

# Polycom Provisioning Server

**Note:** This guide assumes the Polycom VVX phones have 5.x firmware installed out of the box and a Windows based DHCP server. If not please refer to **Appendix I** to upgrade the phones to a 5.x firmware or **Appendix II** for options on Cisco based DHCP servers.

Polycom VVX phones support FTP, TFTP, HTTP, or HTTPS. Out of the box the phones are configured for FTP, but the protocol configuration may be passed via DHCP option.

## 1 TABLE OF CONTENTS

---

2	FTP Server .....	1
2.1	Files & Folders .....	2
2.2	Firewall .....	2
3	HTTPS Server .....	2
3.1	IIS Configuration .....	2
3.2	Files & Folders .....	4
3.3	Firewall .....	5
4	DHCP Server .....	5
5	Skype for Business Server Device Updates .....	6
6	Appendix I – Firmware upgrade from releases prior to 5.x .....	6
7	Appendix II – DHCP Options 43 and 120 for Cisco based DHCP servers .....	6

## 2 FTP SERVER

---

Any FTP server can serve as the provisioning server, but be aware of FTP servers with strict password policies (eg. IIS FTP) as the default user password will not meet complexity requirements. Different credentials require manual configuration, passing the credentials via DHCP, or a multi-step provisioning process where the credentials are passed via an initial configuration file.

**Note:** Polycom does not recommend placing your provisioning server on any Skype for Business servers.

The phones are preconfigured to use the user credentials below to connect to the FTP server. To zero touch provision the phones this user must be configured on your FTP server with the listed permissions.

- Username: PlcmSplp
- Password: PlcmSplp

### Permissions

- Read
- Write

- Modify (including delete and append)

## 2.1 FILES & FOLDERS

Create the following folders (case sensitive):

- calls
- logs
- overrides
- core
- contacts

Place the following included files in the PlcmSplp user home directory:

- 000000000000.cfg – Contains instructions for phones to use the calls and logs folders to store call and debug logs to.
- master.cfg – Configures the phone for Skype for Business profile, DSCP values for QoS, update parameters for device updates from the Skype for Business server and various other parameters.

## 2.2 FIREWALL

If Windows firewall is enabled, create a rule for FTP port TCP/21.

**PowerShell:**

```
New-NetFirewallRule -DisplayName "Provisioning Server (FTP)" -Direction Inbound -Action Allow -Profile Any -Protocol TCP -LocalPort 21
```

# 3 HTTPS SERVER

---

While potentially any web server may be used, this guide discusses configuration of Microsoft IIS for use as the provisioning server. HTTPS requires a certificate is issued to the provisioning server and that the Polycom phones trust the issuer of that certificate. If the certificate is issued from a CA not trusted by the VVX, such as from an enterprise CA, then the root certificate must first be provisioned manually or via HTTP.

There are two options for authentication, digest authentication or certificate authentication (MTLS). Each phone comes with a factory installed device certificate signed by the Polycom PKI that can be used for certificate authentication. Digest authentication requires manual configuration, passing the credentials via DHCP, or a multi-step provisioning process where the credentials are passed via an initial configuration file.

## 3.1 IIS CONFIGURATION

**Prerequisites**

- SSL certificate for provisioning server
- Service account for digest authentication or certificate authentication mapping

### 1. Install IIS Windows Roles and Features

**Certificate authentication (MTLS)**

```
Install-WindowsFeature Web-Server,Web-WebServer,Web-Common-Http,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,Web-Static-Content,Web-DAV-Publishing,Web-Health,Web-Http-Logging,Web-Performance,Web-Stat-Compression,Web-Security,Web-Filtering,Web-Cert-Auth,Web-Mgmt-Tools,Web-Mgmt-Console
```

## Digest Authentication

Install-WindowsFeature Web-Server,Web-WebServer,Web-Common-Http,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,Web-Static-Content,Web-DAV-Publishing,Web-Health,Web-Http-Logging,Web-Performance,Web-Stat-Compression,Web-Security,Web-Filtering,Web-Digest-Auth,Web-Mgmt-Tools,Web-Mgmt-Console

2. Issue SSL certificate with the provisioning server FQDN or friendly URL (eg. polycomprov.domain.com).
3. Import certificate and chain into the provisioning server.
4. Create the HTTPS root directory (eg. c:\inetpub\wwwhttps).
  - a. Add NTFS permissions granting service account Read & Execute, List Folder Contents, Read, and Write.
5. Use IIS Manager to create a HTTPS web site (example name: HTTPS Web Site).
  - a. Set the physical path to the HTTPS root directory.
  - b. Click Connect As... to configure the service account.
  - c. Select the SSL certificate that was provisioned.
6. Enable WebDAV under HTTPS web site.
7. Create WebDAV Authoring Rule for All content to the service account user with Read and Write permissions.
8. Add MIME types for .cfg, .log, and .ld as 'text/plain'.
9. Deploy configuration files to folder structure.
10. Update provisioning server URLs in 000000000000.cfg and initial.cfg files.
11. Update provisioning server certificate root CA in initial.cfg file.

## Certificate Authentication

1. Import the Polycom Root CA into the provisioning server from <http://pki.polycom.com/pki>.
2. Enable anonymous authentication under the HTTP site.
3. Disable all authentication methods under the HTTPS site.

4. Use PS on the HTTPS site to modify the client certificate authentication mappings. Update the variables at the top to reflect the HTTPS site name, username, and password.

```
$HttpsSiteName = "HTTPS Web Site"
$Username = "domain\username"
$Password = "Password1"

Set-WebConfigurationProperty -Filter
"/system.webServer/security/authentication/iisClientCertificateMappingAuthentication" `
    -Name Enabled `
    -Value True `
    -PSPath "IIS:\" `
    -Location $HttpsSiteName

Set-WebConfigurationProperty -Filter
"/system.webServer/security/authentication/iisClientCertificateMappingAuthentication" `
    -Name manyToOneCertificateMappingsEnabled `
    -Value True `
    -PSPath "IIS:\" `
    -Location $HttpsSiteName

Set-WebConfigurationProperty -Filter
"system.webServer/security/authentication/iisClientCertificateMappingAuthentication" `
    -Name oneToOneCertificateMappingsEnabled `
    -Value False `
    -PSPath "IIS:\" `
    -Location $HttpsSiteName

$certMapping = @{
    name      = "Polycom User"
    description = "Polycom service account for access to folder structure"
    userName  = $Username
    password  = $Password
}

Add-WebConfiguration -Filter
"/system.webServer/security/authentication/iisClientCertificateMappingAuthentication/manyToOneMa
ppings" `
    -Value $certMapping `
    -PSPath "IIS:\" `
    -Location $HttpsSiteName
```

5. Under SSL Settings check Require SSL and set Client certificates to Require.

### Digest Authentication

1. Enable Digest Authentication on HTTP and HTTPS web sites.

## 3.2 FILES & FOLDERS

Create the following folders in the HTTPS site root or site-specific directory:

- calls
- logs
- overrides
- core
- contacts

Place the following included files in the HTTP site root (eg. c:\inetpub\wwwroot) or site-specific (eg. c:\inetpub\wwwroot\site1) directory:

- 000000000000.cfg – Contains instructions for phones to use the calls and logs folders to store call and debug logs to.
- initial.cfg – Configures provisioning server and root certificate to trust the provisioning server.

Place the following included files in the HTTPS site root or site-specific directory:

- 000000000000.cfg – Contains instructions for phones to use the calls and logs folders to store call and debug logs to.
- master.cfg – Configures the phone for Skype for Business profile, DSCP values for QoS, update parameters for device updates from the Skype for Business server and various other parameters.

### 3.3 FIREWALL

If Windows firewall is enabled, create rules for HTTP and HTTPS ports TCP/80 and 443.

#### PowerShell:

```
New-NetFirewallRule -DisplayName "Provisioning Server (HTTP)" -Direction Inbound -Action Allow -Profile Any -Protocol TCP -LocalPort 80
```

```
New-NetFirewallRule -DisplayName "Provisioning Server (HTTPS)" -Direction Inbound -Action Allow -Profile Any -Protocol TCP -LocalPort 443
```

## 4 DHCP SERVER

DHCP options configure phones for accurate time for TLS negotiation, the FTP server to retrieve its config, the Skype for Business registrar pool, and the certificate provisioning URL. These options should be configured on each scope (IP subnet) that the IP phones will be deployed.

Class	Option	Data Type	Description	Value
Standard	2	Hex	Time zone offset	<b>See:</b> <a href="http://bit.ly/CiscoTimeOffset">http://bit.ly/CiscoTimeOffset</a> When using a Microsoft DHCP server do not include the period in the values found in the link provided. Doing so will result in everything after the period being dropped and the value translating to UTC.
Standard	42	IP Address	Time server	Time Server IP Address
MSUCClient	43	Hex	Cert provisioning URL	<b>See:</b> <a href="http://bit.ly/MSDHCPOptions">http://bit.ly/MSDHCPOptions</a> Use DHCPUtil using the SipServer and WebServer parameters to populate options 43 and 120.
Standard	120	Hex	SIP server	See above.
Standard	161	String	Polycom provisioning server	FTP: <a href="ftp://provsrv.domain.local">ftp://provsrv.domain.local</a> HTTPS: <a href="https://provsrv.domain.local">https://provsrv.domain.local</a> <b>Note:</b> Lync/SfB SKU devices (PN ending in -018 or -019) default to option 161. Open SIP SKU devices default to option 160.
CPEOCPhone	10	Word	<b>(Optional)</b> VLAN ID – Use if LLDP is not available	VLANID (as decimal value) <b>Note:</b> This class can be added programmatically to the DHCP server with the commands below: netsh dhcp server add class CPEOCPhone "VLAN tagging for the Microsoft Phone Devices" "CPE-OCPHONE" 1

				netsh dhcp server add optiondef 10 VoiceVLAN Word 0 Vendor=CPEOCPhone comment="Phone VLAN" netsh dhcp server set optionvalue 10 Word vendor=CPEOCPhone "%1"
--	--	--	--	--

## 5 SKYPE FOR BUSINESS SERVER DEVICE UPDATES

1. Download the latest 5.x Skype for Business Server CAB firmware package from <http://support.polycom.com>.  
» Polycom CAB file for UC Software 5.0.1 Rev P for upgrades from Lync server
2. Extract the .cab files and upload the relevant packages to the Skype for Business device update service.

## 6 APPENDIX I – FIRMWARE UPGRADE FROM RELEASES PRIOR TO 5.X

1. Download the latest 5.x “combined” firmware from <http://support.polycom.com>.  
» Polycom UC software 5.0.1 Rev P for VVX Business Media Phones and Polycom SoundStructure [combined]  
» Polycom UC Software 5.0.1 Rev P for VVX Business Media Phones and Polycom SoundStructure [split]
2. Extract sip.ld and sip.ver and place into the PlcmSplp user home directory on the provisioning FTP server.
3. Open 000000000000.cfg and set the APPLICATION APP\_FILE\_PATH to “sip.ld”.
4. Once all 4.x release phones have been updated to a 5.x, set the APPLICATION APP\_FILE\_PATH back to “”. If this is not done phones will loop between the firmware on the provisioning server and Skype for Business Server. Additional 4.x release phones should be manually upgraded to a 5.x release. Large quantities of 4.x release phones should be upgraded using a staging environment.

## 7 APPENDIX II – DHCP OPTIONS 43 AND 120 FOR CISCO BASED DHCP SERVERS

The DHCPConfigScript.bat only works for Windows based DHCP server. However, the output from DHCPUtil.exe may be used to populate options for Cisco based DHCP servers.

The full hex values must be entered in each option and additional parameters may be required to accommodate the length of those values. The highlighted values in the example output below are what is needed from DHCPUtil.

If your Cisco platform supports the *option ext* command use that to avoid the values from being truncated. If it does not support *ext* ensure that the full value appears in the running config after entering the command.

```
PS C:\Program Files\Common Files\Skype for Business Server 2015> .\DHCPUtil.exe -SipServer sfbpool.domain.com -WebServer csweb-int.domain.com
```

```
SIP Server FQDN : sfbpool.domain.com
```

```
Certificate Provisioning Service URL : https://csweb-int.domain.com:443/CertProv/CertProvisioningService.svc
```

Option 120:

```
0007736662706F6F6C06646F6D61696E03636F6D00
```

Vendor Class Identifier: MS-UC-Client

Option 43 (for vendor=MS-UC-Client):

Full Option 43 value (Length: 174) :

010C4D532D55432D436C69656E7402056874747073031463737765622D696E742E646F6D61696E2E636F6D040334343305252F4365727450726F762F4365727450726F766973696F6E696E67536572766963652E737663

sub-option 1 <UC Identifier>: 4D532D55432D436C69656E74

sub-option 2 <URL Scheme>: 6874747073

sub-option 3 <Web Server FQDN>: 63737765622D696E742E646F6D61696E2E636F6D

sub-option 4 <Port>: 343433

sub-option 5 <Relative Path for Cert Prov>: 2F4365727450726F762F4365727450726F766973696F6E696E67536572766963652E737663

To configure DHCP Server with appropriate values, you can do one of the following things:

1. Run DHCPUtil on the DHCP Server: use '-RunConfigScript' switch
2. Run the following command on the DHCP Server (modify the path of DHCPConfigScript.bat appropriately):

"C:\Program Files\Common Files\Skype for Business Server 2015\DHCPConfigScript.bat" Configure MS-UC-Client 0007736662706

F6F6C06646F6D61696E03636F6D00 4D532D55432D436C69656E74 6874747073 63737765622D696E742E646F6D61696E2E636F6D 343433 2F4365727450726F762F4365727450726F766973696F6E696E67536572766963652E737663