Device Certificates on Polycom® Phones

Feature Profile 37148

Device Certificates are an important element in deploying a solution that ensures the integrity and privacy of communications involving Polycom® UC Software devices.

Device Certificates are used in the following situations:

- Mutual TLS Authentication: Allows a server to verify that a device is truly a Polycom device (and not a malicious endpoint or software masquerading as a Polycom device). This could be used for tasks like provisioning, or SIP signaling using TLS signaling. For example, certain partner provisioning systems use Mutual TLS as does Polycom® Zero Touch Provisioning (ZTP).
- Secure HTTP (https) access to the web server on the phone at https://<IP ADDRESS OF PHONE>. The web server is used for certain configuration and troubleshooting activities.
- Secure communications utilizing the Polycom Applications API.

There are several options for utilizing device certificates on the phone. This feature profile provides details on how each of these options can be installed and configured:

- A factory installed device certificate. This certificate is installed at the time of manufacture and is unique to a device (based on the MAC address) and signed by the Polycom Certificate Authority (CA). Since it is installed at the time of manufacture, it is the easiest option for out-of-box activities; in particular, device provisioning.
- Two platform device certificates. These certificates are loaded onto the device by the system administrator and can be configured to be used for any of the following purposes: 802.1X Authentication, provisioning, syslog, SIP signaling, browser communications, presence, and LDAP.
- Six Application device certificates. These certificates are loaded onto the device by the system administrator and can be used for all of the operations listed above for platform certificates with the exception of 802.1X, syslog, and provisioning.

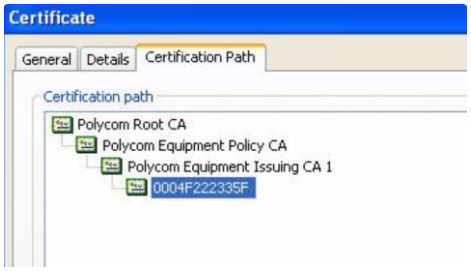
Configuration options are used to select which type of device certificate is used for each of the secure communication options. By default, all operations will utilize the factory installed device certificate.

Note: Terminology Mapping for CA and Device Certificates

In the feature profile, we use the terms CA and device certificates. These are also known as server and client certificates.

To configure your web servers and/or clients to trust Polycom factory installed device certificates, you will need to download the Root CA certificate, which is available at http://pki.polycom.com/pki . You

may also need to download the Intermediate CA certificates; this is determined by the authenticating server. The following figure shows a sample certification path.



Device Certificates

Polycom UC Software devices support several types of device certificates. There is one 'built-in' certificate. In most cases this certificate will have been installed at the Polycom manufacturing facility. If however there is no factory installed certificate, the device will generate a 'self signed certificate' to be used as the 'built-in' certificate.

There are additional certificates that may be installed onto the product by a system administrator. The device may be configured to use either the built-in certificate or one of the installed platform or application device certificates. Different device certificates may be used for different authentication purposes. By default, the built-in certificate is used for all operations.

In addition, you can add custom device certificates to phones running SIP 3.3.2 or later:

- You can add one custom device certificate to a phone running SIP 3.3.2.
- You can add up to eight custom device certificates to a phone running UCS 4.0.0 or later.

Built-In Device Certificates

There are two possible types of 'built-in' device certificates. They can be either a factory installed certificate (most common) or a self-signed certificate, which is created by the device itself if no factory installed certificate exists. See To verify that the certificate you see is an original Polycom Factory certificate, it must be signed by a Polycom intermediate CA **and** have a matching issuer thumbprint. The issuer thumbprint is an MD5 or SHA1 digest unique to only that certificate. Finger prints for Polycom certificates can be found by viewing the certificates at http://pki.polycom.com/pki.

Device Certificates on

Polycom® Phones

Determining Type of Device Certificates on Polycom Phones To verify that the certificate you see is an original Polycom Factory certificate, it must be signed by a Polycom intermediate CA **and** have a matching issuer thumbprint. The issuer thumbprint is an MD5 or SHA1 digest unique to only that certificate. Finger prints for Polycom certificates can be found by viewing the certificates at http://pki.polycom.com/pki.

Determining Type of Device Certificates for detailed information on how to determine if a phone has a certificate installed and what type it is.

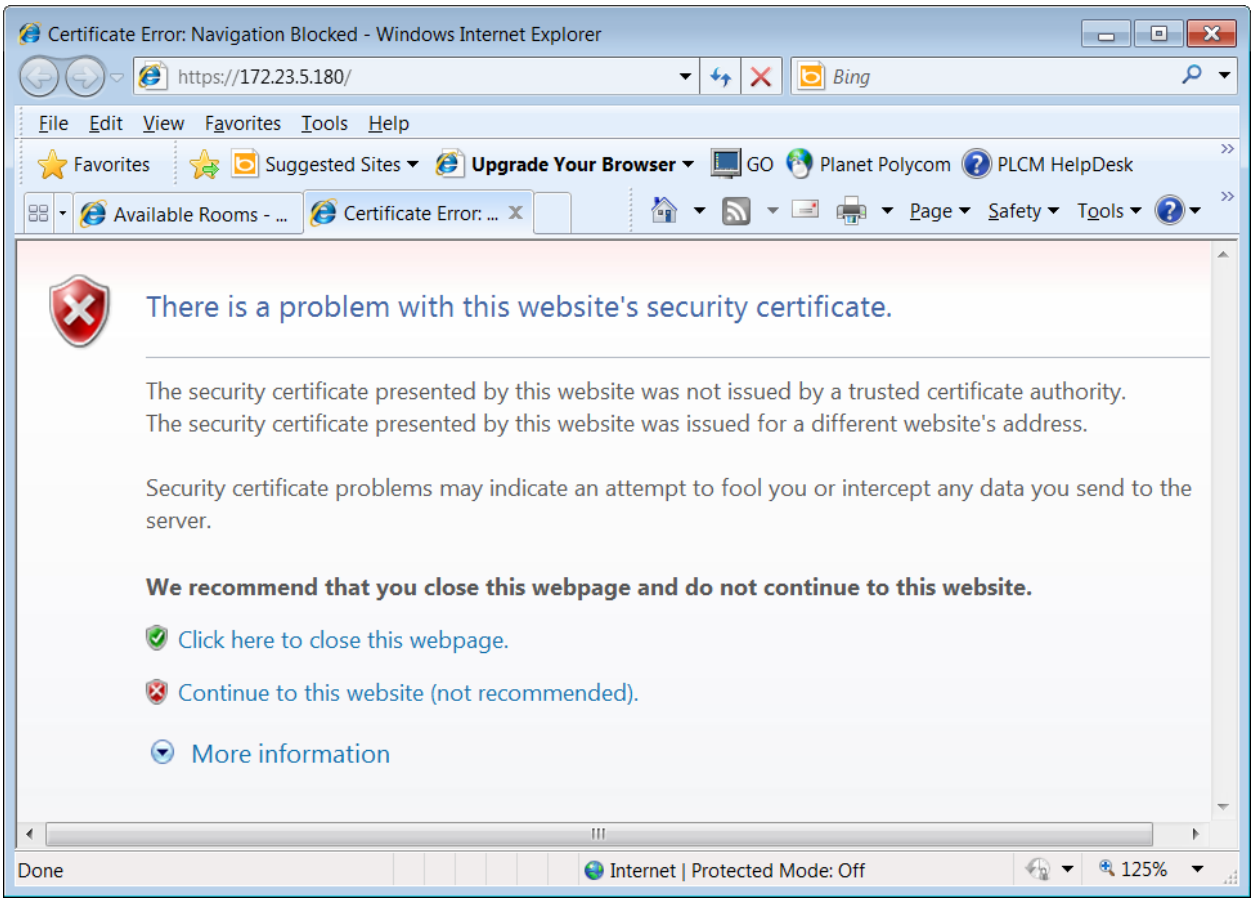
Factory Installed Certificates

A factory installed certificate is installed at time of manufacture at the Polycom manufacturing facility. Factory installation of certificates was initiated in late 2009 and all Polycom phones manufactured since then have such a certificate installed. Each factory installed certificate is assigned to the unique MAC address of each phone and is signed by Polycom as a Certificate Authority (CA). There are a few exceptions for newer products, for example pre-production units of new device models may not have a certificate installed. See Device Certificate Implementation Date to confirm the implementation date for factory installed certificates on Polycom phones.

Self -Signed Certificates

To allow HTTPS transactions with the phone when there is no factory installed certificate, the device will generate a ‘self-signed’ certificate upon upgrade to UC Software 4.0.0 or later. This certificate has both the signing authority and subject of the certificate set to the MAC address of the device. If you want to use the Web Configuration Utility to update the configuration of a phone with a self-signed certificate, you’ll need to accept the self-signed even though most browsers will tell you not to.

The following figure shows what happens when you enter the phone's IP address into Internet Explorer.



These certificates will be identified in the phone's Status menu as 'Self-Signed'.

Note: Issue When Software Downgraded

If a device with a self-signed certificate is downgraded to UC Software 3.3.x or earlier, the menu will incorrectly indicate that a factory installed certificate exists on that device. See the Troubleshooting section for assistance in identifying this type of scenario.

Polycom Phone Device Certificate Types

Beginning in UCS 3.3.2, you can add a custom device certificate to Polycom phones. As of UCS 4.0.0, you can add several different device certificates. There are two types of custom device certificates: platform certificates and application certificates. The two platform certificates are stored in the device's flash memory and are used by both the Updater and the application parts of the UC Software. The six

application certificates are stored in the device's RAM and are used by the application part of the UC Software.

Platform Certificates

Platform certificates can be installed using one of the following methods:

- **Using a configuration file**. You must enter the certificate in PKCS #7 certificate format.
  - In UCS 4.0.x or later, the configuration parameters are:

    `device.sec.TLS.customDeviceCert`**`X`**`.set`

    `device.sec.TLS.customDeviceCert`**`X`**`.publicCert`

    `device.sec.TLS.customDeviceCert`**`X`**`.privateKey`

    where X = 1 or 2.
  - In UCS 3.3.2 and later, the configuration parameters are:

    `device.sec.SSL.customDeviceCert.set`

    `device.sec.SSL.customDeviceCert.publicCert`

    `device.sec.SSL.customDeviceCert.privateKey`
- **From the phone (UCS 4.0.0 or later only)**. Navigate to **Menu > Settings > Advanced > Admin Settings > TLS Security > Configure TLS Profiles > Custom Device Credentials**. You must enter a URI linking to a PEM formatted certificate in PKCS #7 certificate format.
- **From the Web Configuration Utility**. See 'TLS Profiles' in the latest *UC Software Administrators' Guide*. You must enter a URI linking to the device certificate as a single file with the PEM formatted certificate or PKCS #7 certificate chain and private key concatenated together as shown next.

```
-----BEGIN CERTIFICATE-----
MDc1RDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAN9e0DPnIKfDdBTR
+nYK6l5sW0X6W+ygsUdeclsK0+VdEApWSddYnhzfKSRTkwqYRGnxcCzEVqRNcO7c
b5Hac0YZQq9NLPJYjsZRQ8iAxCkwFdqu2jQ398aBM1exPvy6SYHheIkju71giFB6
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEA317QM+cgp8N0FNH6dgrqXmxbRfpb7KCxR15yWwrT5V0QClZJ
11ieHN8pJFOTCphEafFwLMRWpE1w7txvkdpzRhlCr00s8liOxlFDyIDEKTAV2q7a
NDf3xoEzV7E+/LpJgeF4iSO7vWCIUHr/0lGW0TpLzwrpV/cdShMuxyfqWS+Gh8+c
/T42HW3TMSYlXiv6Hr2wvopq+EiRnMDJI1ImA8h7wz6BmXXwpFIBzIbqQwXpxjlJ
-----END RSA PRIVATE KEY-----
```

- **By generating a Certificate Signing Request (CSR).** See Generating a Certificate Signing Request.

The total size of the platform certificate plus private key is restricted as follows:

- Platform Certificate –8192 bytes.
- Platform Private Key–4096 bytes.

If the administrator attempts to download a certificate that is too big, 'Failed to save certificate' displays on the phone's screen and a message appears in the log file (shown next).

```
0529103935|tls  |4|03|Device credential invalid: Cert is not proper in the
certificate
```

Application Certificates

Application certificates can be installed in UCS 4.0.0 or later using one of the following methods:

- **Using a configuration file**. You must enter the certificate in PKCS #7 certificate format. The configuration parameters are:

  `sec.TLS.customDeviceCert.x`

  `sec.TLS.customDeviceKey.x`
- **From the phone**. Navigate to **Menu > Settings > Advanced > Admin Settings > TLS Security > Configure TLS Profiles > Custom Device Credentials**. You must enter a URI linking to a PEM formatted certificate in PKCS #7 certificate format.
- **From the Web Configuration Utility**. See 'TLS Profiles' in the latest *UC Software Administrators' Guide*. You must enter a URI link to the certificate and private key as shown in Platform Certificates.
- **By generating a Certificate Signing Request (CSR).** See Generating a Certificate Signing Request.

There is no size constraint on the application certificate and private key.

Generating a Certificate Signing Request

You may need a certificate to perform a number of tasks, for example, mutual TLS authentication. To obtain a certificate you need to:

- Request a certificate from a Certificate Authority (CA) by creating a certificate signing request (CSR).
- Forward the CSR to a CA to create a certificate. The CA will send back a certificate that has been digitally signed with their private key.

After you receive the certificate, you can download it to the phone.

To generate a certificate signing request on a Polycom phone:

1 Navigate to **Settings** > **Advanced** > **Admin Settings** > **Generate CSR**.

When prompted, enter the administrative password and press the **Enter** soft key. The default administrative password is **456**.

2 From the Generate CSR Screen, enter the desired information as shown next.

You must enter a common name, but organization, email address, country, and state are optional.

3 Press **Generate**.

A message 'CSR generation completed' displays on the phone's screen. The CSR file (<*MAC Address*>.csr) and the private key file (<*MAC Address* >-private.key) are uploaded to the provisioning server. The public key (the other part of the key pair generated by the phone) is included in the CSR.

Configuring the Device Certificate to be Used

This section applies only if UCS 4.0.0 or later is running on your Polycom phones.

The device can be configured to use different device certificates for each operation (or the same device certificate can be used for multiple operations). The operations available are:

- 802.1X
- Syslog
- Provisioning
- SIP
- Browser
- Presence
- LDAP

This configuration can be done:

- Using configuration files.
- From the phone menu.
- From the Web Configuration Utility.

More information can be found in 'TLS Profiles' and '<device/>' in the latest *UC Software Administrators' Guide*.

Device Certificates on

Polycom® Phones

Note: Error in the UC Software Administrators' Guide for UCS 4.0.1

The permitted values for `device.sec.TLS.profile.deviceCert1` and `device.sec.TLS.profile.deviceCert2` are incorrect in the UC Software Administrators' Guide for UCS 4.0.1. The permitted values are **Builtin**, **Platform1**, or **Platform2** only. The UC Software Administrators' Guide will be corrected for the next software release.

Troubleshooting

If the TLS authentication is not working and you suspect there may be an issue with the device certificate, use one of the following options to verify the device certificate.

- **From the phone menu.** Navigate to **Menu > Settings > Advanced > Admin Settings > TLS Security > Configure TLS Profiles > Custom Device Credentials**.
- **From the log files.** In the <MAC Address>-app.log file, look for the messages like the following:
  - Error: Key file too large

    ```
    hwDescSecurityDeviceCredentialsStore: Could not store key for custom device key1, length 4677 is bigger than maximum 4096
    ```

  - Error: forgetting to include "----- Begin PKCS7 ------" and "----- End PKCS7 ------" around the certificate in the configuration file

    ```
    0531131822|hw   |4|03|hwDescSecurityDeviceCredentialsStoreAscii: Could not decode cert chain, results 0
    ```

  - On a successful installation:

```
0531130928|tls  |*|03|Saving new Custom platform device certificate 1
0531130928|tls  |*|03|New Certificate Common Name '0004F206075D' Fingerprint 'CA:70:79:D5:FA:B8:3E:6A:DF:A0:F6:80:3D:53:0B:FC'
  0531130928|tls  |*|03|No previous certificate stored
```

  - On bootup, factory certificate installed as well as 1 custom certificate:

```
000005.930|tls  |3|03|Polycom device certificate length 802
000005.932|tls  |3|03|Polycom device certificate MD5 fingerprint: 70:8B:85:9C:49:4E:28:E2:3C:03:4C:D8:AA:0D:8E:17
000005.932|tls  |3|03|Polycom device certificate common name "0004F206075D"
000005.934|tls  |3|03|Polycom device key length 636
000005.944|tls  |3|03|Custom platform device certificate 1 length 2021
000005.948|tls  |3|03|Custom platform device certificate 1 MD5 fingerprint: CA:70:79:D5:FA:B8:3E:6A:DF:A0:F6:80:3D:53:0B:FC
```

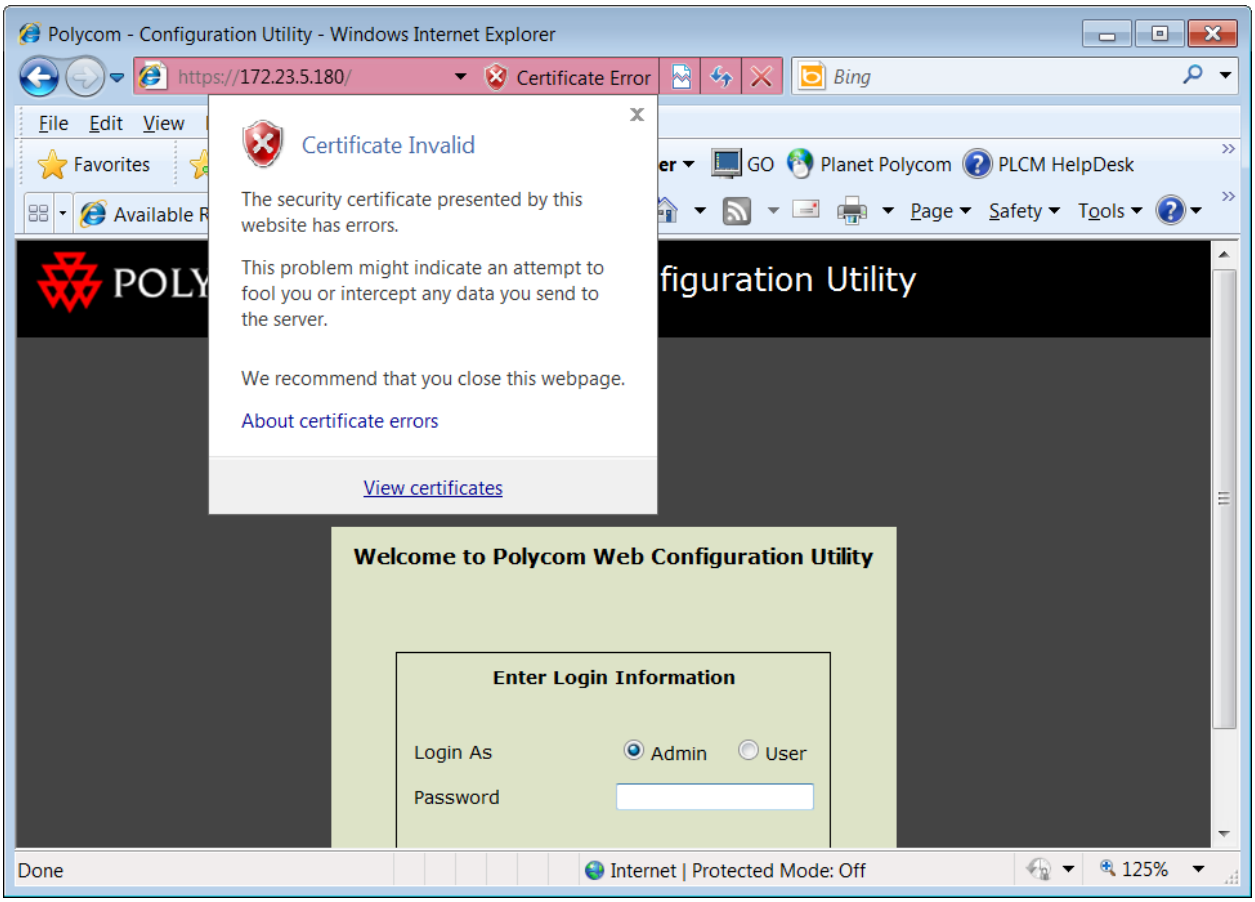
```
000005.948|tls  |3|03|Custom platform device certificate 1 common name
"Custom-0004F206075D"
000005.952|tls  |3|03|Custom platform device key 1 length 2374
000005.952|tls  |3|03|Custom platform device certificate 2 is not
available
```

Note: Log More Information About Certificates

To get more certificate information in the log file, set TLS logging to level 3 and then check the <*MAC Address*>-app.log after the phone reboots.

- **View certificate in a browser (when using the Web Configuration Utility).**

  The following figure shows what happens when you enter the phone's IP address into Internet Explorer and click on **View Certificates**.



To verify that the certificate you see is an original Polycom Factory certificate, it must be signed by a Polycom intermediate CA **and** have a matching issuer thumbprint. The issuer thumbprint is an MD5 or SHA1 digest unique to only that certificate. Finger prints for Polycom certificates can be found by viewing the certificates at http://pki.polycom.com/pki.

Determining Type of Device Certificates on Polycom Phones

You can determine if there is a device certificate on a Polycom phone through the phone's user interface.

To determine if there is a device certificate on a Polycom phone:

1. Press the **Menu** key, and then select **Status > Platform > Phone**.
2. Scroll down to the bottom of screen.

   One of four messages will be displayed:

   a. 'Device Certificate: Factory Installed' or 'Device Certificate: Installed' is displayed if the certificate is available in flash memory, all the certificate fields are valid and certificate has not expired.

   For a list of all certificate fields, see the latest *Administrators' Guide*.

Note: Device Certificate Shown as Self-Signed

Some Polycom phones manufactured since December 2011 will report the device certificate as 'self-signed' and not 'Factory Installed' in the phone's menu. This difference is due to the fact that a different Issuing CA was used to generate the certificates. The phones still operate correctly, providing the authenticating server trusts the Polycom Root CA that issued these certificates. The menu issue (77793) will be fixed in a future software release. Review release notes to determine whether it is addressed in the software you are using.

   b. 'Device Certificate: Not Installed' is displayed if the certificate is not available in flash memory or the flash memory location where the device certificate is to be stored is blank.

   c. 'Device Certificate: Self-signed' is displayed if the certificate is available in the phone's device settings, all the certificate fields are valid, the certificate has not expired, but it is not signed by a Polycom Certificate Authority.

   d. 'Device Certificate: Invalid' is displayed if the certificate is not valid.

Device Certificates on
Polycom® Phones

Device Certificate Implementation Date

The device certificates were installed at different times by phone model and revision. To find out which revision of phone model device certificates were installed, look for the revision letter on the console label on the back of the phone or on the shipping label of the product box.

The revision letter can be found on the console label on the rear of the phone or on the shipping label on the product boxes.

Console Label Revision and Date

The following is an example console label showing revision letter K.

The following table shows the revisions based on the console part number.

Platform	*Console Part Number*	*Revision*	*Date*
SoundPoint IP 321	2201-12360-001	B	May 2009
SoundPoint IP 331	2201-12365-001	B	May 2009
SoundPoint IP 335	2201-12375-001	D	October 2009
SoundPoint IP 450	2201-12450-001	J	July 2009
	2201-12450-002	C	July 2009
	2201-12450-207	C	July 2009
	2201-12451-001	F	July 2009
SoundPoint IP 550	2201-12550-001	L	December 2009
	2201-12550-002	G	December 2009
	2201-12551-001	K	December 2009
	2201-12552-001	J	December 2009
SoundPoint IP 560	2201-12560-001	J	December 2009

Device Certificates on

Polycom® Phones

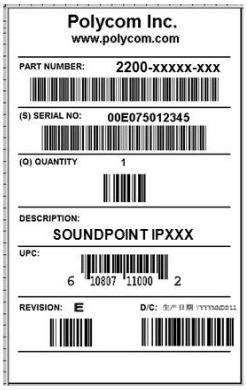
Platform	*Console Part Number*	*Revision*	*Date*
	2201-12561-001	C	December 2009
SoundPoint IP 650	2201-12630-001	K	July 2009
	2201-12630-107	E	July 2009
	2201-12651-001	F	July 2009
	2201-12652-001	F	July 2009
	2201-12660-001	E	July 2009
SoundPoint IP 670	2201-12670-001	J	December 2009
	2201-12671-001	D	December 2009
SoundStation IP 5000	2201-30900-001	B	March 2010
SoundStation IP 6000	2201-15600-001	M	January 2010
SoundStation IP 7000	2201-40000-001	H	January 2010
SoundStation Duo	2201-19000-001	A	September 2011
SpectraLink 8440	2201-36150-102	B	June 2011
	2201-36150-112	A	June 2011
SpectraLink 8450	2201-36153-202	B	June 2011
	2201-36153-212	B	June 2011
SpectraLink 8452	2201-36172-302	2	December 2011
	2201-36172-312	3	December 2011
VVX 500	2201-44500-001	B	December 2011
VVX 1500	2201-18061-001	F	January 2010
	2201-18063-001	F	May 2010
VVX 1500 C	2201-18062-001	D	February 2010
VVX 1500 D	2201-18064-001	B	January 2010

Device Certificates on

Polycom® Phones

Shipping Box Label Revision and Date

The following is an example shipping label showing the revision letter E.



The following table shows the revisions based on the shipping box part number.

Platform	*Box Part Number*	*Revision*	*Date*
SoundPoint IP 321	2200-12360-001	B	May 2009
	2200-12360-025	B	May 2009
SoundPoint IP 331	2200-12365-001	B	May 2009
	2200-12365-025	B	May 2009
SoundPoint IP 335	2200-12375-001	A	October 2009
	2200-12375-025	C	January 2010
SoundPoint IP 450	2200-12450-001	G	July 2009
	2200-12450-002	G	July 2009
	2200-12450-012	J	July 2009
	2200-12450-015	G	July 2009
	2200-12450-016	D	July 2009
	2200-12450-022	D	July 2009
	2200-12450-025	H	July 2009
	2200-12450-030	D	July 2009

Device Certificates on

Polycom® Phones

Platform	*Box Part Number*	*Revision*	*Date*
	2200-12450-122	G	July 2009
	2200-12450-207	C	July 2009
	2200-12451-001	C	July 2009
	2302-12450-012	F	July 2009
	2302-12450-025	D	July 2009
SoundPoint IP 550	2200-12550-001	N	December 2009
	2200-12550-002	N	December 2009
	2200-12550-012	P	December 2009
	2200-12550-015	N	December 2009
	2200-12550-016	M	December 2009
	2200-12550-022	N	December 2009
	2200-12550-025	N	December 2009
	2200-12550-030	H	December 2009
	2200-12550-122	N	December 2009
	2200-12551-001	J	December 2009
	2200-12553-212	F	December 2009
	2302-12550-012	R	December 2009
	2302-12550-025	H	December 2009
	2311-12550-025	J	December 2009
	2505-12550-025	L	December 2009
SoundPoint IP 560	2200-12560-001	P	December 2009
	2200-12560-002	J	December 2009
	2200-12560-012	J	December 2009
	2200-12560-015	J	December 2009

Device Certificates on

Polycom® Phones

Platform	*Box Part Number*	*Revision*	*Date*
	2200-12560-022	D	December 2009
	2200-12560-025	P	December 2009
	2200-12560-030	G	December 2009
	2200-12560-122	J	December 2009
	2200-12560-125	J	December 2009
	2302-12560-025	F	December 2009
	2505-12560-025	K	December 2009
SoundPoint IP 650	2200-12651-001	M	July 2009
	2200-12651-002	K	July 2009
	2200-12651-012	N	July 2009
	2200-12651-015	M	July 2009
	2200-12651-016	K	July 2009
	2200-12651-022	L	July 2009
	2200-12651-025	K	July 2009
	2200-12651-030	D	July 2009
	2200-12651-107	H	July 2009
	2200-12651-122	M	July 2009
	2200-12651-125	L	July 2009
	2308-12651-001	K	July 2009
	2308-12651-012	H	July 2009
	2308-12651-015	K	July 2009
	2308-12651-122	J	July 2009
	2302-12651-012	J	July 2009
	2302-12651-025	D	July 2009

Device Certificates on

Polycom® Phones

Platform	*Box Part Number*	*Revision*	*Date*
	2302-12651-025	G	July 2009
SoundPoint IP 670	2200-12670-001	K	December 2009
	2200-12670-002	J	December 2009
	2200-12670-012	K	December 2009
	2200-12670-015	J	December 2009
	2200-12670-016	G	December 2009
	2200-12670-022	J	December 2009
	2200-12670-025	K	December 2009
	2200-12670-030	E	December 2009
	2200-12670-122	J	December 2009
	2302-12670-025	E	December 2009
	2505-12670-025	H	December 2009
SoundStation IP 5000	2215-30940-001	B	March 2010
SoundStation IP 6000	2200-15600-001	J	January 2010
SoundStation IP 7000	2200-40000-001	K	January 2010
SoundStation Duo	2200-19000-001	A	September 2011
	2200-19000-002	A	October 2011
	2200-19000-015	A	October 2011
	2200-19000-022	A	February 2012
	2200-19000-102	A	October 2011
	2200-19000-107	A	October 2011
	2200-19000-114	A	November 2011
	2200-19000-119	A	October 2011
	2200-19000-120	A	October 2011

Device Certificates on

Polycom® Phones

Platform	*Box Part Number*	*Revision*	*Date*
	2200-10999-122	A	October 2011
SpectraLink 8440	2200-37149-001	B	June 2011
	2200-37159-001	B	June 2011
	2200-37174-001	D	June 2011
	2200-37175-101	D	June 2011
	2200-37175-702	A	June 2011
SpectraLink 8450	2200-37152-001	B	June 2011
	2200-37153-001	B	June 2011
	2200-37176-101	D	June 2011
	2200-37177-101	D	June 2011
	2200-37177-702	A	June 2011
SpectraLink 8452	2200-37172-001	3	December 2011
	2200-37173-001	3	December 2011
VVX 500	2200-44500-001	B	December 2011
	2200-44500-025	B	December 2011
VVX 1500	2200-18061-025	F	January 2010
	2302-18061-025	F	May 2010
VVX 1500 C	2200-18062-025	G	February 2010
VVX 1500 D	2200-18064-025	B	January 2010

Device Certificates on Polycom® Phones

Feature Profile 37148

Trademarks

Disclaimer

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

Limitation of Liability

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

Customer Feedback

We are constantly working to improve the quality of our documentation, and we would appreciate your feedback. Please send email to VoiceDocumentationFeedback@polycom.com.

POLYCOM® | Support

Visit support.polycom.com for software downloads, product document, product licenses, troubleshooting tips, service requests, and more.