

SCOPSERV
INTERNATIONAL INC.

ScopTEL Certificate Manager

Certificate Pre-Requisites

Self Signed Certificates are generally not supported by phone Manufacturer's therefore it is recommended you check with your phone hardware vendor to see which Certificate Authorities are supported.

You will first have to use the ScopTEL Certificate Manager to create your own Certificate Signing Request in order to purchase a Signed Certificate from a supported Certificate Authority

Most Certificate Authorities will provide you with a Root Certificate and a Chained Certificate (Chained Certificates are not mandatory but are very commonplace).

Once you have the Root CA, Certificate Chain, and a Signed Certificate from a supported Certificate Authority you can use the ScopTEL Certificate Manager to create Certificates for the following purposes:

1. Encrypting GUI communications using SSL (HTTPS)
2. Encrypting Phone Provisioning files during phone download using SSL (HTTPS)
3. Encrypting SIP signalling with SSL (TLS)
4. Encrypting SIP audio streams with SSL (SRTP)



Creating the CSR – Certificate Manager - Click on Add a New CSR

Fill in all the required fields

If you are purchasing a Wildcard Certificate put a *. In front of your domain name in the Common Name Field

Example: *.yourdomain.com

When done click on the Key Settings Tab

The screenshot displays the 'Certificate Manager' interface. At the top, there are three tabs: 'Root CA', 'Certificates', and 'Requests (CSR)'. The 'Requests (CSR)' tab is selected. Below this, there is a section titled 'Add a new Request (CSR)'. Inside this section, there are two sub-tabs: 'General' and 'Key Settings'. The 'General' tab is currently active. The form contains several fields, some of which are marked with a red asterisk (*) to indicate they are required. The fields and their values are as follows:

- * Certificate Request Name: csr2016
- * Common Name: sip.yourdomain.com (with a note: Example: your name or your server's hostname)
- * Organization: Your Organization
- Organizational Unit: (empty)
- * Locality (city): Your City
- * State (full name): Your State
- * Country: CA (with a note: 2 letter code)
- Email: youremailaddress@yourdomain.com
- Comment: (empty text area)

At the bottom of the form, there are two buttons: 'Add' and 'Cancel'. Below the form, there is a legend bar with the following information:

- Legend: * Required Field
- Page Refresh on Change (with a refresh icon)

Creating the CSR – Certificate Manager – Key Settings

Select a Digest Algorithm supported by your IP phone's manufacturer

It is recommended to choose a Key Size of at least 2048 bits

Passphrase is not required

Click Add when done

Add a new Request (CSR)

General

Key Settings

Digest Algorithm:

SHA-1

Default: MD5

Key Size:

2048 bits

Default: 1024 bits

Passphrase:

Add

Cancel

Legend:

* Required Field

Page Refresh on Change


Creating the CSR – Certificate Manager – Download your CSR

Certificate Manager

Root CA Certificates Requests (CSR)

Certificate Signing Requests: [1 to 1 of 1] [Add a new Request \(CSR\)](#)

Search:

Name	Common Name	Organization	City	State	Country	Action
csr2016	sip.yourdomain.com	Your Organization	Your City	Your State	CA	 

Action:

Columns to display:

Creating the CSR – Certificate Manager – Download your CSR

Copy and Paste your Certificate Request to your Certificate Authority when you purchase your CA for Domain Validation.

Wait for your CA to send you your Certificate
before generating your Certificate

You will copy and paste the Private Key Data into your Server Authentication Certificate in a later step

Certificate Signing Request Data	
Certificate Data	Click here to Download
<pre>-----BEGIN CERTIFICATE REQUEST----- MIIDATCCAekCAQAwgZ8xCzAJBgNVBAYTAkNBMRMwEQYDVQQIEwpZb3VyIFN0YXRl MRlwEAYDVQQHEwZib3VyIENpdHkxGjAYBgNVBAoTEVlvdXIgT3JnYW5pemF0aW9u MRswGQYDVQQDElzaXAueW91cmRvbWFPbi5jb20xLjAsBgkqhkiG9w0BCQEWH3Iv dXJlbWFPbGFkZHIjI3NAeW91cmRvbWFPbi5jb20wggEiMA0GCSqGSIb3DQEBAQUA A4IBDwAwqqEKAoIBAQCq6h0/mKBvF/53Z8htvyEf4IvIm5/ZEKeEoWkiDE/sPnE</pre>	
Private Key Data	Click here to Download
<pre>-----BEGIN RSA PRIVATE KEY----- MIIEowIBAAKCAQEA3KuodP5igb3/+d2fIbcshH+CL5Zuf2RCnhKfPlwxP7D5xFKR y1k61bVXx2z3t0RRGd7yNve4gT1s0ypoS8z7CSyEgLA3hA4sNPO7IIhC4pdFESW2 YE/Ls7zeEPW+74wrnynH04n4HB46zTxQqDOhfmoN0weFgzYjVJlKigAtL5Txk6D U83Uo6Ei04hT1Y7dh4HzhLD06DI+hsQLCLOMEN4WaaOv73CpISnAKVufPI/LCU55 fiSNxYj977jImatarWoQbKiPEkI+zjD+XLxZKxTT95NI9rukE13/pQMvI9IPAK</pre>	
PEM (Privacy Enhanced Mail) Data	Click here to Download
<pre>-----BEGIN CERTIFICATE REQUEST----- MIIDATCCAekCAQAwgZ8xCzAJBgNVBAYTAkNBMRMwEQYDVQQIEwpZb3VyIFN0YXRl MRlwEAYDVQQHEwZib3VyIENpdHkxGjAYBgNVBAoTEVlvdXIgT3JnYW5pemF0aW9u MRswGQYDVQQDElzaXAueW91cmRvbWFPbi5jb20xLjAsBgkqhkiG9w0BCQEWH3Iv dXJlbWFPbGFkZHIjI3NAeW91cmRvbWFPbi5jb20wggEiMA0GCSqGSIb3DQEBAQUA A4IBDwAwqqEKAoIBAQCq6h0/mKBvF/53Z8htvyEf4IvIm5/ZEKeEoWkiDE/sPnE</pre>	



Creating the CSR – Certificate Manager – Import a Certificate (Root CA)

Copy and Paste your CA's Root CA into the text box and click Add

Certificate Manager

Root CA

Certificates

Requests (CSR)

Add a new Root CA

General

* Certificate Authority Name:

yourcarootca

Import a Certificate (Root CA) ?

☒

* Certificate (Root CA):

-----BEGIN CERTIFICATE-----
MIIDFTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA
IAVT
MRAwDgYDVQQKEwdFcXVpZmF4MS0wKwYDVQQLEyRfcXVpZmF4IFNIY3VyZ
SBDZXJ0
aWZpY2F0ZSBBDXRRob3JpdHkwHhcNMDIwNTIxMDQwMDAwWhcNMjgwODI
xMDQwMDAw
WjBCMQswCQYDVQQGEwJVUzEWMBQA1UEChMNR2VvVHJlcnQgSW5jaEJl
MBkGA1UE

Add

Cancel



Creating the CSR – Certificate Manager – Add a new Certificate

Give your Certificate a name

Select Import Certificate & Key = Signed Certificate

Then click on the Certificate & Key tab

The screenshot shows the 'Certificate Manager' web interface. At the top, there are three tabs: 'Root CA', 'Certificates', and 'Requests (CSR)'. Below these is a section titled 'Add a new Certificate'. Inside this section, there are two sub-tabs: 'General' and 'Certificate & Key'. The 'Certificate & Key' tab is selected. The form contains the following fields:

- * Certificate Name:** A text input field containing 'yourcertname'.
- Import a Certificate & Key?** A dropdown menu with a green icon, currently set to 'Signed Certificate'. Below it, the text 'Default: No' is displayed.
- Comment:** A large text area for entering a comment.

At the bottom of the form, there are two buttons: 'Add' and 'Cancel'.

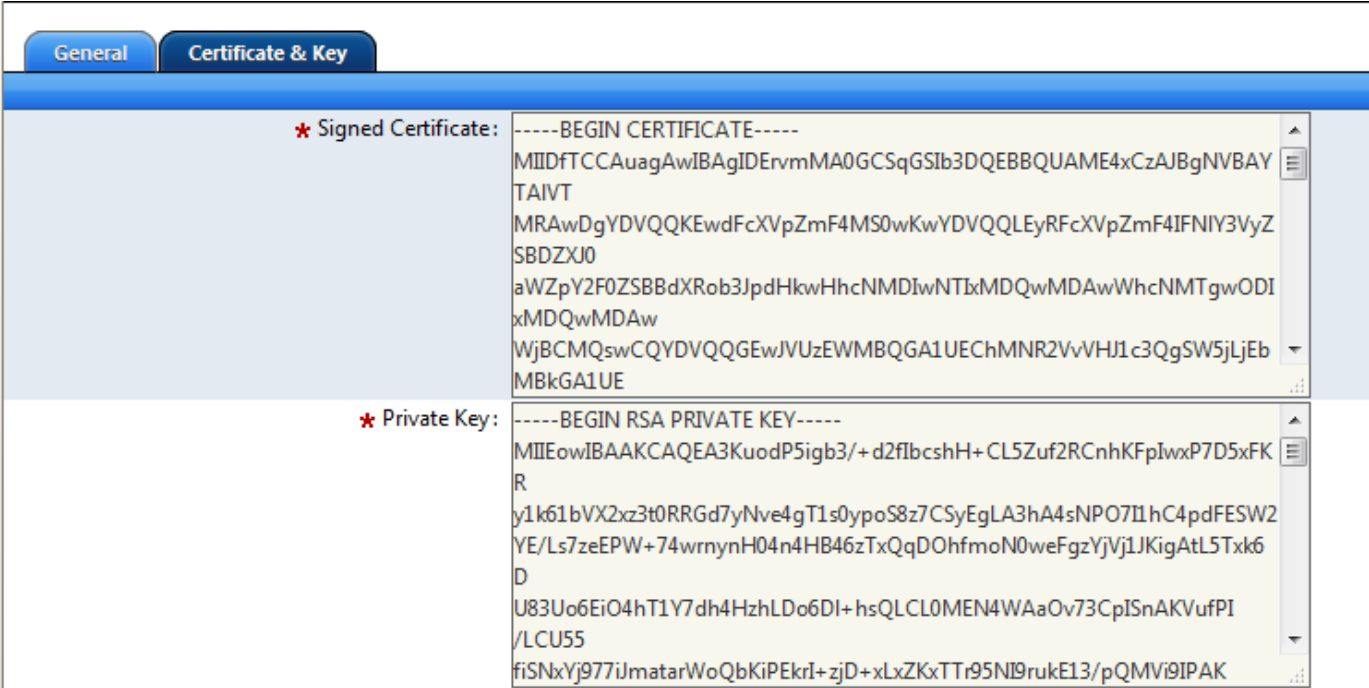


Creating the CSR – Certificate Manager – Add a new Certificate

Copy and Paste your CA's Signed Certificate data into the Signed Certificate text box

Copy and Paste your CSR's Private Key data into the Private Key text box

Click Add



The screenshot shows a web interface with two tabs: 'General' and 'Certificate & Key'. The 'Certificate & Key' tab is active. It contains two text input fields. The first field, labeled '* Signed Certificate:', contains a long string of text starting with '-----BEGIN CERTIFICATE-----' and ending with '-----'. The second field, labeled '* Private Key:', contains a long string of text starting with '-----BEGIN RSA PRIVATE KEY-----' and ending with '-----'. Both fields have a vertical scrollbar on the right side.

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYT
AIVT
MRAwDgYDVQQKEwdFcXVpZmF4MS0wKwYDVQQLEyRfcXVpZmF4IFNlY3VyZ
SBDZXJ0
aWZpY2F0ZSBBdXR0b3JpdHkwHhcNMMDIwNTIxMDQwMDAwWhcNMTgwODI
xMDQwMDAw
WjBCMqswCQYDVQQGEwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjEjEjE
MBkGA1UE
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA3KuodP5igb3/+d2f1bcshH+CL5Zuf2RCnhKFpIwxP7D5xFK
R
y1k61bVX2xz3t0RRGd7yNve4gT1s0ypoS8z7CSyEgLA3hA4sNPO7I1hC4pdFESW2
YE/Ls7zeEPW+74wrnynH04n4HB46zTxQqDOhfmoN0weFgzYjVj1JKigAtL5Txk6
D
U83Uo6EiO4hT1Y7dh4HzhLDo6DI+hsQLCL0MEN4WAaOv73CpISnAKVufPI
/LCU55
fiSNxYj977iJmatarWoQbKiPEkrl+zjD+xLxZKxTT95NI9rukE13/pQMVi9IPAK
-----
```

Creating the CSR – Certificate Manager – Add a new Certificate – Certificate Chain

Certificate Type = Intermediate and Chain Certificate

Certificate Name: Enter a name in the text field

Click on the Certificate tab

Copy and Paste the Certificate Chain data you received from your CA when they issued your Certificate

Click Add

Congratulations you have configured your Certificates

Certificate Manager

Root CA | **Certificates** | Requests (CSR)

Add a new Certificate

General | **Certificate**

* Certificate: -----BEGIN CERTIFICATE-----
U0hBMjU2IENBIC0gRzRwMwggEiMA0GCSqGSIb3DQEBAQUAA4IDRwAwggEKA
oIBARAR
VJvZWFOeLFbG1eh/9HDAG
//Qi1rkjqfdVC7UBMBdmJyNkA+8EGVf2prWRHzAn723
SowLBkMEu/SW4ib2YQGRZjEiwzQ0Xz8/kS9EX9zHFLYDn4ZLDqP
/oIACg8PTH2IS
1p1kD8mD5xvEcKyU58Okaiy9uJ5p2L4KjxZjWmhxgHsw3hUEv8zTvz5IBVV6s9cQ
DAP8m/0Ip4yM26eO8R5j3LMBL3+vV8M8SKeDaCGnL+enP
/C1DPz1hNFTvA5yT2PM
qwVkdBF9qn1luMrMTjAdBgNVHQ4EFgQUw5zz/NNGCDS7zkZ
/oHxb8+Ily1kwEgYD
VR0TAQH/BAgwBOOG
/wIBADAOBgNVHQ8BAf8EBAMCAQYwNQYDVROfBC4wLDAqoDAG
JoYkaHR0cDovL2cuc3ltY2lY29tL2NybmVzZ3RnbG9iYWw3Y3JsMC4GCCsGA
QUF
BwEBBCIwIDAeBggrBgEFBQcwAYYSaHR0cDovL2cuc3ltY2lY29tMEwGA1UdI
ARF
MEMwQYKYIZIAYb4RQEHnjAzMDEGCCsGAQUFBwIBFiVodHRwOi8vd3d3Lm
dlb3Ry
dXN0LmNvbS9rZXNvdXJjZXNvY3BzMA0GCSqGSIb3DQEBCwUAA4IBAQCjWB7

Add Cancel

Configuring the Server to Enable SSL (GUI)

Go to Server>Configuration and click on the Security (SSL) Tab

Enable SSL (GUI)?

For the Private Key select your Certificate

For the Certificate select the same Certificate

Highlight the Certificate Chain you create d earlier

Click Save

The Web server will restart once you click save and you will have to login to your server replacing <http://yourserver.com> with <https://yourserver.com>

Congratulations you have enabled TLS encryption on the ScopTEL Management GUI

The screenshot displays the 'Server Configuration' window with the 'Configuration' tab selected. Under the 'Configuration' section, the 'Security (SSL)' tab is active. The 'Enable SSL (GUI)?' checkbox is checked. Below this, the 'Private Key' and 'Certificate' dropdown menus are both set to 'yourcertname'. The 'Certificate Chain' dropdown menu is set to 'yourcachain'. A note at the bottom states: 'To select multiple items, hold down the Control (PC) or Command (Mac) key while clicking.' At the bottom of the window are 'Save' and 'Cancel' buttons.

Configuring the Server to use HTTPS Provisioning for your IP Phones

Go to Server>Configuration and click on the Provisioning Tab

From the HTTPS Provisioning Menu change the HTTP Protocol to HTTPS

Enter the LAN or WAN address specific to your server in each field (the screen shot only displays examples)

Click Save

The Web server will restart

Congratulations you have enabled SSL encryption for the Automatic Provisioning System

The screenshot displays the 'Server Configuration' interface with the 'Configuration' tab selected. Under the 'Configuration' section, the 'Provisioning' sub-tab is active. The 'SIP Server Address' is set to 172.16.78.1. The 'TFTP Provisioning' section shows 'Enable TFTP support' and 'Enable Syslog Logging' both checked, with 'Default: True' for each. 'Enable Write permission' is unchecked. The 'TFTP Server Address' is also 172.16.78.1. The 'HTTP Provisioning' section shows 'Enable HTTP support' checked with 'Default: True'. The 'Protocol' is set to 'HTTPS'. The 'Server (Hostname or IP)' is 192.168.78.1, with a default of 192.168.192.78. The 'Listen on Port' is 5555, with a default of 5555. The 'TFTP Alias' is /tftpboot/, with a default of /tftpboot/. 'Enable Auto-Create support if configuration doesn't exist' is unchecked. 'Enable HTTP Authentication' is also unchecked. The 'ScopCOMM Provisioning' section shows 'Enable ScopCOMM Provisioning service' unchecked. At the bottom, there are 'Save' and 'Cancel' buttons.

Server Configuration

Configuration

General Provisioning Proxy Settings SMTP Settings Performance Tuning Security (SSL)

* SIP Server Address: 172 . 16 . 78 . 1

TFTP Provisioning

Enable TFTP support ? ☒ : Default: True

Enable Syslog Logging ? ☒ : Default: True

Enable 'Write' permission ? : ☐

TFTP Server Address: 172 . 16 . 78 . 1

HTTP Provisioning

Enable HTTP support ? ☒ : Default: True

* Protocol: HTTPS

* Server (Hostname or IP): 192.168.78.1
Default: 192.168.192.78

* Listen on Port ☒ : 5555
Default: 5555

* TFTP Alias: /tftpboot/
Default: /tftpboot/

Enable Auto-Create support if configuration doesn't exist : ☐

Enable HTTP Authentication ? ☐

ScopCOMM Provisioning

Enable ScopCOMM Provisioning service ? ☐

Save Cancel

Configuring Telephony – Channels - SIP Channel

Enable support for SIP TLS (Secure)

Select your Certificate

Highlight your Certificate Chain

Click Save

Commit your Telephony changes

Restart the Telephony Server

Congratulations you have enabled SIP TLS support for the Telephony Server

Telephony Settings: Channels

Configuration Channels Language Time Zones Asterisk Manager External API Monitoring Scheduled Tasks Help

Channels

General RTP Options Codecs **SIP Channel** IAX Channel Woomera Channel ENUM mISDN Channel Jitter Buffer

Port (UDP): 5060
Default: 5060

Bind Address (UDP): IPv4: 0 . 0 . 0 . 0
IPv6:

Enable support for SIP TCP ? ☒ :
Port (TCP): 5060
Default: 5060

Bind Address (TCP): IPv4: 0 . 0 . 0 . 0
IPv6:

Enable support for SIP TLS (secure) ? ☒ :
Port (TLS): 5061
Default: 5061

Bind Address (TLS): IPv4: 0 . 0 . 0 . 0
IPv6:

* Certificate: yourcertname
Certificate Chain: yourcachain

To select multiple items, hold down the Control (PC) or Command (Mac) key while clicking.

Enable Outbound Proxy support ? ☐ :
When enabled, the server will send outbound signalling to the specified server, not directly to devices.

Configuring Telephony – Extension – Phone Options

Edit an extension's Phone Options so that it will use Transport Mode TLS and Enable SRTP encryption AES 80

Save and Commit your changes

Congratulations you have just enabled TLS/SRTP on this extension and restricted all communications to use encryption

Telephony Settings: Channels

Configuration Channels Language Time Zones Asterisk Manager External API Monitoring Scheduled Tasks Ha

Channels

General RTP Options Codecs SIP Channel IAX Channel Woomera Channel ENUM mISDN Channel Jitter Buffer

Port (UDP): 5060
Default: 5060

Bind Address (UDP): IPv4: 0 . 0 . 0 . 0
IPv6:

Enable support for SIP TCP ? ☒

Port (TCP): 5060
Default: 5060

Bind Address (TCP): IPv4: 0 . 0 . 0 . 0
IPv6:

Enable support for SIP TLS (secure) ? ☒

Port (TLS): 5061
Default: 5061

Bind Address (TLS): IPv4: 0 . 0 . 0 . 0
IPv6:

* Certificate: yourcertname

Certificate Chain: yourcachain

To select multiple items, hold down the Control (PC) or Command (Mac) key while clicking.

Enable Outbound Proxy support ? ☐
When enabled, the server will send outbound signalling to the specified server, not directly to devices.

Configuring Telephony – Automatic Provisioning System - Snom

In this example we are configuring a template and only the options needed to secure communications on the phone.

Configure the Provisioning tab to use HTTPS by putting https in the provisioning URL and by selecting the certificates you created earlier.

Then click on the Options tab

The screenshot shows the 'Phone Provisioning' configuration window. At the top, there is a blue header bar with the title 'Phone Provisioning'. Below the header is a row of tabs: 'General', 'Provisioning', 'Options', 'Servers', 'Network', 'Date and Time', 'Phone Options', 'Audio', 'Soft Keys', and 'Security'. The 'Provisioning' tab is currently selected. Below the tabs, there is a 'Multicast Paging' sub-tab. The main configuration area contains several fields and dropdown menus. The 'Firmware Version' field is set to '8.x' with a dropdown arrow. Below it, the 'Default: 8.x' is noted. The 'Firmware URL' field contains 'https://yourserverip.yourdomain.com:55'. The 'Firmware Status URL' field is empty. Below it, a note says 'URL of the firmware configuration file. e.g. http://www.company.com/settings/snomXXX-firmware.htm'. The 'Configuration Server' field is marked with a red star and contains 'https://yourserverip.yourdomain.com:55'. Below it, an example URL is provided: 'Example: http://server:5555/tftpboot/snom/{mac}.xml'. The 'Web Language URL' field contains 'http://provisioning.snom.com/config/w'. Below it, the default URL is 'http://provisioning.snom.com/config/web_lang.xml'. The 'GUI Language URL' field contains 'http://provisioning.snom.com/config/g'. Below it, the default URL is 'http://provisioning.snom.com/config/gui_lang.xml'. The 'Update Policy' dropdown is set to 'Automatic Update'. Below it, the default is 'Settings Only (no Firmware)'. At the bottom, there is a checkbox labeled 'User can write/overwrite existing configuration: on phone ?' which is currently unchecked. At the very bottom, there are 'Add' and 'Cancel' buttons.

Phone Provisioning

General Provisioning Options Servers Network Date and Time Phone Options Audio Soft Keys Security

Multicast Paging

Firmware Version : 8.x
Default: 8.x

Firmware URL : https://yourserverip.yourdomain.com:55

Firmware Status URL :
URL of the firmware configuration file. e.g. http://www.company.com/settings/snomXXX-firmware.htm

* Configuration Server : https://yourserverip.yourdomain.com:55
Example: http://server:5555/tftpboot/snom/{mac}.xml

Web Language URL : http://provisioning.snom.com/config/w
Default: http://provisioning.snom.com/config/web_lang.xml

GUI Language URL : http://provisioning.snom.com/config/g
Default: http://provisioning.snom.com/config/gui_lang.xml

Update Policy : Automatic Update
Default: Settings Only (no Firmware)

User can write/overwrite existing configuration: ☐
on phone ?

Add Cancel

Configuring Telephony – Automatic Provisioning System - Snom

Edit the path for the Certificate URL to include https and select the Certificates you created earlier

Then click on the Servers tab

Phone Provisioning

General Provisioning **Options** Servers Network Date and Time Phone Options Audio Soft Keys Security LDAP PBX Services

Multicast Paging

Syslog Server:
Server to store the log messages coming from the phone.

Certificate URL:
Example: http://192.168.0.1:5555/tftpboot/snom/{mac}.DER

Certificate:
If you want to use TLS encryption, you must specify a Client Certificate.

Certificate Chain:
To select multiple items, hold down the Control (PC) or Command (Mac) key while clicking.

Display Name (Global):
You can use the following macros: \${EXTEN}, \${NAME}, \${USER}

Add Cancel



Configuring Telephony – Automatic Provisioning System - Snom

Change both the Registrar Port and Proxy Port to 5061

You must enter both the Registrar and SIP Proxy IP

Then click on the PBX Services tab

Phone Provisioning

General Provisioning Options **Servers** Network Date and Time Phone Options Audio Soft Keys Security LDAP PBX Services

Multicast Paging

★ Registrar:	172	. 16	. 78	. 1	Port	5061
SIP Proxy:	172	. 16	. 78	. 1	Port	5061

Start RTP Port:
Default: 10000

Stop RTP Port:
Default: 20000

SIP Retry T1:
Set the retry timer in milliseconds after which an unanswered request is resent. If it is set to 500, the phone will resend the unanswered request after 500, 1000, 2000, 4000, 6000 ... 31500 ms. If the request is still unanswered after this procedure, an error message will be shown on the display.

Subscription (SUBSCRIBE) expiration (in seconds):
Default: 360

Subscription (SUBSCRIBE) delay (in seconds):
Selects a random number around the given value in seconds to send delayed batch subscriptions (Minimum value is 60 seconds).



Configuring Telephony – Automatic Provisioning System - Snom

Change the GUI Protocol selection to HTTPS

In the GUI Server (hostname or IP) field enter the required IP address or Fully Qualified Host Name of the server

Click Add when done

The screenshot shows the 'Phone Provisioning' interface with the 'Multicast Paging' tab selected. The 'GUI Protocol' is set to 'HTTPS'. The 'GUI Server (Hostname or IP)' field contains '172.16.78.1' with a default of '192.168.192.78'. The 'GUI Port' is set to '5555' with a default of '5555'. There are three checkboxes: 'Use Micro-Browser ?' (checked), 'Use internal Directory ?' (checked), and 'Enable Hotline support ?' (checked). Below these are several fields for URLs: 'URL to display on Snom/Services key:', 'URL to display on Directory key:', 'Action URL for Incoming Call:', 'Action URL for Outgoing Call:', 'Action URL for an Off-Hook:', 'Action URL for an On-Hook:', 'Action URL on Connected Call:', 'Action URL on Disconnected Call:', and 'Action URL on Missed Call:'. At the bottom are 'Add' and 'Cancel' buttons.

Phone Provisioning	
General Provisioning Options Servers Network Date and Time Phone Options Audio Soft Keys Security LDAP PBX Services	
Multicast Paging	
GUI Protocol:	HTTPS
★ GUI Server (Hostname or IP):	172.16.78.1 Default: 192.168.192.78
★ GUI Port:	5555 Default: 5555
Use Micro-Browser ?	<input checked="" type="checkbox"/>
Use internal Directory ?	<input checked="" type="checkbox"/>
Enable Hotline support ?	<input checked="" type="checkbox"/>
URL to display on Snom/Services key:	
URL to display on Directory key:	
Action URL for Incoming Call:	
Action URL for Outgoing Call:	
Action URL for an Off-Hook:	
Action URL for an On-Hook:	
Action URL on Connected Call:	
Action URL on Disconnected Call:	
Action URL on Missed Call:	
Add	Cancel

Configuring Telephony – Automatic Provisioning System - Snom

Edit an existing or create a new MAC object for your Snom phone

Click on the Lines tab

Assign an extension to Line 1 (other lines are optional)

Enable Secure RTP (SRTP) must be checked

Only Accept SRTP (secure) calls must be checked

Enable TLS transport must be checked

Save your changes

Commit Telephony changes

Commit APS changes

Reboot the phone so it downloads its new configuration files

Phone Provisioning


General


Lines

Network

PBX Services

Multicast Paging

Line 1 

112: Test 112 (SIP) 


Display Name:

If empty, we will use the value of 'Display Name (Global)'. You can


Enable ICE support ?:

☐

Default Ring Tone:

Ringer 1 

Default: Ringer 1

Enable Secure RTP (SRTP)? 

☒

Only accept SRTP (secure) calls?:

☒

If checked, the SAVP header will be mandatory.


Enable TLS transport ?:

☒

You must define a SIP (Outbound) Proxy and set TLS port (5061).


Enable SIP INFO (DTMF) ?:

☐


Use Custom Dial Plan ? 


☐


Failover Identity:


None 


This identity will be used as a backup for failover, i.e. if the current


Line 2 

None 

Line 3 

None 

Line 4 

None 

Save

Copy

Cancel



Configuring Telephony – Automatic Provisioning System - Polycom

In this example we are configuring a template and only the options needed to secure communications on the phone.

Configure the Provisioning tab to use HTTPS by putting https in the provisioning URL and by selecting the certificates you created earlier.

Then click on the Lines tab

The screenshot shows the 'Phone Provisioning' configuration page. The 'Provisioning' tab is selected, and the 'Security' sub-tab is active. The configuration fields are as follows:

- Provisioning Server:**
Use this provisioning server if the DHCP client is disabled, if the DHCP server does not send a boot server option, or if the boot server parameter is set to Static. If using a URL, you can apply a user name and password.
- Provisioning Server Type:**
Default: TFTP
- Provisioning Server Username:**
- Provisioning Server Password:**
- Firmware Version:**
Default: 4.0+
- Firmware Application:**
Default: sip.ld
- Certificate:**
If you want to use TLS encryption, you must specify a Client Certificate.
- Certificate Chain:**
To select multiple items, hold down the Control (PC) or Command (Mac) key while clicking.
- Trusted Root CA:**

At the bottom, there are 'Add' and 'Cancel' buttons.

Configuring Telephony – Automatic Provisioning System - Polycom

Enable SRTP (secure) calls?

Then click on the Servers tab

Phone Provisioning

General

Provisioning

Lines

Servers

Network

PBX Services

Security

Enable SRTP (secure) calls?  : ☒

Only accept SRTP (secure) calls?: ☐

Customize number of Lines / Soft Keys?  : ☐

Enable Enhanced Function Key (EFK) support ? : ☐



Add

Cancel



Configuring Telephony – Automatic Provisioning System - Polycom

Change the SIP Transport to TLS

Change the SIP Proxy Port to 5061

Click on the PBX Services Tab

Phone Provisioning

General Provisioning Lines Servers Network Options Date and Time User Preferences Audio/RingTone
PBX Services Security

SIP Transport: TLS

* SIP Proxy: 172 . 16 . 78 . 1 Port 5061

Backup Proxy: Port

Outbound Proxy: Port

Emergency Proxy: Port

Emergency Number(s):

Please note that you must define an Emergency Proxy. Coma-separated list (Example: 911, 9911)

Keepalive (SIP UDP/TCP/TLS)

Enable Session Timers?: ☐

Enable TCP keep-alive for TLS transport?: ☒

Wait Time before sending Keep-alive message to: 30 server? *Permitted Value 10 to 7200 seconds.*

Retry Time before sending Keep-alive message to: 20 server? *If no response is received to a keep-alive message, subsequent messages are sent at this interval. Permitted Value 5 to 120 seconds.*

Add Cancel

Configuring Telephony – Automatic Provisioning System - Polycom

Change the GUI Protocol to use HTTPS

And edit the GUI Server (Hostname or IP) to match your required configuration.

Click Add when done

Provision MAC addresses for your Polycom phones and apply the template to each required phone

Commit Telephony changes

Commit APS changes

Reboot the phone so it can download its required configuration files

Phone Provisioning

General Provisioning Lines Servers Network Options Date and Time User Preferences
PBX Services Security

Note: You must have Firmware SIP 2.1 or later to get Microbrowser support on SoundPoint IP 430 and 501 platform.

GUI Protocol:

* GUI Server (Hostname or IP):
Default: 192.168.192.78

* GUI Port:
Default: 5555

Proxy Server: . . . Port

Use Micro-Browser ? ☐

Use internal Directory ? ☐

Refresh Interval (in seconds):
Default: 15

URL to display on Idle:

URL to display on the Main page:

Add Cancel

Configuring Telephony – Automatic Provisioning System - Polycom

Edit the MAC address object of your Polycom phone

Select the desired Tenant

Choose the correct Phone Model from the list

Choose the Phone Template you configured with HTTPS parameters

Click on the Lines tab and assign an extension

Save your settings

Commit Telephony changes

Commit APS changes

Reboot the phone to download the configuration files

The screenshot shows the 'Phone Provisioning' interface with the 'Lines' tab selected. The interface includes a 'Local SIP Port' field, a 'Key/Line 1' dropdown menu set to '5000: (SIP)', and a 'Number of line keys appearances' field set to '1'. Below this is a 'Number of Calls per Line key' field set to '8'. There is also an 'Auto off hook' checkbox and an 'Auto off hook contact' field. At the bottom, there are 'Key/Line 2', 'Key/Line 3', and 'Key/Line 4' dropdown menus, all set to 'None'. The interface has a blue header and footer with 'Add' and 'Cancel' buttons.

Phone Provisioning

General Lines Network PBX Services License

Local SIP Port:

Key/Line 1 : 5000: (SIP) Default: none

* Number of line keys appearances?: This tells phone how many line appearances each line definition should take.

* Number of Calls per Line key: Default: 8

Auto off hook?: ☐

Auto off hook contact:

Key/Line 2 : None Default: none

Key/Line 3 : None Default: none

Key/Line 4 : None Default: none

Add Cancel



Configuring Telephony – Automatic Provisioning System - Yealink

In this example we are configuring a template and only the options needed to secure communications on the phone.



Configure the Provisioning tab to use HTTPS by putting https in the provisioning and Firmware URL and by selecting the certificates you created earlier.



Then click on the Server tab

Phone Provisioning

General | **Provisioning** | Server | Network | Date and Time | Phone Options | DSS Keys | Programmable Keys | Audio/Volume

Internal Ringer | Multicast Paging | PBX Services | LDAP

Firmware Version : Version 80 (or later) 
Default: Version 80 (or later)


Provisioning Mode : Power on + Repeatedly 
Default: Power on

Sync Interval (in Minutes): 60
Value: 1 to 43200 minutes


Provisioning URL: https://yourserverip.yourdomain.com:55
Example: http://192.168.0.1:5555/tftpboot/


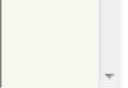
Protect personalized settings?: ☐
If enabled, personalized settings configured via web or phone user interface will be protected and remained after

Periodically upload personalized settings?: ☐
If enabled, the IP phone will periodically upload the MAC-local CFG file to the provisioning server. During auto provision the MAC-local CFG file from the provisioning server.


HTTP Upload method: PUT 
Default: PUT

Firmware URL: https://192.168.0.1:5555/tftpboot/yealink
Example: http://192.168.0.1:5555/tftpboot/yealink/2.70.0.50.rom

Certificate: yourcertname 
If you want to use TLS encryption, you must specify a Client Certificate.

Certificate Chain: yourcachain 


To select multiple items, hold down the Control (PC) or Command (Mac) key while clicking.

Trusted Root CA: yourcarootca 

Accept only trusted certificates?: ☒



Configuring Telephony – Automatic Provisioning System - Yealink

Change the Registrar Port to 5061

Then click on the PBX Services tab

Phone Provisioning

General

Provisioning

Server

Network

Date and Time

Phone Options

DSS Keys

Internal Ringer

Multicast Paging

PBX Services

LDAP

* Registrar:	172	.	16	.	78	.	1	Port	5061
Outbound Proxy Server:		.		.		.		Port	
Backup Registrar:		.		.		.		Port	
Backup Outbound Proxy Server:		.		.		.		Port	
* Registration Expiration Time:	3600 Default: 3600								
* Registration Retry Counts:	3 Default: 3								
Failback Mode:	New Requests ▼								
* Failback Timeout:	3600 Default: 3600								
Register on Enable?:	<input type="checkbox"/> <i>Enables or disables the IP phone to register to the secondary server</i>								

Save

Copy

Cancel

Configuring Telephony – Automatic Provisioning System - Yealink

Change the GUI Protocol to use HTTPS

And edit the GUI Server (Hostname or IP) to match your required configuration.

Phone Provisioning

General Provisioning Server Network Date and Time Phone Options

Internal Ringer Multicast Paging **PBX Services** LDAP

GUI Protocol: HTTPS

* GUI Server (Hostname or IP): 172.16.78.1
Default: 192.168.192.78

* GUI Port: 5555
Default: 5555

Configuring Telephony – Automatic Provisioning System - Yealink

Edit the MAC address object of your Yealink phone

Select the desired Tenant

Choose the correct Phone Model from the list

Choose the Phone Template you configured with HTTPS parameters

Click on the Lines tab and assign an extension

Choose Transport: TLS

Enable Voice Encryption (SRTP)

Save you settings

Commit Telephony changes

Commit APS changes

Reboot the phone to download the configuration files

The screenshot displays the 'Phone Provisioning' interface with the 'Lines' tab selected. The configuration for 'Line 1' is shown with the following settings:

- Line 1**: 5000: (SIP)
- Label (Phone Display)**: 5000
- Display Name**: (empty)
- Ring Type**: Common (Default: Common)
- Caller ID Source**: PAI-FROM
- Transport**: TLS (highlighted with a red box)
- DTMF Mode**: RFC2833 (Default: RFC2833)
- Enable Voice Encryption (SRTP)?**: ☒ (highlighted with a red box)
- Only accept SRTP (secure) calls?**: ☐
- Enable Auto-Answer?**: ☐
- Customize Voicemail Button?**: ☐

Verifying Operation

In the Asterisk CLI

```
sip*CLI> sip show tcp
```

Address	Transport	Type
192.168.192.191:12501	TLS	Client
192.168.192.191:11880	TLS	Server
192.168.192.6:2057	TLS	Server
192.168.192.6:2075	TLS	Server

Transport TLS confirms that the peer is configured to use TLS

If you want to check the validity of your SSL Certificate use this URL

<https://cryptoreport.rapidssl.com/checker/views/certCheck.jsp>



Vous avez besoin de plus d'information?

ScopServ Europe
(via Channel Plus)

5 Place de la Pyramide
Paris La Défense
92088 FRANCE

Téléphone: +33 1 55 68 12 79
Mobile : +33 7 62 92 41 61

Courriel : info@scopserv.fr
Contact : Hervé Loustalot

ScopServ International Inc.
Siège social

4486, Boul. Gouin Ouest
Montréal (Québec)
Canada H4J 1B7

Téléphone : 514-373-8102
Sans frais : 1 866-722-3292

Courriel: info@scopserv.com
Contact : Denis Trépanier

ScopServ South Africa PTY
ScopServ Integrated Services

9 Kingfisher Drive
Douglasdale, Johannesburg
Gauteng, 2129 Afrique du Sud

Téléphone : +27 11 700 3800
Téléc. : +27 11 700 3810

Courriel : info@scopservice.co.za
Contact : Janet Souter

Nous vous remercions pour votre intérêt envers nos solutions.



Need more information?

ScopServ Europe
(via Channel Plus)

5 Place de la Pyramide
Paris La Défense
92088 FRANCE

Phone: +33 1 55 68 12 79
Cell: +33 7 62 92 41 61

Email: info@scopserv.fr
Contact: Hervé Loustalot

ScopServ International Inc.
Corporate Headquarters

4486, Gouin W. Blvd
Montreal (Quebec)
Canada H4J 1B7

Phone: 514-373-8102
Toll Free: 1 866-722-3292

Courriel: info@scopserv.com
Contact: Denis Trépanier

ScopServ South Africa PTY
ScopServ Integrated Services

9 Kingfisher Drive
Douglasdale, Johannesburg
Gauteng, 2129 South Africa

Phone: +27 11 700 3800
Fax: +27 11 700 3810

Email: info@scopservice.co.za
Contact: Janet Souter

We thank you for your trust and interest in our solutions.





Because Communications Matter

Aim high, aim right!

Ask your preferred integrator for a free consultation.

scopserv.com



La solution pour vos communications d'entreprise

Visez loin, visez juste !

Contactez votre intégrateur préféré et demandez une consultation gratuite.

scopserv.com