Technical Bulletin 57352

Deploying and Configuring Polycom Phones in 802.1X Environments

This document provides system administrators with the procedures and reference information needed to successfully deploy and configure Polycom SIP phones in a secure 802.1X environment.

You can configure 802.1X authentication on all SoundPoint IP, SoundStation IP, VVX 1500, and SpectraLink 8440 Series phones installed with UC Software version 4.0.0 or later on an 802.1X-enabled network.

Introduction

The 802.1X authentication feature provides authentication services for higher security networks that use 802.1X as the authentication protocol. Polycom SIP phones support seven EAP protocols for 802.1X authentication as listed in the next section. You can configure the 802.1X authentication feature using a central provisioning server, the Polycom Web Configuration Utility, or the phone's keypad interface.

For a list of the acronyms used in this document, refer to Defined Acronyms.

Supported EAP Authentication Protocols

Polycom SIP phones support the authentication protocols listed next. Note that the SpectraLink 8400 Series phones support only the protocols indicated in **bold**.

- EAP-TLS
- **EAP-PEAPv0/MSCHAPv2**
- EAP-PEAPv0/GTC
- EAP-TTLS/EAP-MSCHAPv2
- EAP-TTLS/EAP-GTC
- **EAP-FAST**
- EAP-MD5

EAP Authentication Requirements

This section shows you how to authenticate Polycom phones in 802.1X environments using each of the supported EAP protocols. Each authentication protocol has a unique configuration. The parameters you need to configure are listed under each protocol.

EAP-TLS

- Device certificate
- Trusted pool of root/CA certificates
- Identity (user name)

EAP-PEAPv0/EAP-MSCHAPv2 or **EAP-PEAPv0/EAP-GTC**

- Trusted pool of root/CA certificates
- Identity (user name)
- Password

EAP-TTLS/EAP-MSCHAPv2 or **EAP-TTLS/EAP-GTC**

- Trusted pool of root/CA certificates
- Identity (user name)
- Password

EAP-MD5

- Identity (user name)
- Password

EAP-FAST

- Identity (user name)
- Password
- Optional PAC file, provisioned automatically through the network or manually using a PAC file password.

Note: Using EAP-FAST Authentication for the First Time

The first time you perform EAP-FAST dynamic PAC file provisioning (also known as in-band provisioning), the server will provision the phone with a PAC file and the 802.1X authentication will fail. This will be followed by a successful 802.1X authentication. In some cases, the network switch may impose a delay of about 60 seconds before initiating the 802.1X authentication following a failed authentication attempt.

Note: Using EAP-FAST Authentication with a Network Switch in MDA Mode

If you are using a network switch in MDA mode, be aware of the following:

- MDA does not enforce the order of device authentication; however, when using an MDA-enabled port, Polycom recommends authenticating your voice device before a data device.
- When a network switch detects a data or voice device on a port, the switch blocks the device's MAC address until authorization succeeds. If authorization fails, there will be a delay, depending on the network switch setup, before the phone can authenticate.

Configuring 802.1X Authentication

You can configure 802.1X authentication in the following three ways:

- Configuring 802.1X Using a Central Provisioning Server
- Configuring 802.1X Using the Polycom Web Configuration Utility
- Configuring 802.1X Using the Local Phone User Interface

Refer to *Configuring 802.1X Using a Central* Provisioning Server (discussed next) for detailed descriptions of the parameters that apply to all three methods. If you wish to set up more than 10 phones, Polycom recommends using a central provisioning server. If you are provisioning fewer than 10 phones, you can use the Web Configuration Utility or the phone's user interface to configure the parameters listed in *Configuring 802.1X Using a Central* Provisioning Server.

Configuring 802.1X Using a Central Provisioning Server

The following sections outline TLS profile configuration and 802.1X setup. Each EAP protocol requires a slightly different configuration:

- If you are using EAP-TLS, EAP-PEAP, or EAP-TTLS, see *Configuring Your TLS* Profile and then go to *Setting Up* .
- If you are using EAP-FAST or EAP-MD5, go directly to *Setting Up* .

Refer to *EAP Authentication Requirements* in this document for a list of the parameters that you will need to configure for each authentication protocol.

Configuring Your TLS Profile

Only EAP-TLS, EAP-PEAP, and EAP-TTLS require a TLS Profile. Configure either TLS Platform Profile 1 or TLS Platform Profile 2 for these authentication protocols.

Choose the parameters ending in *1* to configure TLS Platform Profile 1 (for example, device.sec.TLS.profile.caCertList1) or choose the parameters ending in *2* to configure TLS Platform Profile 2 (for example, device.sec.TLS.profile.caCertList2). You must then specify which Platform Profile

you have configured by setting the `device.sec.TLS.profile.profileSelection.dot1x` parameter shown in ***Table 1**: TLS Profile Configuration Parameters* to *TLS Platform Profile 1* or *TLS Platform Profile 2*.

You can locate the configuration parameters shown in **Table 1** in the **device.cfg** configuration file template located in the **Config** folder of your UC Software distribution. You can make a copy of **device.cfg** and edit the parameters directly or create a new configuration file containing only the parameters you wish to modify.

Table 1: TLS Profile Configuration Parameters

Parameter	*Values*
device.sec.TLS.profile.caCertList1 **device.sec.TLS.profile.caCertList2** Choose the CA certificate(s) to use for authentication: • The built-in default certificate • The built-in and Custom #1 certificates • The built-in and Custom #2 certificates • Any certificate (built in, Custom #1 or Custom #2) • Only the Custom #1 certificate • Only the Custom #2 certificate • Either the Custom #1 or Custom #2 certificate	**Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2**
device.sec.TLS.profile.cipherSuite1 **device.sec.TLS.profile.cipherSuite2** The cipher suite to use for the Platform Profile.	**string**
device.sec.TLS.profile.cipherSuiteDefault1 **device.sec.TLS.profile.cipherSuiteDefault2** If set to 1, the default cipher suite will be used. If set to 0, the custom cipher suite will be used.	**0 or 1**
device.sec.TLS.profile.customCaCert1 **device.sec.TLS.profile.customCaCert2** The custom certificate to use if `device.sec.TLS.profile.caCertList` is configured to use a custom certificate.	**string**
device.sec.TLS.profile.deviceCert1 **device.sec.TLS.profile.deviceCert2** Choose the device certificate(s) to use for authentication.	**Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2**
device.sec.TLS.profile.profileSelection.dot1x Choose the TLS Platform Profile that you have configured.	**PlatformProfile1, PlatformProfile2**

Once you have finished configuring your TLS Profile for EAP-TLS, EAP-PEAP, or EAP-TTLS, go to *Setting Up* .

Setting Up 802.1X

To configure the EAP-TLS, EAP-PEAP, and EAP-TTLS protocols, you must first configure your certificates by setting up a TLS Profile (see Configuring Your TLS *Profile)*. To set up 802.1X authentication, configure the parameters in ***Table 2**: 802.1X Setup Parameters*.

You can locate the following configuration parameters in the **device.cfg** configuration file template located in the **Config** folder of your UC Software distribution. You can make a copy of **device.cfg** and edit the parameters directly or create a new configuration file containing only the parameters you wish to modify.

Table 2: 802.1X Setup Parameters

Parameter	*Value*
device.net.dot1x.enable Enable 802.1X authentication.	**1**
device.net.dot1x.method	**0**, **1**, **2**, **3**, **4**, **5**, **6**, or **7**
Specify the 802.1X authentication method where the numbers 0 to 7 refer to the following protocols: **0**: None, **1**:EAP-TLS, **2**:EAP-PEAPv0-MSCHAPv2, **3**:EAP-PEAPv0-GTC, **4**:EAP-TTLS-MSCHAPv2, **5**:EAP-TTLS-GTC, **6**:EAP-FAST, **7**:EAP-MD5	
device.net.dot1x.identity The identity (user name) for authentication.	**string**
device.net.dot1x.password	**string**
The password for 802.1X authentication. This parameter is required for all methods except EAP-TLS.	
device.net.dot1x.anonid EAP-TTLS and EAP-FAST only. The anonymous identity (user name).	**string**
device.net.dot1x.eapFastInBandProv	**0** or **1**
EAP-FAST only, optional. Choose 1 to enable EAP In-Band Provisioning by server unauthenticated PAC provisioning using anonymous Diffie-Hellman key exchange. Choose 0 to disable EAP In-Band Provisioning. *Reserved for Future Use – Choose 2 to enable EAP In-band provisioning by server authenticated PAC provisioning using certificate based server authentication.*	

Parameter	*Value*
device.pacfile.data	**string**
EAP-FAST only, optional. The PAC file (base 64 encoded). To generate a base 64-encoded PAC file, generate the PAC file using your authentication server and then convert it to base 64. You can convert the file to base 64 using the following openssl commands: `$ openssl enc -base64 -in myfile -out myfile.b64`	
device.pacfile.password	**string**
EAP-FAST only, optional. The password for the PAC file.	

Applying the Configuration Files to your Phone

Once you have created a new configuration file or edited a copy of the **device.cfg** template configuration file using the parameters in ***Table 1*** and ***Table 2***, apply the files to your phone.

To apply the configuration files to your phone:

1. Connect your phone to a staging network (a network that is not 802.1X-enabled).
2. Apply the configuration files to the phone.

   For more information on applying configuration files to your phone, consult the *Polycom UC Software Administrator's Guide*, available from http://www.support.polycom.com/voice/.
3. Reboot the phone.

   Once the phone reboots, it will be ready to connect to the 802.1X-enabled network.
4. Connect the phone to the 802.1X-enabled network and reboot the phone.

   Verify that your phone is authenticated by making a phone call.

Troubleshooting: What if my Phone Doesn't Authenticate?

If your phone does not authenticate, navigate to the Configuration menu (**Menu** > **Status** > **Platform** > **Configuration**) and check for errors in your configuration files. If you see the message *Errors Found* instead of *Parameters Accepted* for one or more of the files, verify the parameters in the file.

Configuring 802.1X Using the Polycom Web Configuration Utility

You can configure the 802.1X authentication parameters using the Polycom Web Configuration Utility. This section shows you where to find the 802.1X settings on the Web Configuration Utility. Refer to

Configuring 802.1X Using a Central Provisioning Server for an interpretation of the configuration parameters.

To set up a TLS Profile:

1. Connect your phone to a staging network (a network that is not 802.1X-enabled).
2. Launch the Web Configuration Utility by navigating to http://*<phoneIPaddress>*.

   Log in using your administrator credentials.
3. Navigate to **Settings** > **Network** > **TLS**.
4. Expand the **Certificate Configuration** menu and install the required certificates.
5. Expand the **TLS Profiles** menu and configure either Platform Profile 1 or Platform Profile 2.
6. Expand the **TLS Applications** and choose the Platform Profile that you configured (either TLS Platform Profile 1 or TLS Platform Profile 2) from the drop-down list next to the **802.1X** label.
7. Click **Save** at the bottom of the page.

   Your phone will reboot or restart.

To enable 802.1X authentication:

1. Launch the Web Configuration Utility by navigating to http://*<phoneIPaddress>*.
2. Navigate to **Settings** > **Network** > **Ethernet**.
3. Expand the **Ethernet 802.1X** menu and configure the settings as described in ***Table 2****: 802.1X Setup Parameters*.
4. To configure EAP-FAST with a PAC file, expand **PAC File Info** and install the PAC file (base 64 encoded)

Configuring 802.1X Using the Local Phone User Interface

You can configure the 802.1X authentication parameters using your phone's user interface. This section shows you how to find the 802.1X settings using the phone menus. Refer to *Configuring 802.1X Using a Central* Provisioning Server for an interpretation of the configuration parameters.

To set up a TLS Profile:

1. Navigate to the **TLS Security** menu (**Menu** > **Advanced** > **Admin Settings** > **TLS Security**).
2. Select **Custom CA Certificates** to configure your CA Certificates, or select **Custom Device Credentials** to configure the Device Credentials.
3. From the **TLS Security** menu, select **Configure TLS Profiles** and choose either **TLS Platform Profile 1** or **TLS Platform Profile 2**.
4. Configure the profile as shown in ***Table 1****: TLS Profile Configuration Parameters*.

5 From the TLS Security menu, select **TLS Applications** > **802.1X**.

6 Select the TLS Platform Profile that you configured (either **TLS Platform Profile 1** or **TLS Platform Profile 2**).

7 Save the configuration.

The phone will reboot.

To enable 802.1X Authentication:

1 Navigate to the **Ethernet Menu** (**Menu** > **Advanced** > **Admin Settings** > **Network Settings** > **Ethernet Menu**).

2 Scroll down to **802.1X Auth** and select **Enabled**.

3 From the **Ethernet Menu**, select **802.1X Menu**.

See ***Table 2****: 802.1X Setup Parameters* for the list of parameters to configure. PAC file configuration for EAP-FAST can also be performed from the 802.1X Menu by selecting **PAC File Info**. The PAC file must be base 64 encoded.

Defined Acronyms

The following acronyms are used in this document:

- **EAP** Extensible Authentication Protocol
- **TLS** Transport Layer Security
- **PEAP** Protected Extensible Authentication Protocol
- **TTLS** Tunneled Transport Layer Security
- **FAST** Flexible Authentication via Secure Tunneling
- **MD5** Message-Digest Algorithm
- **MS-CHAPv2** Microsoft Challenge-Handshake Authentication Protocol (version 2)
- **GTC** Generic Token Card
- **IEEE** Institute of Electrical and Electronics Engineers
- **LAN** Local Area Network
- **WLAN** Wireless Local Area Network
- **EAPOL** EAP over LAN (Extensible Authentication Protocol over Local Area Network)
- **PAC** Protected Access Credential
- **MDA** Multi-Domain Authentication

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.