configured on the DN object in the Genesys configuration environment. The User ID parameter is used to authenticate line registration or an outgoing INVITE.

<table>
<tr>
<td>TLS/SRTP</td>
<td>

1. Using the Web interface, specify the SIP Server IP **Address** and **TLS Port**.



Or,
Using the phone configuration file (.cfg), specify the following parameters:

reg.1.address="1669"
reg.1.outboundProxy.address="192.168.3.241"
reg.1.outboundProxy.port="5061"
reg.1.outboundProxy.transport="TLS"
reg.1.server.1.address="192.168.3.241"
reg.1.server.1.port="5061"
reg.1.server.1.transport="TLS"
reg.1.server.1.expires="1800"

2. Using the phone, specify a custom CA Certificate (.pem file) at Home -> Settings -> Advanced -> Administration Settings -> TLS Security -> Custom CA Certificates -> Platform CA 1 -> Install -> Enter URL.

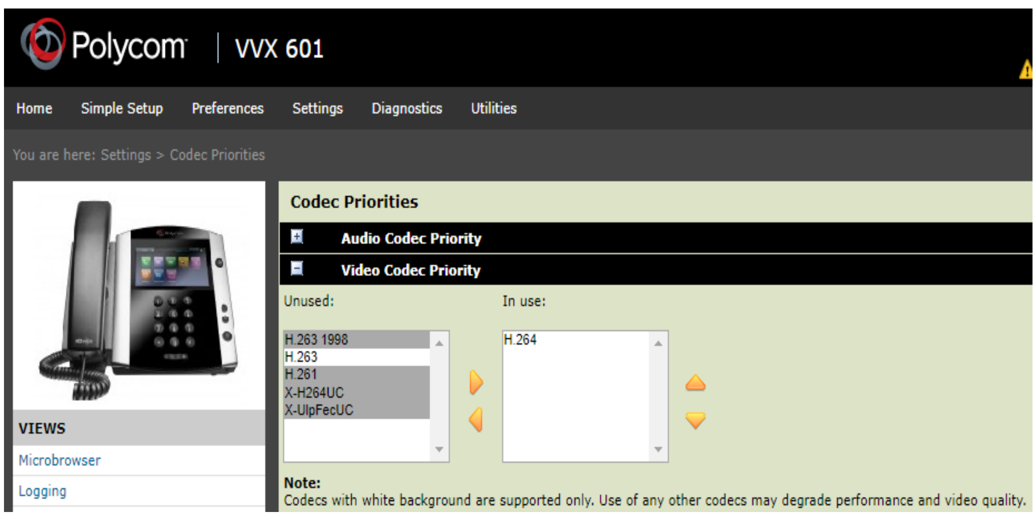
3. Restart the phone.

</td>
</tr>
</table>

<table>
<tr>
<td>Video Support</td>
<td>

1. Configure H.264 video codec.

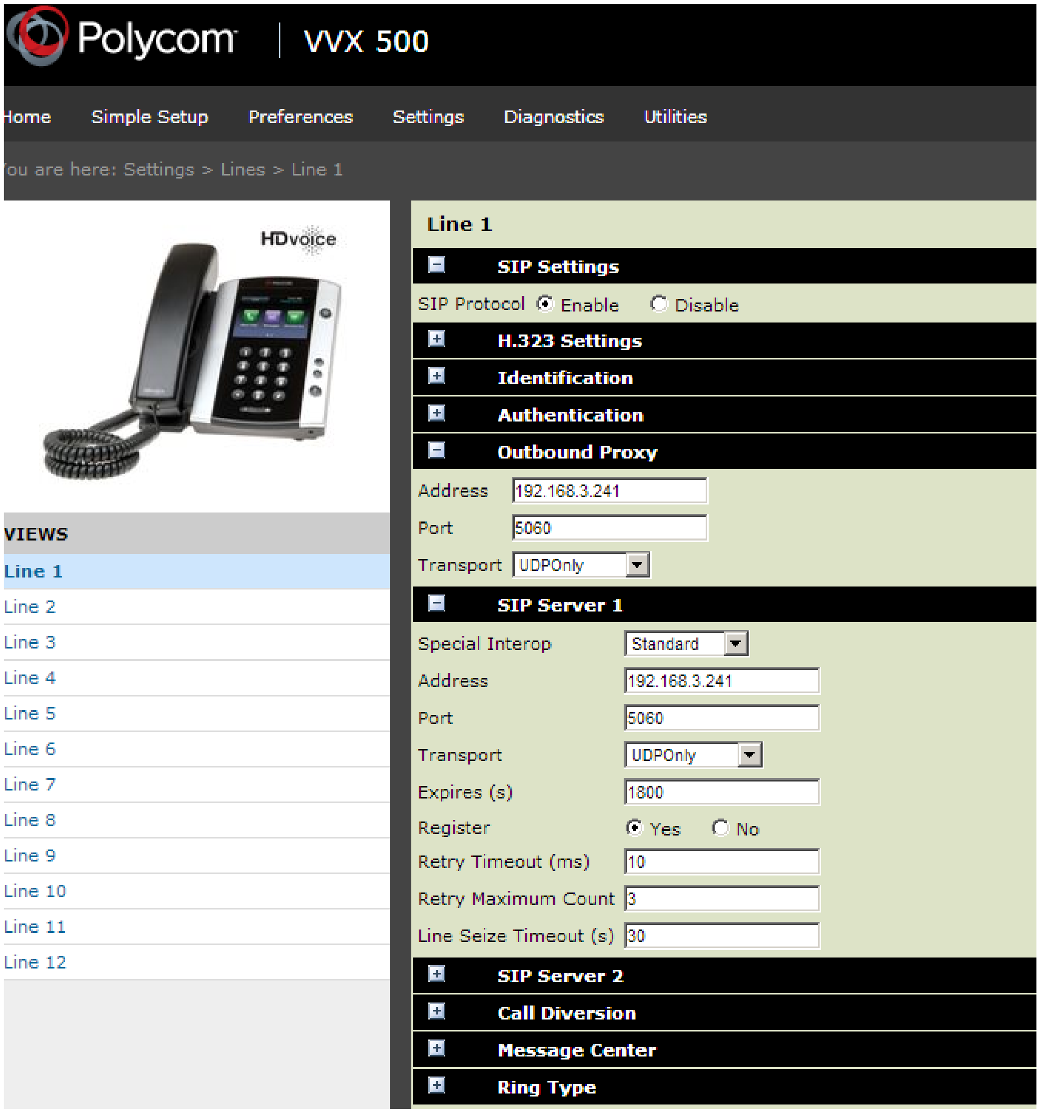
2. Set video codec priorities.



3. Using the phone configuration file (.cfg), specify the following parameters:
video.profile.H264.packetizationMode="1"
video.iFrame.period.onBoard="3"

Note: The Iframe update interval may increase the bandwidth use.

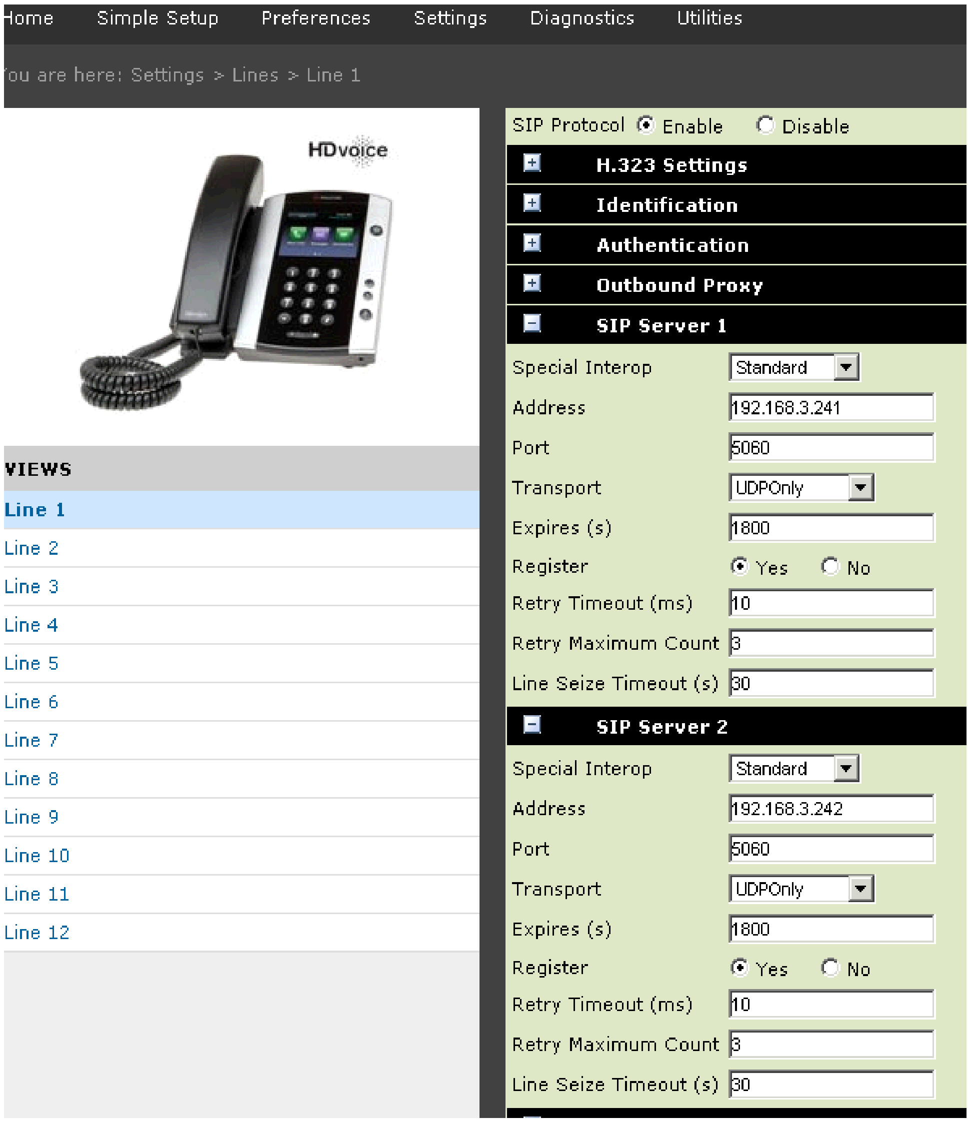
</td>
</tr>
</table>

<table>
<tr><th colspan="2">Call Control Using Phone</th></tr>
<tr><th>Feature</th><th>Key Actions and Procedures</th></tr>
<tr><td>Basic calling (incoming and outgoing calls)</td><td>Using the Web interface, specify the SIP Server IP Address and SIP Port.


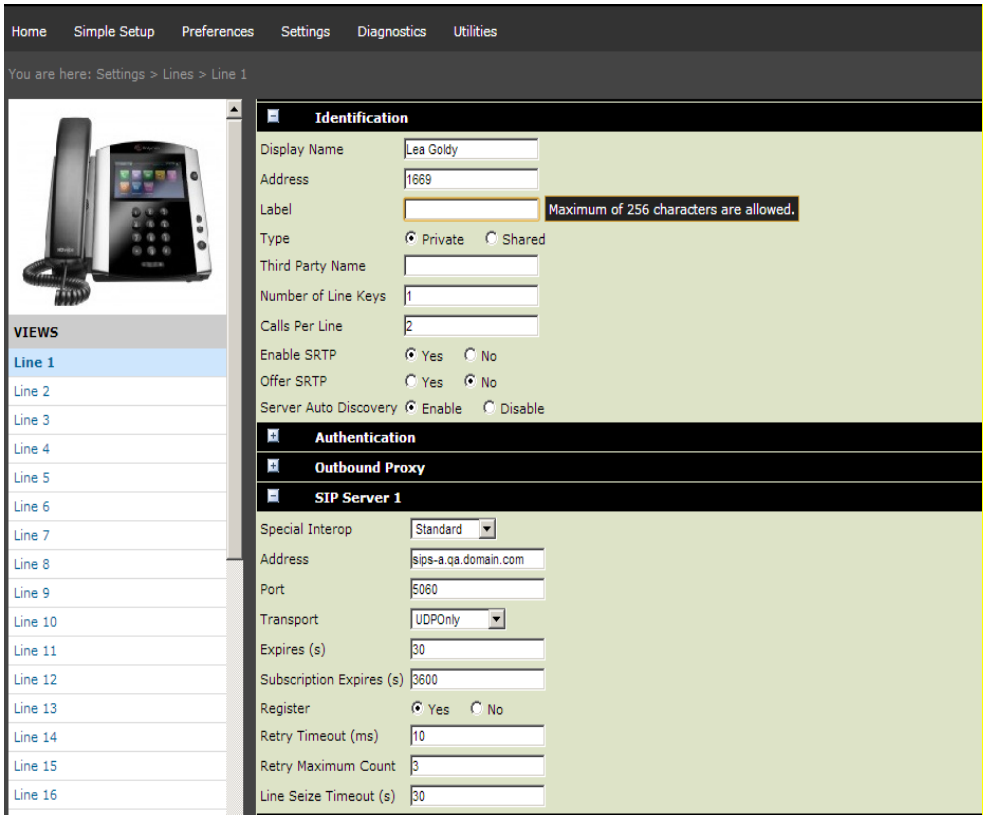
Or,
Using the phone configuration file phone (.cfg), specify the following parameters:

reg.1.address="1669"
reg.1.outboundProxy.address="192.168.3.241"
reg.1.outboundProxy.port="5060"
reg.1.outboundProxy.transport=" UDPOnly "
reg.1.server.1.address="192.168.3.241"
reg.1.server.1.port="5060"
reg.1.server.1.transport=" UDPOnly "
reg.1.server.1.expires="1800"</td></tr>
</table>

Conference	No configuration is required.
Hold/Retrieve	No configuration is required.
Unattended (blind) transfer	Using the phone, press the Transfer button, then select -> more -> blind.
Semi-attended (two-step) transfer	No configuration is required.
Attended (consultative) transfer	No configuration is required.
Call Control Using Desktop Client	
Feature	**Key Actions and Procedures**
Answer Incoming Call	No configuration is required.
Conference	No configuration is required.
Hold/Retrieve	No configuration is required.
Make Outgoing Call	See the Basic calling (incoming and outgoing calls) feature.
Remote Auto-Answer	Using the phone configuration file (.cfg), specify the following parameters: **alertInfo voIpProt.SIP.alertInfo.1.value="info=alert-autoanswer"** **voIpProt.SIP.alertInfo.1.class="4"** **Note:** The "info=alert-autoanswer" value must match the values of **make-call-alert-info** and **sip-alert-info** options in the Genesys configuration environment. See the Remote Auto-Answer feature configured in the Genesys configuration environment.
Unattended transfer	No configuration is required.
Semi-attended transfer	No configuration is required.
Attended (consultative) transfer	No configuration is required.

Genesys Business Continuity	Specify the SIP Server address. **1. For dual registration:** Using the Web interface, specify the SIP Server IP **Address** and SIP **Port** of DR Peer1 in the **SIP Server 1** line settings, and specify the SIP Server IP **Address** and SIP **Port** of DR Peer2 in the **SIP Server 2** line settings. For the Genesys Business Continuity (BC) deployment, the phone must register (SIP REGISTER) with both DR Peers simultaneously. Refer to the following diagram.  Or, Using the phone configuration file (.cfg), specify the following parameters: **reg.1.server.1.address=" 192.168.3.241"** **reg.1.server.1.expires="1800"** **reg.1.server.1.port="5060"** **reg.1.server.1.retryTimeOut="10"** **reg.1.server.2.address=" 192.168.3.242"** **reg.1.server.2.expires="1800"** **reg.1.server.2.port="5060"** **reg.1.server.2.retryTimeOut="10"**

2. For single registration:
Using the Web interface, specify the FQDN to be resolved in two IP addresses that correspond to SIP Server peer 1 and SIP Server peer 2.



Or,
Using the phone configuration file (.cfg), specify the following parameters:

reg.1.server.1.address=" sips-a.qa.domain.com "
reg.1.server.1.failOver.failBack.mode="registration"
reg.1.server.1.failOver.failRegistrationOn="1"
reg.1.server.1.failOver.reRegisterOn="1"
reg.1.server.1.port="5060"
reg.1.server.1.expires="30"
reg.1.server.1.port="5060"
reg.1.server.1.retryTimeOut="10"
reg.1.server.1.transport="UDPOnly"

Note: The "Agent State Control from the Phone" feature requires single registration phone configuration to work in the BC deployment.

Examples of the phone configuration file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- Application SIP Helford 5.9.0.9373 06-Dec-18 01:52 -->
<!-- Created 01-01-1970 00:05 -->
<!-- Base profile Generic --><PHONE_CONFIG>
      <PHONE_LOCAL
            np.normal.ringing.toneVolume.chassis="-51"
            se.rt.custom1.name="Low Double Trill"
            se.rt.custom1.ringer="ringer3"
            se.rt.custom2.name="Medium Trill"
            se.rt.custom2.ringer="ringer4"
            se.rt.custom3.name="Triplet"
            se.rt.custom3.ringer="ringer11"
            voIpProt.SIP.alertInfo.1.class="custom1"
            voIpProt.SIP.alertInfo.2.class="custom2"
            voIpProt.SIP.alertInfo.3.class="custom3"
            voIpProt.SIP.alertInfo.1.value="internal"
            voIpProt.SIP.alertInfo.2.value="external"
            voIpProt.SIP.alertInfo.3.value="directory"
      />
</PHONE_CONFIG>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- Application SIP Helford 5.9.0.9373 06-Dec-18 01:52 -->
<!-- Created 01-01-1970 00:05 -->
<!-- Base profile Generic --><PHONE_CONFIG>
      <!-- Note: The following parameters have been excluded from the export:
            reg.1.auth.password=""
      -->
      <WEB
            feature.acdAgentAvailability.enabled="1"
            feature.acdLoginLogout.enabled="1"
            log.level.change.log="0"
            log.level.change.sip="0"
            np.normal.ringing.calls.tonePattern="ringer3"
            np.normal.ringing.toneVolume.chassis="-45"
            msg.mwi.1.callBack="888@92.168.3.241:5060"
            msg.mwi.1.callBackMode="contact"
            msg.mwi.1.subscribe="12003@192.168.3.241:5060"
            reg.1.acd-agent-available="1"
            reg.1.acd-login-logout="1"
            reg.1.address="1669"
            reg.1.auth.userId="nina"
            reg.1.callsPerLineKey="2"
            reg.1.displayName="Lea Goldy"
            reg.1.outboundProxy.address="192.168.3.241"
            reg.1.outboundProxy.port="5060"
            reg.2.outboundProxy.port="5060"
            reg.1.outboundProxy.transport="UDPOnly"
            reg.2.outboundProxy.transport="UDPOnly"
```

```
            voIpProt.server.1.expires="10"
            voIpProt.server.1.register="0"
            reg.1.server.1.address="192.168.3.241"
            reg.1.server.1.expires="1800"
            reg.1.server.2.expires="1800"
            reg.2.server.1.expires="60"
            reg.1.server.1.port="5060"
            reg.2.server.1.port="5060"
            reg.1.server.1.retryTimeOut="10"
            reg.1.server.2.retryTimeOut="10"
            reg.1.server.1.transport="UDPOnly"
            reg.1.server.2.transport="UDPOnly"
            reg.2.server.1.transport="UDPOnly"
            video.codecPref.H261="0"
            video.codecPref.H263="1"
            video.codecPref.H2631998="0"
            video.codecPref.H264="1"
            video.codecPref.XH264UC="0"
            video.codecPref.XUlpFecUC="0"
            video.profile.H264.profileLevel="2"
            video.camera.contrast="3"
            video.profile.H264.profileLevel="2"
            video.profile.H264.packetizationMode="1"
            video.iFrame.period.onBoard="3"
      />
</PHONE_CONFIG>
```

6 Known Issues and Limitations

Issues and Limitations Identified with Genesys Products

When SIP Server is operating with Polycom phones:

- Three-way conference on the phone is not supported in a call center deployment. Call participants can talk to each other, but such a call is not reported as a conference.

Issues and Limitations Identified with Third-Party Products

When Polycom phones are operating with SIP Server:

- When using TLS over TCP, if the connection from the phone is dropped for any reason, such as switchover of the primary/backup SIP Server, the phone might become unreachable for 40 seconds or more.