SCOPTEL IP PBX Software - Automatic Provisioning System

Contents

Background

- The APS (Automatic Provisioning System) is used to create the required configuration files needed for many SIP end devices. The APS assigns SIP usernames and passwords, network options, time settings, QoS settings, dial plans , firmware upgrade policies, soft key programming, DSS/BLF programming, security settings, DTMF modes, LDAP settings,

- Templates can be configured to simplify tedious configuration settings for as many supported SIP end points as required

- Extensions you wish to assign to a MAC address must already exist so they must be created first before trying to assign then them to hardware using the APS.

- Here is a list of supported vendors :

    - Yealink

    - Aastra

    - Polycom

    - Cisco

    - Sipura/Linksys/Cisco

    - Panasonic SIP and SIP DECT

    - VtechHospitality Phones

    - Snom

    - CyberdataIntercoms

    - Grandstream

    - SpectraLink

    - Alcatel

    - AudioCodes

    - LG-Ericsson

Security

- Hackers are routinely scanning IP addresses for open ports and if they find an IP address vulnerable to brute force scanning they will execute a remote Provisioning scan using the first 6 digits of popular vendor ID's like Polycom, Yealink and then brute force the last 6 digits of a 12 digit MAC address.

- By example a SCOPTEL server using the default HTTP listen port of 5555 can be attacked using this method. Other vendors are also vulnerable on whatever HTTP listen port they use to remotely provision IP phones.

- TFTP is especially vulnerable on UDP port 69 because no specific path is required to the MAC.cfgfile. Only the <MAC>.cfgvariable is required to harvest the MAC.cfgfile. TFTP should be denied on the Firewall whenever possible.

- If you have enabled Telephony>Configuration>Security>Flood Protection and the SCOPTEL Firewall and Telephony Flood Protection (Fail2ban) Service then the remote attacker's IP address will be blacklisted by the Firewall when a brute force attack is detected.

- But if the remote attacker knows of a valid MAC address on the network then this MAC.cfgfile can easily be harvested unless HTTP Authentication is configured. The exact methodology won't be published here as this should not be public knowledge.

- Refer to: https://blog.scopserv.com/2018/10/securing-configuration-files-with-http-authentication/

IP/DNS Mapping explained

The purpose of the IP/DNS Mapping it to replace a 'dummy' IP address or static IP address with a FQDN (Fully Qualified Domain Name)

- FQDN's are highly advantageous for the following reasons :

    - A public DNS A record can help a remote VoIP phone contact the SCOPTEL server's public IP address in order to register its SIP account and update its provisioning settings.

    - A local DNS A record can help a local VoIP phone contact the SCOPTEL server's public IP address in order to register its SIP account and update its provisioning settings.

- If either the server's LAN or WAN addresses changes the APS configurations will not require changing

- Only the DNS A records will require any changes and since the phone will always use DNS lookups to re - register or reconfigure itself, downtime is kept to a minimum

- In any of these scenarios the phone only is always configured with the same FQDN and if the DNS A record requires changing on the IP/DNS Mapping needs to be edited.

Add a new Provisioning System

- From Configuration > Telephony > Provisioning click on "Add a new Provisioning System "

IP/DNS Mapping

- From the Tenant drop list selector choose Tenant>All (Global) so that all tenants can use the same IP/DNS Mapping. Or select the specific tenant you would like to restrict the IP/DNS Mapping to.

- In this example the source IP address 1.1.1.1 is a dummy address which will be replaced with master88.commzilla.net in the /tftpboot/<mac>.cfg files.

- When done editing Add the object and carry on adding hardware based templates and then add MAC address based objects using the templates.

- This replacement is automatically done for all instances of 1.1.1.1 in any template or MAC based APS object as shown in these examples :

Auto Provisioning System (APS): Phone Provisioning

| Phone Provisioning | Firmware |

Phone Provisioning

| General |

* Tenant ⟳ :	All (Global) ▼
* Phone Model ⟳ :	IP/DNS Mapping ▼
* Source :	1 . 1 . 1 . 1
* Destination :	master88.commzilla.net

Add   Cancel

Phone Provisioning

General	Provisioning	Server	Network	Date and Time	Phone Options	DSS Keys	Programm
Power Saving	Security	Internal Ringer	Multicast Paging	PBX Services	LDAP	Custom Settings	

* Registrar :	1	. 1	. 1	. 1	Port 5060
Outbound Proxy Server :		.	.	.	Port
Backup Registrar :		.	.	.	Port
Backup Outbound Proxy Server :		.	.	.	Port

Adding a new Hardware based template

- From Configuration > Telephony > Provisioning click on "Add a new Provisioning System"
- From the Tenant drop list selector choose Tenant>All (Global) so that all tenants can use the same IP/DNS Mapping. Or select the specific tenant you would like to restrict the vendor template to.
- From the Phone Model drop list select the matching hardware for the phones you will be deploying.
- Make sure you click on the 'Create Template' checkbox.
- Give this template a meaningful name
- Click on the Provisioning tab

General

- Use the drop list selector to choose the installed firmware version of the device so this template will write compatible files.

- Use the drop list to choose the preferred sync method.

- Provisioning URL : enter the full path to the provisioning server in format : < http_protocol >://<WAN_IP/LAN_IP>:< Listen_on_Port >/< TFTP_Alias >/

- Example : http://master 88.commzilla.net:5555/tftpboot/

- Firmware URL : Enter the full path to the provisioning server in format : < http_protocol >://<WAN_IP/LAN_IP>:Listen_on_Port >/< TFTP_Alias >/< firmware _filename >

- Example : http://master88.commzilla.net:5555/tftpboot/T48-35.83.0.50.rom

- Click on the Server tab

Server

- In the Registar boxes enter the dummy IP address created for the IP/DNS Mapping
- Click on the Network tab

Network

- Use NAT option is recommended so that rport may be enabled.

- STUN Server : not recommended

- Enable Link Layer Discovery Protocol (LLDP) is an optional open standard Layer 2 protocol that allows automatic VLAN membership.

- Enable Cisco Discovery Protocol (CDP) is an optional Cisco Layer 2 protocol that allows automatic VLAN membership.

- Click on Date and Time tab when done

Date and Time

- Modify the Date and Time configuration if needed

- Click on Phone Options

Phone Provisioning

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

| Power Saving | Security | Internal Ringer | Multicast Paging | PBX Services | LDAP | Custom Settings |

Enable Time Server? ☑
Default: True

* Primary NTP Server : `pool.ntp.org`
Default: pool.ntp.org

Secondary NTP Server :

NTP Refresh Time (in seconds) : `3600`
Default: 3600

Enable Daylight Saving Time? ☑
Default: True

Daylight Saving Mode : Automatic ▾
Default: Automatic

DST Time Type : By Date ▾

DST Start Date :
The value formats are 'MM/DD/HH' (for By Date) or 'Month/Day of Week/Day of Week Last in Month/Hour of Day' (for By Week)

DST End Date :
The value formats are 'MM/DD/HH' (for By Date) or 'Month/Day of Week/Day of Week Last in Month/Hour of Day' (for By Week)

DST Offset time (in minutes) :
Range: -300 to +300

Display Date format : WWW MMM DD ▾

Display Time in 24 hour format? : ☐
Default: True

Time Zone : -5 United States-Eastern Time ▾
Default: -5 United States-Eastern Time

Phone Options

Modify settings like :

- The Phone Language for the end user interface
- Country Tone
- Set Custom Tones
- Any other preferred options
- Click on DSS Keys

Phone Provisioning

| General | Provisioning | Server | Network | Date and Time | **Phone Options** | DSS Keys | Programmable Ke |
| Power Saving | Security | Internal Ringer | Multicast Paging | PBX Services | LDAP | Custom Settings |

Phone Language : English ▼
Default: English

Ringer device : Speaker & Headset ▼
Default: Speaker & Headset

Country Tone : United States ▼
Default: United States

Set Custom Tones? ↻ : ☑

Custom Tones

Dial :

Ring Back :

Busy :

Congestion :

Call Waiting : 0/100,500/100,0/100,500/100,0/100,500/100,0/500

Dial Recall :

Record :

Info :

Stutter : 0

DSS Keys Vs Programmable Keys
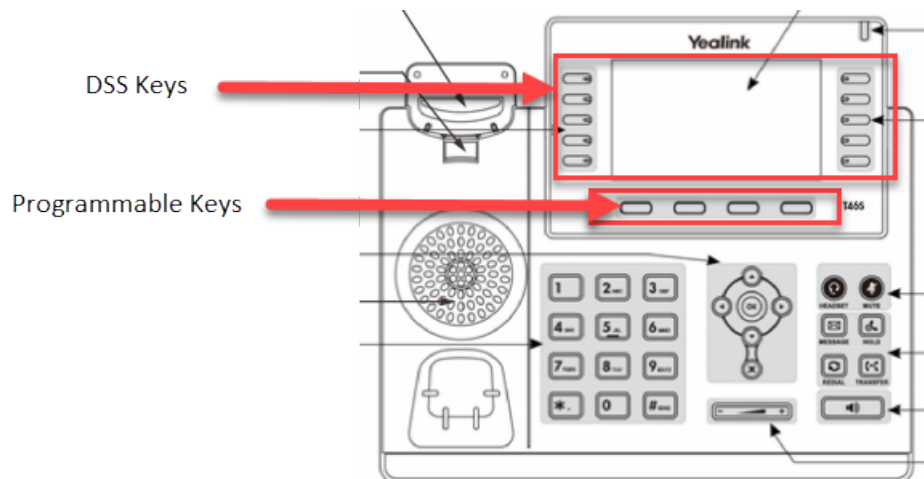
DSS Keys

- DSS Keys are the

- Enable Enhanced DSS Keys (EDK) support to enable SCOPTEL PBX Features in the drop lists

- Deal Type recommendation is Attended Transfer for proper PBX Features functionality

- Expansion Module type and Number of Expansion Modules assigned is dependent on additional hardware and optional.

- Key 1 is used for the Extension assignment. Leave the Label blank and the Line drop list set to Line 1. NOTE : each line key can process 8 concurrent calls. There is no need to have more than one Key assignment per Extension. Remaining Key buttons can be allocated for BLF, Key Event, Speed Dials, Features, DTMF events, Directory lookups, etc…

- Click on Programmable Keys when you are done editing.

Programmable Keys

- Programmable Keys can be reassigned from their Factory Defaults
- Click On Security tab when done

Phone Provisioning

Key 1 (Soft Key 1) ⟳ : [History ▼]
Label : [_____]

Key 2 (Soft Key 2) ⟳ : [XML Phone Book ▼]
Label : [lab88_____]
XML Phone Book URL : [_____]

Key 3 (Soft Key 3) ⟳ : [PBX Feature ▼]
Label : [Park_____]
* Feature : [One Touch Park (EDK) ▼]

Key 4 (Soft Key 4) ⟳ : [Menu ▼]
Label : [_____]

Key 5 (UP key) ⟳ : [History ▼]
Label : [_____]

Key 6 (DOWN key) ⟳ : [XML Phone Book ▼]
Label : [_____]
XML Phone Book URL : [_____]

Key 7 (LEFT key) ⟳ : [Switch Account ▼]
Label : [_____]

Key 8 (RIGHT key) ⟳ : [Switch Account ▼]
Label : [_____]

Key 9 (OK key) ⟳ : [Status ▼]
Label : [_____]

Security

- It is recommended to change the Admin Password

- It is quite common for a user to experience ghost calls on their phones. This happens when a firewall binds the default SIP signaling port udp / 5060 of the phone with the public interface of the firewall as a badly implemented SIP ALG.

- Public tools like http://blog.sipvicious.org/ are often used to port scan public IP addresses on port 5060 looking for devices with weak security to exploit. When this happens we often see and hear the ghost calls.

To prevent this it is recommended to : * Disable Allow Direct IP Call * Enable Accept SIP Trust Server Only * On the Line Key assignment use a non standard UDP port between the values of udp / 10000 - 20000 * NOTE that the Local SIP Port cannot be configured in any template and must be assigned to the APS MAC configuration. * Click on the Multicast Paging tab when done

Multicast Paging

- Multicast Paging is beyond the scope of this document.
- Refer to : https://blog.scopserv.com/2018/02/how-to-setup-paging-in-SCOPTEL/
- When you are finished setting up Multicast Paging click on the PBX Services tab

Phone Provisioning

| General | Provisioning | Server | Network | Date and Time | Phone Options | DSS Keys | Programmable Keys |

| Power Saving | Security | Internal Ringer | Multicast Paging | PBX Services | LDAP | Custom Settings |

Multicast Page Group #1

Label : MG10

Listen IPAddress : 224 . 0 . 0 . 1   Port 11000

Multicast Page Group #2

Label :

Listen IPAddress : . . .   Port

PBX Services

- PBX Services allow you to configure the URL for the phones to do internal Directory Lookups
- Click on the LDAP tab when done

Phone Provisioning

| General | Provisioning | Server | Network | Date and Time | Phone Options | DSS Keys |

| Power Saving | Security | Internal Ringer | Multicast Paging | PBX Services | LDAP | Cus |

GUI Protocol : HTTP ▼

＊ GUI Server (Hostname or IP) : master88.commzilla.net

Default: master88.commzilla.net

＊ GUI Port : 5555

Default: 5555

Remote Phone Book #1

Name : lab88

Use internal directory ? ⟳ : ✔

Directory Order : Name ▼

＊ Directory Name : lab88 ▼

Remote Phone Book #2

Name :

URL :

Use internal directory ? ⟳ :

LDAP

- LDAP configuration is beyond the scope of this document
- Refer to : https://blog.scopserv.com/2012/08/setting-up-an-ldap-directory-server-on-SCOPTEL-pbx/
- Once you have completed your template Click on the Add button

Phone Provisioning

General	Provisioning	Server	Network	Date and Time	Phone Options	DSS Keys	Programmable Keys	Audio/Volume	Power LED	LCD Display
Power Saving	Security	Internal Ringer	Multicast Paging	PBX Services	LDAP	Custom Settings				

Enable LDAP support? ⟳ : ☑

LDAP Source ⟳ : None (Custom) ▼

LDAP Server

* Server Address : [_____]
This setting refers to the DNS name or IP address of the LDAP server.

* Port : [389]
This setting specifies the LDAP server port. The default LDAP port is 389.

Protocol Version : Version 3 ▼
Default: Version 3

* Base DN : [_____]
This setting specifies the LDAP search base (the distinguished name of the search base object) which corresponds to the location in the directory from which the LDAP search is requested to begin.

Authentication

Username : [_____]
This setting specifies the bind 'Username' for LDAP servers. Most LDAP servers allow anonymous binds in which case the setting can be left blank. However if the LDAP server does not allow anonymous binds, you will need to provide the Username and Password allowed to query the LDAP server.

Password : [_____]
This setting specifies the bind 'Password' for LDAP servers. This setting can be left blank in case the server allows anonymous binds, otherwise you will need to provide the Password along with the Username in order to access the LDAP server.

LDAP Options

Enable LDAP Lookup for Outgoing Call ? : ☐

Adding a MAC address and assigning an Extension

- From Configuration > Telephony > Provisioning click on "Add a new Provisioning System "

Auto Provisioning System (APS): Phone Provisioning   ⚙ **Network Auto-Discovery (Scan)**   📥 **Import MAC**

Phone Provisioning	Firmware

IP/DNS Mapping [1 to 1 of 1]   ⊕ **Add a new Provisioning System**

🔍 Search: [_____] [Search]

		▲ Source	Destination						Tenant		
☐ 📝 🔍		1.1.1.1	master88.commzilla.net						debcomainbtn	☑	✖

≡ Action: - select an action - ▼   ▯ Columns to display: Select ▼

Polycom: [1 to 4 of 4]

🔍 Search: [_____] [Search]

		Mac Address	Firmware	Description	Type	Extension(s)	Time Server	DHCP	Template Name	Tenant		
☐ 📝 🔍		00:04:F2:D6:88:A2			Polycom VVX 500	211 (1)		✓	vvx500	debcomainbtn	☑	✖
☐ 📝 🔍		00:04:F2:40:96:79			Polycom IP600/650	212 (1)		✓	ip650	debcomainbtn	☑	✖
☐ 📝 🔍		vvx500	4.0		Polycom VVX 500	N/A	✓			debcomainbtn	☑	✖
☐ 📝 🔍		ip650	4.0		Polycom IP600/650	N/A	✓			debcomainbtn	☑	✖

≡ Action: - select an action - ▼   ▯ Columns to display: Select ▼

Yealink: [1 to 21 of 21]

🔍 Search: [_____] [Search]

		Mac Address	Description	Type	Extension(s)	Time Server	DHCP	Template Name	Tenant		
☐ 📝 🔍		00:15:65:BF:66:21		Yealink T41	214 (1)		✓	t41	debcomainbtn	☑	✖
☐ 📝 🔍		t48s		Yealink T48	N/A				debcomainbtn	☑	✖
☐ 📝 🔍		00:15:65:C1:4B:BC		Yealink T48	225 (1)		✓	t48s	debcomainbtn	☑	✖
☐ 📝 🔍		t41		Yealink T41	N/A				debcomainbtn	☑	✖
☐ 📝 🔍		t28p		Yealink T28	N/A				debcomainbtn	☑	✖
☐ 📝 🔍		t38p		Yealink T38	N/A				debcomainbtn	☑	✖
☐ 📝 🔍		00:00:00:00:00:11		Yealink T48	110 (1)		✓	t48g	debcomainbtn	☑	✖
☐ 📝 🔍		00:15:65:65:9E:6C		Yealink T48	216 (1)		✓	t48g	debcomainbtn	☑	✖
☐ 📝 🔍		t42gtest		Yealink T42	N/A				debcomainbtn	☑	✖

Assigning a MAC address

- You must use the Tenant selector to choose a dedicated Tenant. You cannot use Tenant 'All (Global)'
- Use the Phone Model drop list selector to find matching hardware for your phone deployment
- Choose from an already configured template
- Enter the unique MAC address of your hardware in the MAC Address field
- Click on Lines when done

Lines

- In the template example only one DSS Key was given a Line 1 assignment, so we will only configure Line 1
- Use the drop list selector to assign an unassigned Extension
- Enter the Label (Phone Display) text you wish to display on the phone's LCD screen
- In order to support P - Asserted CallerID connected line updates you must change the default Caller ID Source selection to PAI - FROM
- You may change the Local SIP Port to any custom value from 10000 - 20000 to reduce the likelihood of ghost calls
- You may optionally enable SRTP Voice Encryption but this has pre - requisite configurations that must be done in advance. Refer to : https://blog.scopserv.com/2016/09/how-to-use-the-SCOPTEL-certificate-manager-to-enable-tls-encryption/
- Click on the PBX Services tab when done

PBX Services

- Using the drop list selector choose the Extension you assigned to Line 1
- Click on Add when done

Provisioning

- Security   is   a   critical   so   before   proceeding   refer   to   :
  https://blog.scopserv.com/2018/10/securing-configuration-files-with-http-authentication/
- The SIP Server Address is used for the Auto Provisioning Feature Code at Telephony Settings : Configuration>Provisioning. It must be an address physically assigned to the server
- The TFTP server address must be an address physically assigned to the server and should be the address bound to the interface running DHCP.
- The Server Hostname must have a matching DNS A record on the DNS Server supporting this network.

- If 'Enable Auto - Create support if configuration doesn't exist' is enabled when DHCP detection detects a supported device it's MAC address will be added to the APS MAC address list. If this option is enabled then configuring the Whitelist should be considered mandatory for security purposes.
- Supported devices are : Aastra Snom Polycom Yealink

Configuration

General	**Provisioning**	Proxy Settings	SMTP Settings	Performance Tuning	Authentication (LDAP)	Security (SSL)

* SIP Server Address : `172` . `31` . `240` . `1`

TFTP Provisioning

Enable TFTP support ? ⟲ : ☑
Default: True

Enable Syslog Logging ? : ☑
Default: True

Enable 'Write' permission ? : ☑

TFTP Server Address : `172` . `31` . `240` . `1`

HTTP Provisioning

Enable HTTP support ? ⟲ : ☑
Default: True

* Protocol : `HTTP ▼`

* Server (Hostname or IP) : `master88.commzilla.net`
Default: master88.commzilla.net

* Listen on Port ⟲ : `5555`
Default: 5555

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

Enable Auto-Create support if configuration doesn't exist ? ⟲ : ☑

Allow Auto-Create from the following IP address (Whitelist) :
```
172.16.240.0/20 192.168.192.0/24
```
If empty, we will accept request from any IP addresses.
You can specify multiple addresses separated by space.
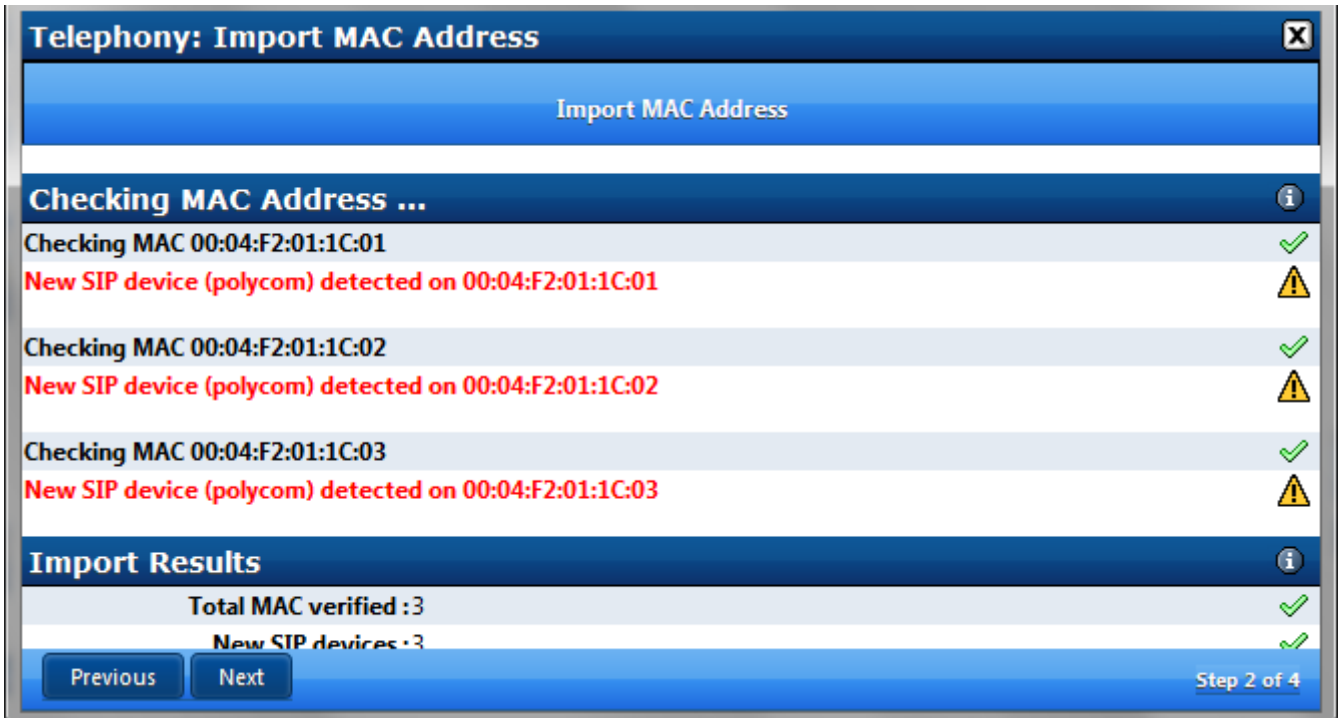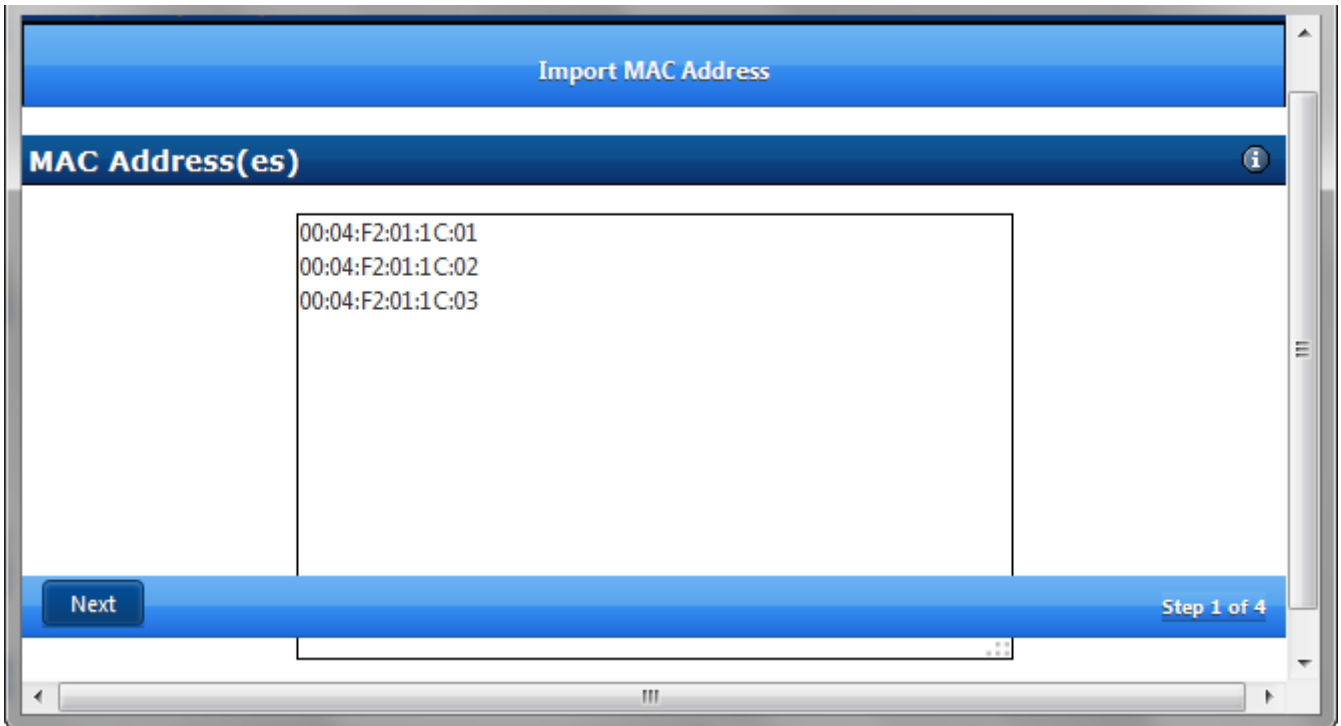Example: 192.168.0.1 172.16.240.0/24

Enable HTTP Authentication ? ⟲ : ☑
* Master Username : `admin`
* Master Password : `•••••••••••`

In addition to manually configuring MAC addresses for supported SIP devices SCOPTEL also supports several mass deployment methods

- Text import of MAC addresses from a file
- Network Scan of selected IP addresses on selected subnets
- DHCP detection of new devices when the SCOPTEL DHCP server is the only DHCP server on the LAN SCOPTEL Minimum Package Requirements
- scopserv_yum install nmap (if nmap is not already installed)
- scopserv-network-2.6.4-1.nodist. scopserv.noarch.rpm
- scopserv-server-2.6.4-1.nodist. scopserv.noarch.rpm
- scopserv-telephony 25-2.6.52-1.el5.scopserv.noarch.rpm

Text import of MAC addresses from a file

- From the APS Main Page click on Import MAC
- Enter a list of MAC addresses or copy and paste from a ASCII file
- Click Next
- A New SIP device list appears showing that the MAC vendor ID matches supported hardware (in this case 3 new Polycom phones)
- Press Next

Import MAC Address

MAC Address(es)

```
00:04:F2:01:1C:01
00:04:F2:01:1C:02
00:04:F2:01:1C:03
```

Next   Step 1 of 4

Telephony: Import MAC Address

Import MAC Address

Checking MAC Address ...

Checking MAC 00:04:F2:01:1C:01 ✓
New SIP device (polycom) detected on 00:04:F2:01:1C:01 ⚠

Checking MAC 00:04:F2:01:1C:02 ✓
New SIP device (polycom) detected on 00:04:F2:01:1C:02 ⚠

Checking MAC 00:04:F2:01:1C:03 ✓
New SIP device (polycom) detected on 00:04:F2:01:1C:03 ⚠

Import Results

Total MAC verified : 3 ✓
New SIP devices : 3 ✓

Previous   Next   Step 2 of 4

- Since the system cannot know the model number of each device you must select a matching model number from the list for each MAC address using the drop down list selections
- Click Next
- Click Finish to add the new MAC's to the APS list

Telephony: Import MAC Address ☒

Import MAC Result

Please select phone model for each detected devices. ✓
You can ignore device by uncheck it.

☐ MAC Address	Phone Model(s)
☑ 0004F2011C01	Polycom IP450 ▼
☑ 0004F2011C02	Polycom IP600 ▼
☑ 0004F2011C03	Polycom SpectraLink 8440/8450/8452 ▼

Previous Next

Step 3 of 4

Telephony: Import MAC Address ☒

Summary

Configuration completed ... ⓘ

| Adding information for 00:04:F2:01:1C:01 (Polycom IP450)	✓
Adding information for 00:04:F2:01:1C:02 (Polycom IP600)	✓
Adding information for 00:04:F2:01:1C:03 (Polycom SpectraLink 8440/8450/8452)	✓

Previous Finish

Step 4 of 4

## Network Scan of selected IP addresses on selected subnets

- This method will only add un-configured MAC addresses to the APS list
- Click on Network Auto - Discovery (Scan)
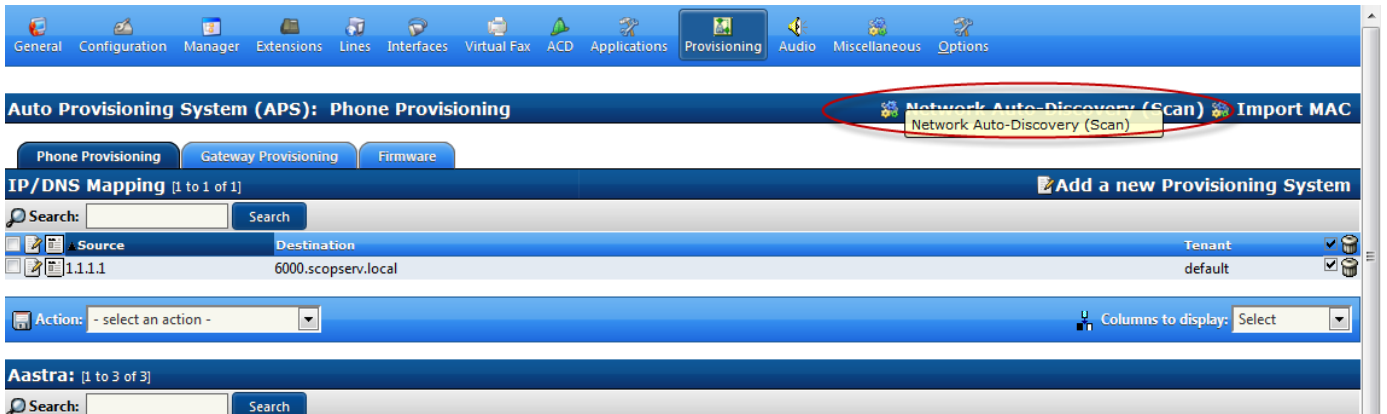
- Enter the first available IP address on a valid subnet (normally the first IP address in a DHCP pool)

- Enter the last available IP address on a valid subnet (normally the last IP address in a DHCP pool)

- Choose the Network Interface that services the valid subnet

- Choose the desired tenant

- Enter the IP address of the SIP Server (usually the IP address of the Network Interface servicing the local subnet)

- Click Next
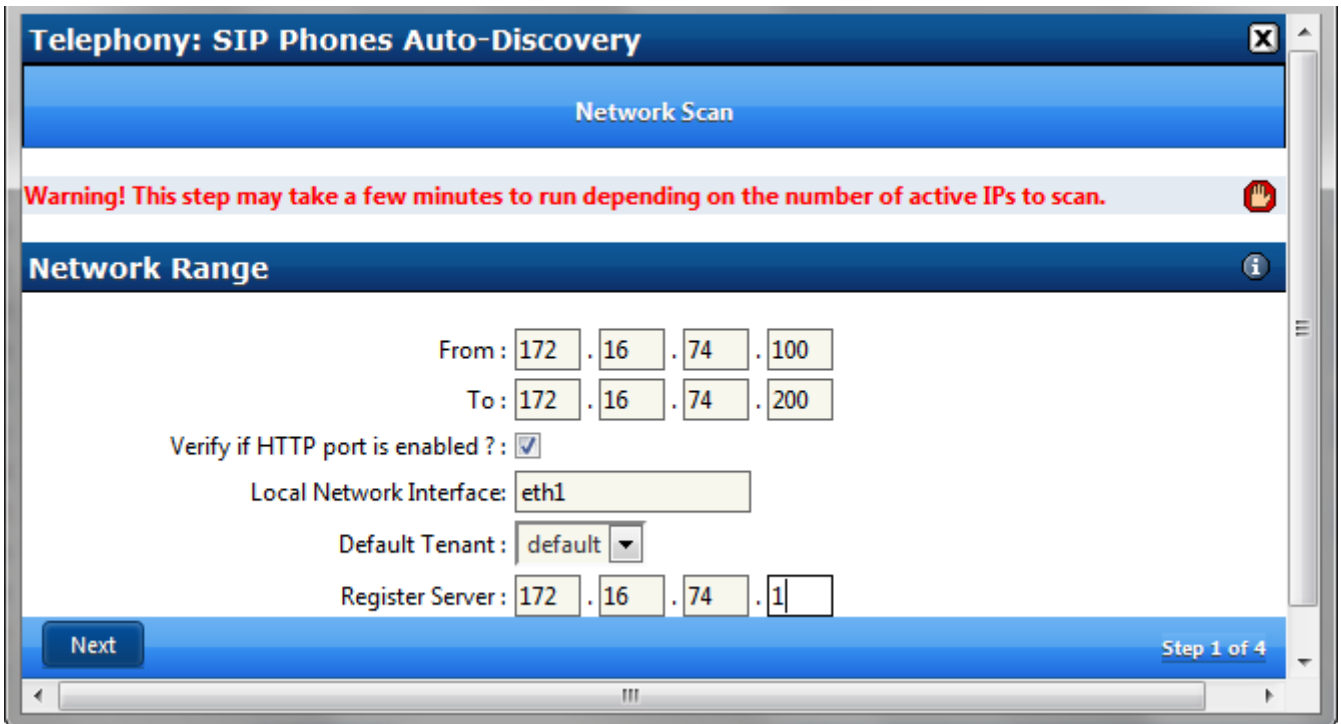
- The new window will show a list of detected MAC addresses
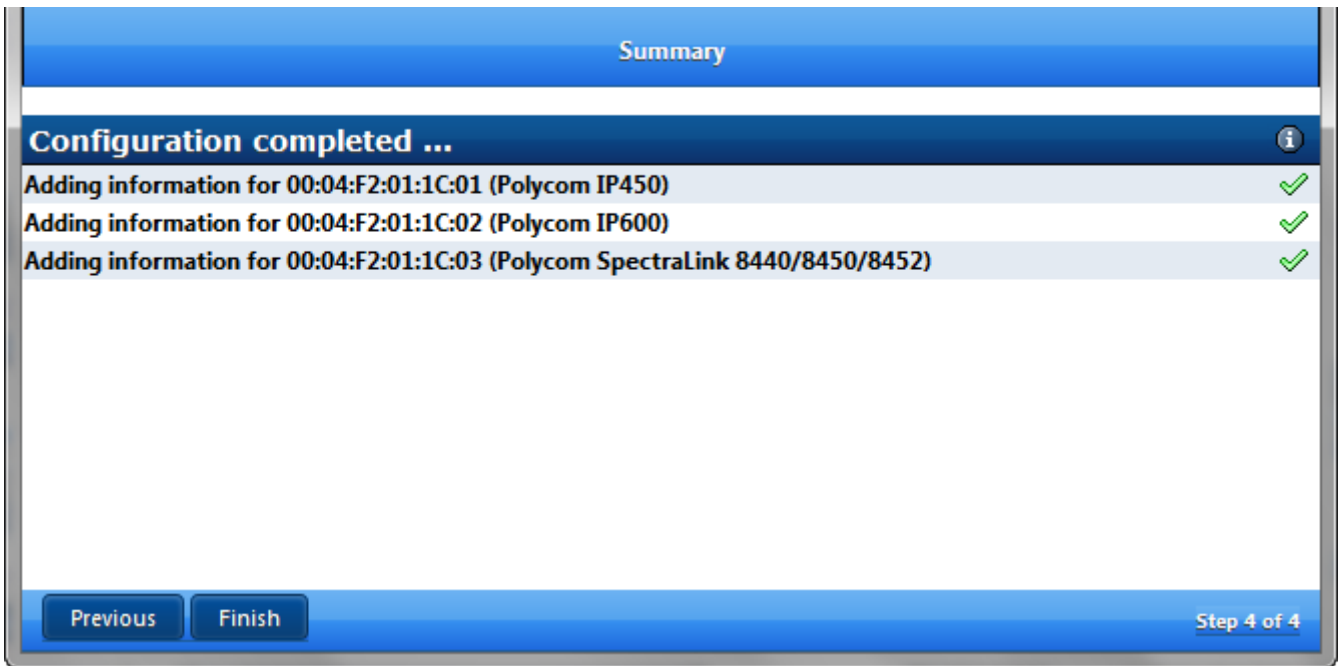
Automatic Addition of Supported Devices via DHCP Classes

Pre-requisites :

Network Module Pre-requisites :

- Network>DHCP Server must be enabled and properly configured

By creating DHCP Classes a default list of supported devices will be added by known Vendor ID.

- Each Class will use default provisioning options for each supported hardware vendor

- This simplifies the editing of options like TFTP option 66 or 150 depending on vendor

After creating the Default Classes the Classes must be added to the DHCP Subnet

DHCP Server:

| Configuration | **Subnet** | Dynamic DHCP | Static DHCP | Classes |

Subnet

| General | DNS Configuration | **Classes** | DHCP Options |

Include DHCP Classes:
- ☑ AASTRA_00085D
- ☑ AUDIOCODES_00908F
- ☑ CISCO_00036B
- ☑ CISCO_00036C
- ☑ GRANDSTREAM_000B82
- ☑ LINKSYS_000C41
- ☑ LINKSYS_000E08
- ☑ LINKSYS_000F66
- ☑ LINKSYS_001A70
- ☑ LINKSYS_001C10
- ☑ LINKSYS_001D7E
- ☑ LINKSYS_001EE5
- ☑ LINKSYS_001217
- ☑ LINKSYS_001310
- ☑ LINKSYS_0014BF
- ☑ LINKSYS_0016B6
- ☑ LINKSYS_0018F8
- ☑ LINKSYS_001839
- ☑ LINKSYS_002129
- ☑ LINKSYS_00226B
- ☑ LINKSYS_002369
- ☑ LINKSYS_00259C
- ☑ POLYCOM_0004F2
- ☑ SIPURA_1CDF0F
- ☑ SNOM_000413
- ☑ SWISSVOICE_000590
- ☑ YEALINK_001565

Select all, Select none, Invert selection

- Commit Network changes
- Restart the DHCP Server Service to enable the changes

| General | Network | Firewall | Traffic Shaper | DHCP Server | DNS Server | VPN Client/Server | Radius Server | Options | | Commit |

ⓘ You must click on Commit button in order to apply Change.

Services Status:

Network: Running	Restart Network	
Firewall: Running	Restart Service	Stop Service
Traffic Shaper: Service Disabled		
DHCP Server (IPv4): Running	Restart Service	Stop Service
Dynamic DNS: Service Disabled		
DNS Server: Running	Restart Service	Stop Service
VPN Server (PPTP): Service Disabled		
OpenVPN Client/Server: Service Disabled		
Radius Server (AAA): Service Disabled		

| Edit Services | Refresh |

Telephony Module Pre-requisites :

- Telephony>Configuration>Channels>SIP Channel>Auto-Create Peers=yes
- WARNING Auto-Create Peers can be vulnerable to malicious SIP attacks so the server should not have SIP ports exposed to the public (firewall your SIP ports to external subnets and follow SCOPSERV security best practices)

Telephony Settings: Channels

| Configuration | Channels | Language | Time Zones | Asterisk Manager | Monitoring | Scheduled Tasks | Hangup Causes | Synchronization |

Channels

| General | RTP Options | Codecs | SIP Channel | IAX Channel | UDPTL (T.38) | Jitter Buffer | Guest Account |

Port (UDP):	5060
Bind Address (UDP):	
Enable support for SIP TCP ?:	No
Enable support for SIP TLS (secure) ?:	No
Enable Outbound Proxy support ?:	No

SIP Options

Realm for Digest Authentication:	scopserv
User Agent:	Asterisk PBX (ScopServ)
Record SIP History:	No
Auto-create Peers:	Yes
Enable RTP Auto Framing ?:	No
Enable DNS SRV lookups on outbound calls:	No
Max length of incoming registration:	3600
Default length of incoming/outgoing registration:	120

- Telephony>Configuration>Provisioning
- Change the Unprovisioned Feature PIN to a complex number for security
- Enter the SIP Server address required for registration
- Save and Commit changes

Telephony Settings: Configuration

| Configuration | Channels | Language | Time Zones | Asterisk Manager |

Configuration

| General | Telephony Modules | Advanced Modules | Commit Menu | Feat |
| Recording/Monitoring | Sound Manager | Provisioning | Security |

Unprovisioned Feature PIN	7788
Default SIP Server:	172.16.74.1

Edit

USAGE

- Plug a supported SIP device into the voice subnet
- Wait for it to boot (it may reboot after it downloads its configuration from the server for the first time)
- Once the phone boots up you should see its MAC address in the APS list as an unprovisioned device
- Once the phone displays UNPROV on its display you can begin the registration process
- Dial any phone number to hear the password prompt
- Enter the Provisioning PIN number defined in Telephony>Configuration>Provisioning using the keypad
- Enter a defined but unused extension number using the keypad when prompted

- Edit the MAC address in the APS list and change any required settings like the template used, name, soft key assignments etc .

- Commit

- Reboot the phone to download the final configurations