# Best Practices Guide:
# Mutual TLS Certificate Validation

## EA 196390 | 3725-87285-001A

This document applies to:

All Poly, Polycom, and Obihai desk phones, conference phones, DECT mobile handsets, and voice adapters (ATAs).

Poly devices are installed at the time of manufacture with a unique RSA certificate & key pair referred to hereafter as the "device certificate". Device certificates enable Poly and our partner services to authenticate the device holding the certificate is what it declares itself to be. Device certificates are commonly used in the following situations:

- **Mutual TLS Authentication**: Just as the phone will verify that the server is who it claims to be, device certificates allows a server to verify that a device is truly a Poly device and not a malicious endpoint or software masquerading as a Poly device. This could be used for tasks like file provisioning or SIP signaling using TLS.
- **Secure HTTP** (https): Secures HTTP access to the web server on the phone at https://<IP ADDRESS OF PHONE>
  The web server is often used for configuration and troubleshooting activities.
- **Securing API**: Secures API communications and partner integrations
- **Restricting access:** Restrict access to Poly cloud services such as ZTP, PDMS, or Lens

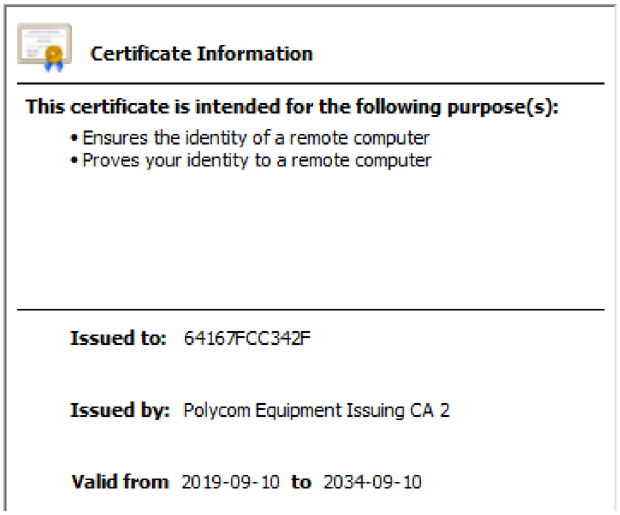
For more detail on the device certificates themselves, please refer to Feature Profile 37148: Device Certificates on Polycom Phones

# Contents

## Device Certificates – Authenticating a Poly Device

Poly devices can provide a certificate issued by the Polycom Root Certificate Authority. There are several components that should be checked by any service when authenticating a device based on this certificate:

1) **The Common Name (CN)** - also represented as the "Issued to" attribute. Poly devices will use their MAC address as the CN allowing a one-to-one mapping of certificate to device. This unique identifier is crucial to the security of any service as it will allow a means to restrict delivery of a file or service to any device requesting something for which its particular MAC is not entitled. Poly device certificates do not use Subject Alternative Name (SAN) fields to represent their MAC address.
2) **The Issuing Authority** - All Poly devices will be issued a device certificate by the Polycom Root Certificate Authority (CA). Much like any root CA, the Polycom Root CA has a public certificate that will require installation on any server providing service to Poly devices. By trusting this root, you are extending trust to all devices who have been issued certificates by that root.
3) **The Validity Period -** Poly devices will receive a certificate with a validity period of 15 years from the date of manufacture.



**Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

**Issued to:** 64167FCC342F

**Issued by:** Polycom Equipment Issuing CA 2

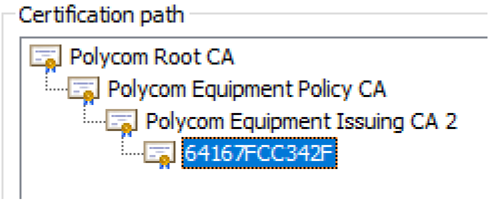
**Valid from** 2019-09-10 **to** 2034-09-10

*Figure 1 - Viewing a Poly device certificate*

## Polycom Root and Intermediate Certificates

The Polycom Root CA has created several intermediate root CA's who perform the role of creating and signing the certificates found on your Poly devices. When a Poly device provides its certificate, it will also provide the chain of intermediate CAs that issued its certificate so that your service may establish the complete chain of trust from device up to the root.

**You may download the Polycom Root and Intermediate CA certificates at:**
**http://pki.polycom.com/pki**



Certification path

- Polycom Root CA
  - Polycom Equipment Policy CA
    - Polycom Equipment Issuing CA 2
      - 64167FCC342F

*Figure 2 - The certificate chain of a Poly device*

## Certificate Revocation

In the event a device certificate or root certificate must be revoked, the Certificate Revocation List (CRL) will be published at http://crl.polycom.com/crl.

Poly devices support the Online Certificate Status Protocol (OCSP) and can check if a server certificate has been revoked.

| Parameter | Values | Default |
|---|---|---|
| `device.sec.TLS.OCSP.enabled` | 0 or 1 | 0 |
| When enabled, the OCSP retrieves information on whether the received server certificate is valid or revoked | | |

## Security Recommendations

### Guidelines Suitable for all Partner Services

Whereas private key infrastructure (PKI) allows the authentication of a device, it is recommended that more than one layer of authentication be considered beyond who holds a certificate.

1) **Trust Specific Devices**
   The most restrictive and therefore secure policy would be to know exactly which devices belong on your service and which do not. By creating an access control list (ACL) or allow list of MAC addresses, each requestor's certificate may be compared against that list and only when a match is achieved will the device be permitted to request files or services.
2) **Verify the files requested belong to the requestor**
   Poly devices are typically set up to request configuration files, and the primary means of uniquely identifying the correct file is to include the MAC address of the device it belongs to in the file name. When a request for a file is received, your service must check to see that the file requested truly belongs to the requestor by matching the MAC address in the filename to the MAC address provided as the Common Name in the requestor's certificate. This will prevent

exploitation of your services where simply presenting a Polycom issued certificate would otherwise allow access to any file hosted by your service.

3) **Use Multi-Factor Authentication**
   Requiring a username and password in addition to a valid certificate will greatly enhance the security of your service. Ideally the password is unique to each device but even a common username and password can provide an additional hurdle for attackers. See the section titled "Password Based Provisioning Recommendations" for more information.

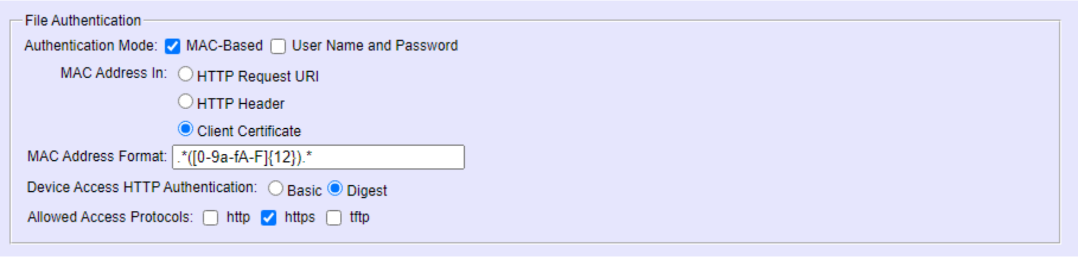
## For Cisco/Broadworks Environments

The Cisco BroadWorks DMS supports two types of file access control: username/password and MAC-based.

Prior to R22 & R21.sp1, should you choose the MAC-based file access, the requesting CPE's MAC address was pulled from the HTTP Request URI or from the HTTP headers without authentication. Because of the security shortcomings to this method, BroadWorks introduced an improved mutual TLS authentication in R22/R21.sp1 where the DMS extracts the requesting CPE's MAC address from the client certificate common name field (CN).

To enable secure MAC-based authentication BroadWorks:

1) Set Authentication Mode to "**MAC-Based**"
2) Select the "**Client Certificate**" as the source
3) Include the following regular expression as the MAC Address Format: `.*([0-9a-fA-F]{12}).*`



File Authentication

Authentication Mode: ☑ MAC-Based □ User Name and Password

MAC Address In: ○ HTTP Request URI<br>○ HTTP Header<br>● Client Certificate

MAC Address Format: .*([0-9a-fA-F]{12}).*

Device Access HTTP Authentication: ○ Basic ● Digest

Allowed Access Protocols: □ http ☑ https □ tftp

*Figure 3 – A completed MAC-Based File Authentication Page from the Broadworks Admin Portal*

For the feature and server configuration details, see the XSP Client Certificates Verification Enhancements feature description R21.0 supplied by Cisco.

Note: If upgrade to R22 or R21.sp1 or later is not possible and you cannot implement mutual TLS / MAC-based file authentication, then Cisco recommends using the username/password method rather than the less secure MAC-based authentication where the MAC address is taken from the HTTP Request URI or HTTP header.

## For Apache Based Provisioning Servers

Apache directives can make use of variables to compare the common name from a Poly device certificate against the requested URL. Provided that all your configuration files contain the MAC address of a phone, or that you enable this check only for select files, you can effectively block queries made by devices or malicious users requesting files that do not belong to the requesting device.

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
ServerName example.com
DocumentRoot /var/www/html
#- Verify the client CN against the request URI.
#- Allow only if the SSL_CLIENT_S_DN_CN (mac address) is a part of the request URI
<Directory "/var/www/html/polycom/configuration/ ">
        <If "%{REQUEST_URI} -strcmatch \"*%{SSL_CLIENT_S_DN_CN}*\"">
                Require all granted
        </If>
        <Else>
                Require all denied
        </Else>
</Directory>
```

## Password Based Provisioning Recommendations

When using a username and password to protect provisioning server access, the first issue encountered is how to safely install that username and password on the device. Ideally a unique username and password is used however that presents logistical issues that are more difficult to resolve and so use of a common password may still be favorable and may be achieved using any of the following methods:

1) **At the Distributor**
   Many partners already contract a distributor for out of box setup and configuration. Passwords set up at this stage need never be shared with end users, however the primary negative to this method is that any device that is factory reset will lose the password and require a device RMA by the distributor.
2) **Poly's Zero Touch Services**
   Poly provides both the ZTP and the PDMS zero touch service. Both of these services are well suited to installing a password before the device ever reaches your service. Any device that is factory reset will also always return to the Poly service so RMAs would not be required.
3) **One-time Password Generation Portal**
   For partners not using either of the above services, any device that is factory reset or part of a BYOD offering requires the end user to enter the provisioning server address for your service. A partner developed web portal that users must first log into could accept as input the MAC address of a device and output a one-time password the user may enter into their phone at the same time they enter your provisioning server address.
   Once the device reaches your service using the one-time password, you may serve only a small configuration file that installs the primary common password and common provisioning address

prompting the phone to retry its provisioning requests. Now, since it is using the common password, the true file set will be delivered enabling the phone to register for regular service.

4) **Use Strong Passwords and Change Them Often**
Poly recommends enabling your devices to periodically poll your server for configuration updates, even if it is performed only on a weekly basis. By creating two or more passwords that grant access to provisioning files, a new password can be inserted into configuration templates on a regular basis and wait for devices to pick up the changes before later retiring older passwords. This rotating window should be long enough that devices may be powered off for a reasonable period of time without missing the window since if they do miss the update, you will require an onboarding service to enable them access again, such as described in items 1 through 3 above.

## Poly Security Center

Information security is a top priority for Poly across all products and services. Security bulletins and advisories may be accessed from our security center at https://support.polycom.com/content/support/security-center.html