



VOSS Insights Install Guide

Jan 14, 2022

Legal Information

Please take careful note of the following legal notices:

- Copyright © 2022 VisionOSS Limited.
All rights reserved.
- VOSS, VisionOSS and VOSS Automate are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

Contents

- 1 VMWare Specification and Requirements 1**
 - 1.1 Dashboard Reporting VM Sizing Specifications 1
 - 1.2 Arbitrator VM Sizing Specifications 2
 - 1.3 Arbitrator Correlation Consolidation VM Sizing Specifications 3
 - 1.4 DS-9 Netflow VM Sizing Specifications 3
 - 1.5 Raptor Call Path Generation VM Sizing Specifications 4

- 2 Port Requirements 5**
 - 2.1 Correlation and Dashboard System Connectivity 5
 - 2.2 Cisco UC Monitoring System Connectivity 5
 - 2.3 MS Teams System Connectivity 6
 - 2.4 Netflow and DS9 Monitoring System Connectivity 6
 - 2.5 VOSS Automate Port Usage 7
 - 2.6 Skype for Business Monitoring System Connectivity 7

- 3 Deploy 8**
 - 3.1 Deploy and VM Installation Steps 8

- 4 Networking Setup 11**
 - 4.1 Arbitrator Networking Setup 11
 - 4.2 Dashboard Reporter Networking Setup 13

- 5 Database and System Setup 14**
 - 5.1 VOSS Automate Database Setup 14
 - 5.2 Install Arbitrator System 16
 - 5.3 Set up Arbitrator to Arbitrator Communication 21
 - 5.4 Install Dashboard System 24

- 6 Certificates 27**
 - 6.1 Add Certificates 27

- 7 CUCM Asset Onboarding 28**
 - 7.1 Customer Onboard 28
 - 7.2 Call Manager Configuration 42

1. VMWare Specification and Requirements

1.1. Dashboard Reporting VM Sizing Specifications

Size	Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Storage (Gb)	Storage Spec	Network
Up to 5k users	8	2,8	16	500	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
5k to 20k users recom- mended option	12	2,8	32	500	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
20k to 40k users	16	2,8	128	500/1000	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB

- The specs for 5k up to 20k users is the recommended option.

1.2. Arbitrator VM Sizing Specifications

Size	Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Storage (Gb)	Storage Spec	Network
Up to 10k	8	2,8	64	1000	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
10k to 30k	16	2,8	64	1000	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
>30k up to 60K recom- mended option	16	2,8	128	1000	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB

- The specs for >30k up to 60k users is the recommended arbitrator specification option.

Scalability questions to consider:

- Number of log devices
- Number of devices
- Number of users
- Number of Datacentres
- Storage retention Period
- Other Data external Data Sources
- System intergration
- Archiving requirements
- Local attached storage an not Network attached

Notes:

- The CPU an RAM needs to be reserved a top priority (all the cores and memory)
- Bandwidth between devices an Arbitrator needs to capable of data flows

1.3. Arbitrator Correlation Consolidation VM Sizing Specifications

Arbitrator Correlation Consolidation recommended option:

Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Storage (Gb)	Storage Spec	Network
16	2,8	128	1000	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB

Scalability questions to consider:

- Number of devices
- Number of flows per second
- Storage retention Period
- Local attached storage and not Network attached

Notes:

- The CPU an RAM needs to be reserved a top priority (all the cores and memory)
- Bandwidth between devices an Arbitrator needs to capable of data flows

1.4. DS-9 Netflow VM Sizing Specifications

Size	Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Storage (Gb)	Storage Spec	Network
Small	12	2,8	32	500	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
Medium	16	2,8	64	500	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
Large	16	2,8	64	500	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB

Scalability questions to consider:

- Number of devices
- Number of flows per second

- Storage retention Period
- Local attached storage an not Network attached

Notes:

- Larger then 200k flows per second requires distributed netflow servers
- The CPU and RAM needs to be reserved at top priority (all the cores and memory)
- Bandwidth between devices and Arbitrators needs to capable of data flows
- The CPU an RAM needs to be reserved a top priority (all the cores and memory)
- Bandwidth between devices an Arbitrator needs to capable of data flows

1.5. Raptor Call Path Generation VM Sizing Specifications

1.5.1. Raptor Server

Size	Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Storage (Gb)	Network
Per Server	1	2	2	30	100MB

1.5.2. Raptor Client

Size	Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Storage (Gb)	Network
Per client	1	2	2	30	100MB

2. Port Requirements

2.1. Correlation and Dashboard System Connectivity

This table includes connectivity requirements between VAA Arbitrator, Reporting Dashboard, as well as connectivity between these and the following: VOSS Automate, NTP, DNS and AD.

Source	Destination	Port / protocol	Notes
Correlation Server / Dashboard Server	Correlation Server / Dashboard Server	5432, 5433, 5000, 60514, 64514, 64515, 65515, 65516, 64005, 64004, 62009, 62010 (all TCP)	Note: Intra-system communication and queries – Bi-directional
Correlation Server	Correlation Server	62002, 62003, 62004, 62005, 62006, 11501,30501, 30503, 40501, 40503 (all TCP)	Note: VOSS Fabric TLS tunnel Connection Ports – Bi-directional between Customer systems and NOC systems for event forwarding
Correlation Server / Dashboard Server	Network Resources (NTP, DNS)	53, 123 UDP	Time and DNS
Client PC – GUI Interface and CLI Management Access	Correlation Server / Dashboard Server	443, 8443, 22, 80 TCP	User Interface Access
VOSS Automate	Dashboard Server	27020	Database access
Correlation Server / Dashboard Server	AD	389 636 TCP UDP	Authentication

2.2. Cisco UC Monitoring System Connectivity

Source	Destination	Port / protocol	Notes
Monitored Cisco UC system	Correlation Server / Dashboard Server	514 tcp/udp, 22 tcp, 162 udp	Cisco syslog, snmp trap, CDR/CMR file transfer
Correlation Server	Monitored Cisco UC system	443 tcp, 8443 tcp, 22 tcp, 21 tcp, 161 udp	Correlation server AXL query, ssh and snmp query

2.3. MS Teams System Connectivity

Source	Destination	Port / protocol	Notes
MS Teams - Cloud Agent	Cloud Arbitrator	5432 tcp 443 tcp	Collects data from the MS Teams Tenant to the arbitrator
Cloud Arbitrator	Dashboard Server	5432 tcp	Pushes data to the dashboard to display dashboard data
Client PC – GUI Interface and CLI Management Access	Correlation Server / Dashboard Server	443, 8443, 22, 80 TCP	User Interface Access

2.4. Netflow and DS9 Monitoring System Connectivity

2.4.1. Communication ports between Netflow Source and DS9

Source	Destination	Protocol	Port	Direction	Description
Netflow Source	DS9	UDP	9996	Unidirectional	Netflow v5 (Optional)
DS9	Netflow Source	UDP	161	Unidirectional	SNMP queries

2.4.2. Communication ports between the DS9 Server and Dashboard Server

Unless the DS9 and Dashboard Servers are located in the same subnet, system administrators need to ensure the following network ports are open between these two components.

Source	Destination	Protocol	Port	Direction	Description
Dashboard Server	DS9	TCP	8082	Unidirectional	Data repository access
DS9	Dashboard Server	TCP	443	Unidirectional	DS9 System Stats
DS9	Dashboard Server	UDP	514	Unidirectional	DS9 System Logs

2.5. VOSS Automate Port Usage

VOSS Automate port usage for each node type:

Protocol	Ports	WebProxy node	Application node	Database node
ssh / sFTP	TCP 22	X	X	X
http	TCP 80	X	X	
https	TCP 443, 8443	X	X	
snmp	TCP/UDP 161, 162	X	X	X
mongodb	TCP 27017, 27030		X	
mongodb	TCP 27019, 27020			X
LDAP	TCP/UDP 389 (636 TLS/SSL)		X	
NTP	UDP 123		X	
SMTP	TCP25		X	X

2.6. Skype for Business Monitoring System Connectivity

Source	Destination	Port / protocol	Notes
VOSS Forwarder installed on Windows Machine	Customer SfB Monitoring Server (SQL)	1433	Collection of CDR/QoS Data. SfB monitoring server is typically deployed on the SfB Front-End Server (Option 1)
VOSS Forwarder installed on Windows Machine	Separate Customer SfB Reporting Server - QoE DB (SQL)	1433	Collection of CDR/QoS Data from the Reporting (QoE) Server that is a replication of the SfB Monitoring Server (Option 2)
VOSS Forwarder installed on Windows Machine	Arbitrator Correlation	62009-62010, 514	Management and Syslog Traffic
VOSS Forwarder installed on Windows Machine	Dashboard / Reporting	62009-62010, 5432-5433, 80, 443, 514, 1194	Management and Syslog Traffic
SfB Monitoring Server	Dashboard / Reporting	1433	SQL Transactional Data Replication
SfB Monitoring Server	Arbitrator Correlation	80, 443	SDN Traffic
SfB Monitoring Server	Dashboard / Reporting	80, 443	SDN Traffic

3. Deploy

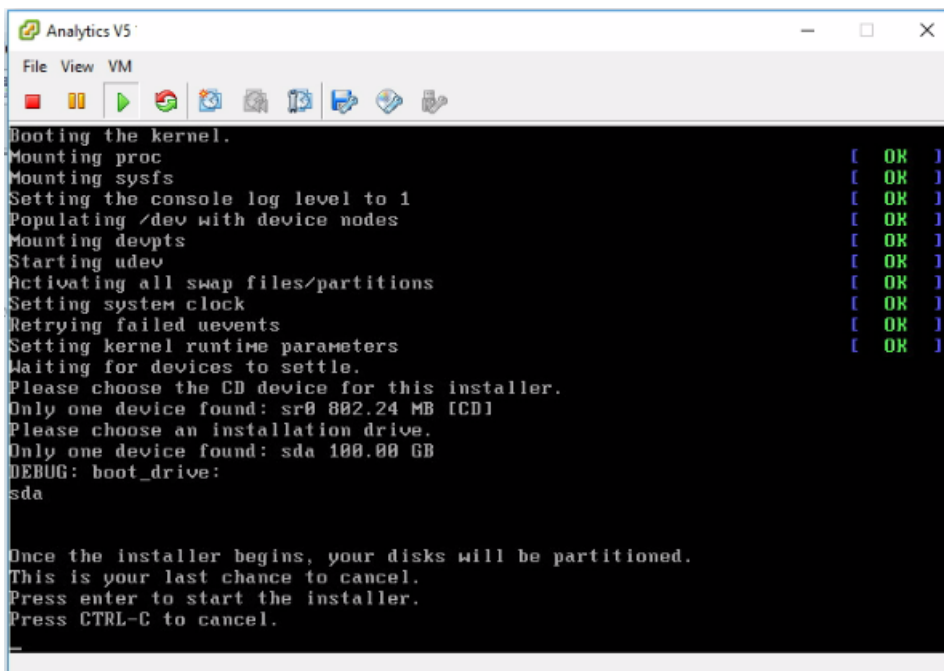
3.1. Deploy and VM Installation Steps

1. Download the ISO to directory accessible by the VSphere client.
2. In the vSphere client, create a new Debian Linux 64-bit guest operating system VM with:
 - disk space
 - RAM
 - vCPU

according to the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements*.

Choose a VM name, for example “VAA”.

3. Attach the downloaded ISO to the CD/DVD drive. For Device Status, select Connect at power on. Make sure that the CD/DVD drive with the attached ISO is set to boot first.
4. Power on the VM.
5. You will be prompted with the following message:



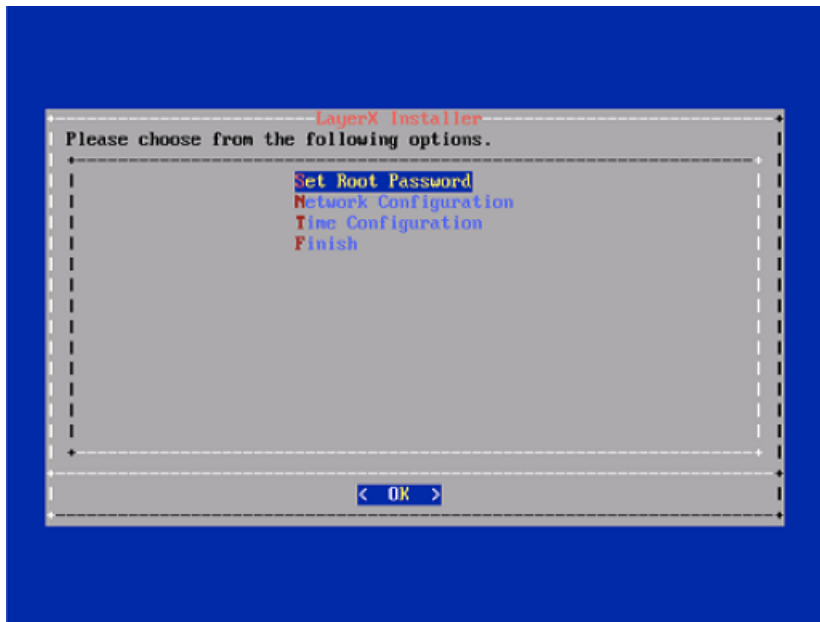
```
Analytics VS
File View VM
Booting the kernel.
Mounting proc [ OK ]
Mounting sysfs [ OK ]
Setting the console log level to 1 [ OK ]
Populating /dev with device nodes [ OK ]
Mounting devpts [ OK ]
Starting udev [ OK ]
Activating all swap files/partitions [ OK ]
Setting system clock [ OK ]
Retrying failed uevents [ OK ]
Setting kernel runtime parameters [ OK ]
Waiting for devices to settle.
Please choose the CD device for this installer.
Only one device found: sr0 802.24 MB [CD]
Please choose an installation drive.
Only one device found: sda 100.00 GB
DEBUG: boot_drive:
sda

Once the installer begins, your disks will be partitioned.
This is your last chance to cancel.
Press enter to start the installer.
Press CTRL-C to cancel.
```

6. Press <Enter> (to start install) or <Ctrl> + C to exit.
7. You will see .lxp packages being installed. This takes a while.

```
Info: install_package : Unpacking /mnt/cd/pkg/iana-etc.lxp
Info: install_package : Unpacking /mnt/cd/pkg/nan-pages.lxp
Info: install_package : Unpacking /mnt/cd/pkg/attr.lxp
Info: install_package : Unpacking /mnt/cd/pkg/bc.lxp
Info: install_package : Unpacking /mnt/cd/pkg/berkeley-db.lxp
Info: install_package : Unpacking /mnt/cd/pkg/bglibs.lxp
Info: install_package : Unpacking /mnt/cd/pkg/bridge-utils.lxp
Info: install_package : Unpacking /mnt/cd/pkg/dhcpd.lxp
Info: install_package : Unpacking /mnt/cd/pkg/diffutils.lxp
Info: install_package : Unpacking /mnt/cd/pkg/dnapi.lxp
Info: install_package : Unpacking /mnt/cd/pkg/ethtool.lxp
Info: install_package : Unpacking /mnt/cd/pkg/expat.lxp
Info: install_package : Unpacking /mnt/cd/pkg/gmp.lxp
Info: install_package : Unpacking /mnt/cd/pkg/iso9660.lxp
Info: install_package : Unpacking /mnt/cd/pkg/ndadm.lxp
Info: install_package : Unpacking /mnt/cd/pkg/ncurses.lxp
Info: install_package : Unpacking /mnt/cd/pkg/net-tools.lxp
Info: install_package : Unpacking /mnt/cd/pkg/patch.lxp
Info: install_package : Unpacking /mnt/cd/pkg/paxctl.lxp
Info: install_package : Unpacking /mnt/cd/pkg/perl-SSLey.lxp
Info: install_package : Unpacking /mnt/cd/pkg/popt.lxp
Info: install_package : Unpacking /mnt/cd/pkg/speex.lxp
Info: install_package : Unpacking /mnt/cd/pkg/strace.lxp
Info: install_package : Unpacking /mnt/cd/pkg/tar.lxp
```

8. After all the packages are installed you will automatically be presented with a basic configuration.



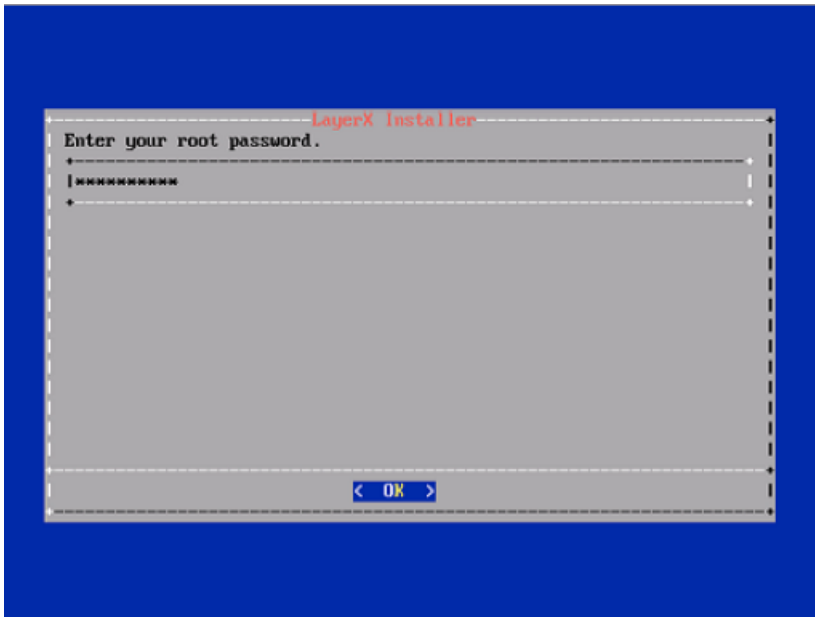
This allows you to set the following:

- Root Password
- Hostname
- IP Configuration
- DNS
- Time

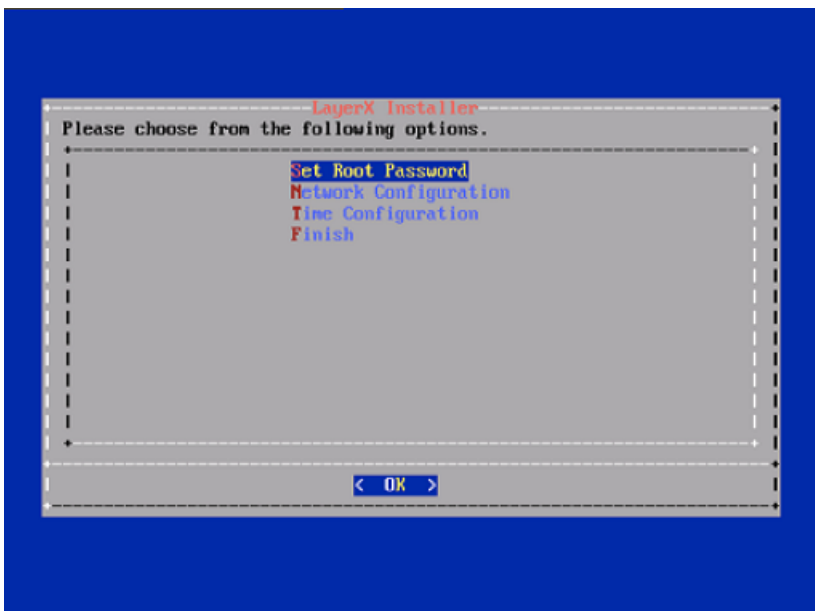
Navigate to each of the setup screens using the following keys:

- <Up> Arrow key

- <Down> Arrow key
 - <TAB>
 - <Enter>
9. To set the root password use the <Up> and <Down> arrow keys until Set Root Password is highlighted. Then press <Enter>.
 10. You will then be asked to type the Root Password twice.



11. After entering the new Root Password you will return to the Main configuration screen.

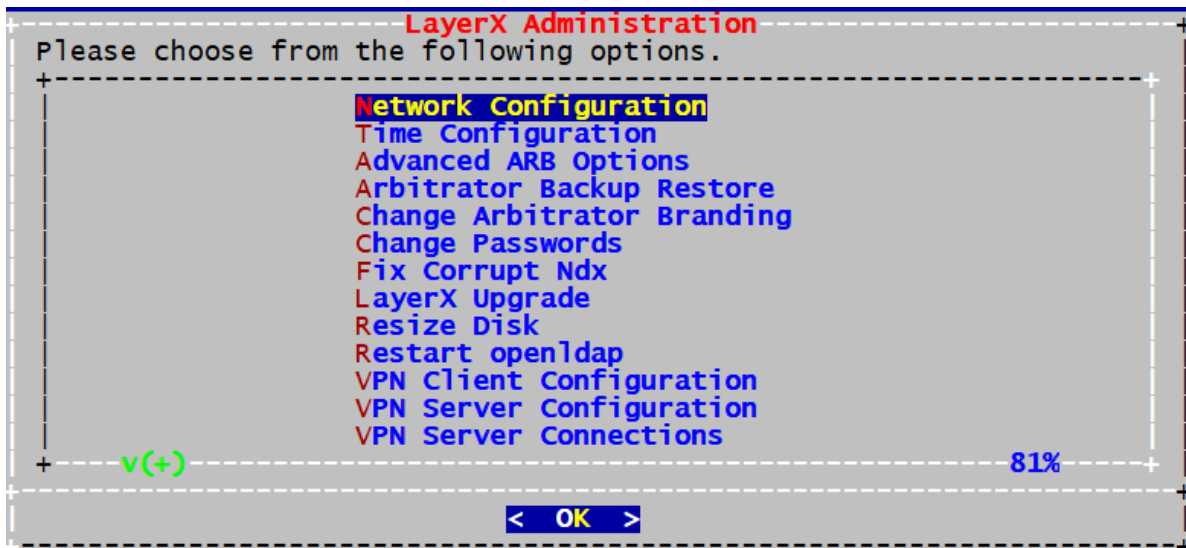


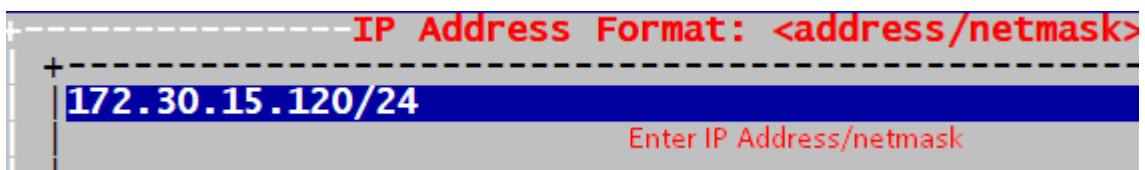
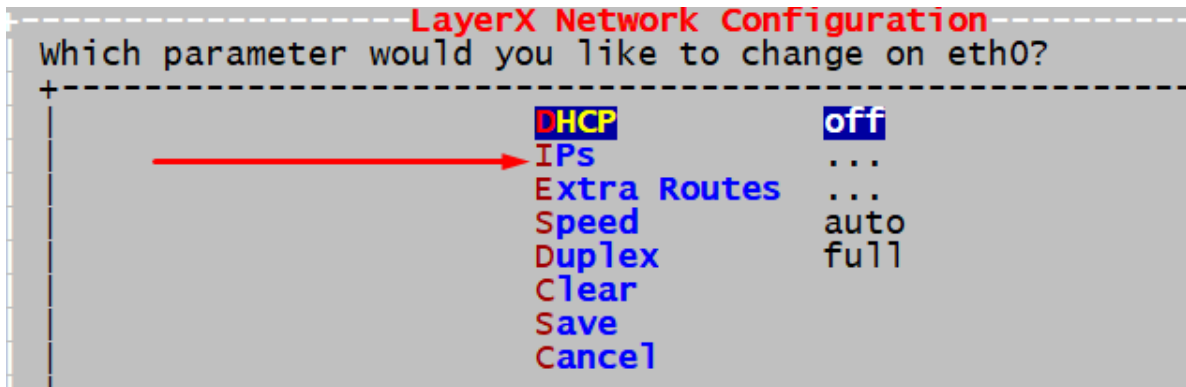
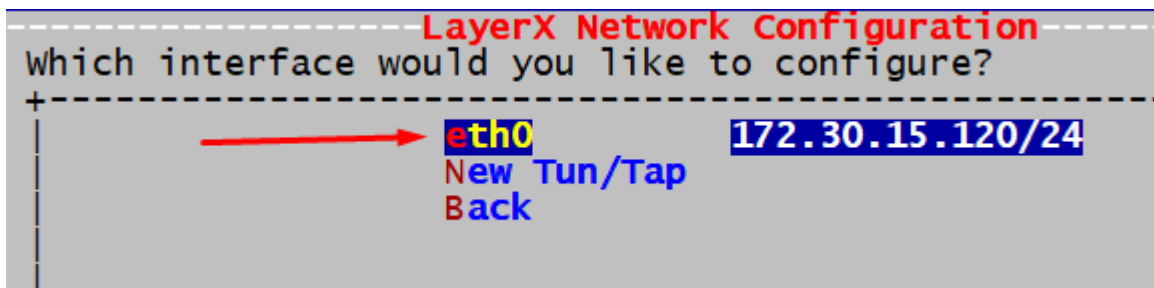
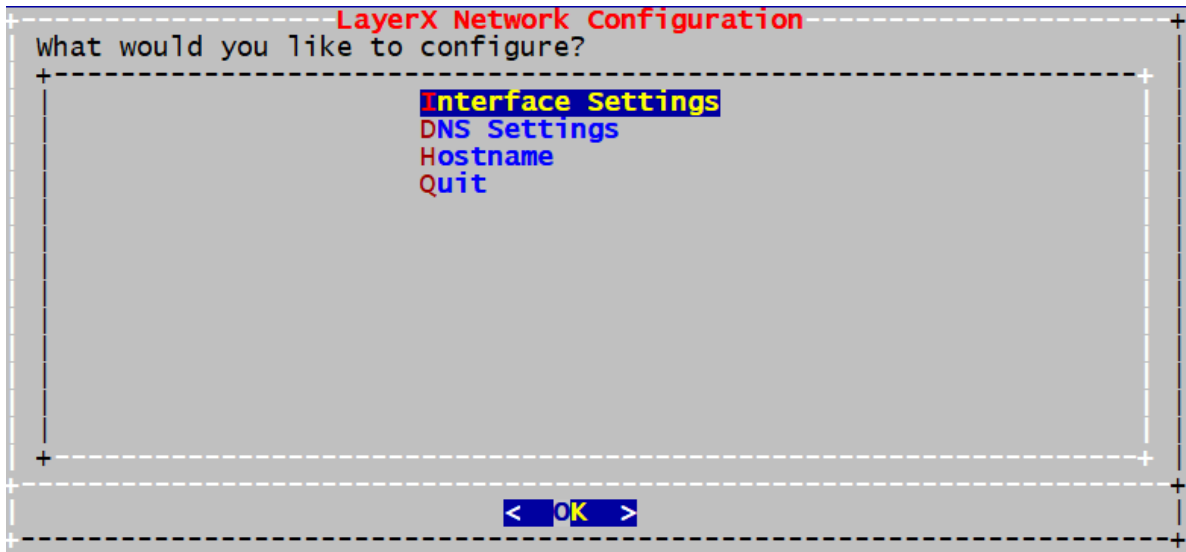
You can now proceed to the *Networking Setup* section in the VOSS Insights Install Guide.

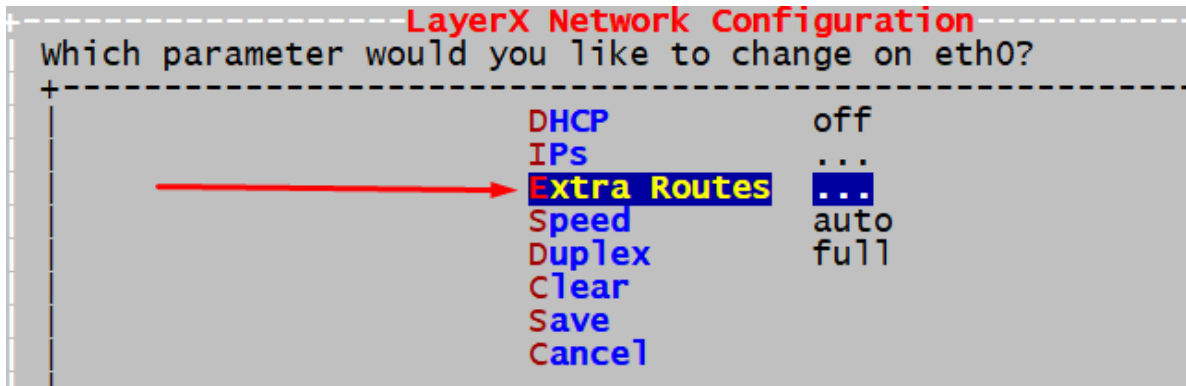
4. Networking Setup

4.1. Arbitrator Networking Setup

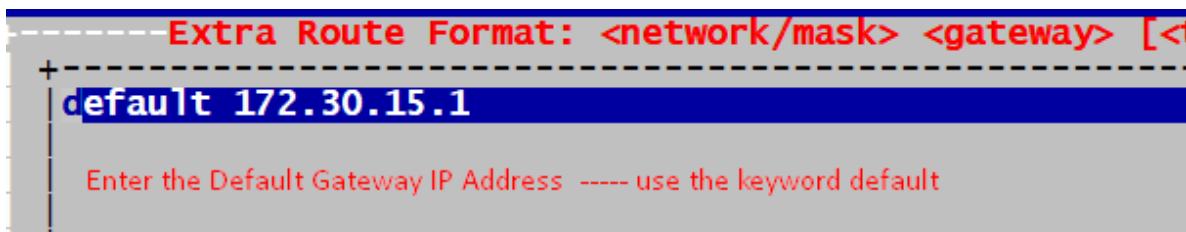
1. Deploy OVA Arbitrator
2. From the console login as `admin/admin`
3. Configure networking







- Once you have configured networking go back to Interface settings and set the hostname of the server and any DNS Settings.



- Save then Quit.

4.2. Dashboard Reporter Networking Setup

- Deploy OVA Dashboard/Reporter
- Repeat the *Arbitrator Networking Setup* steps to configure Network/Hostname and DNS for the Dashboard/Reporter.

5. Database and System Setup

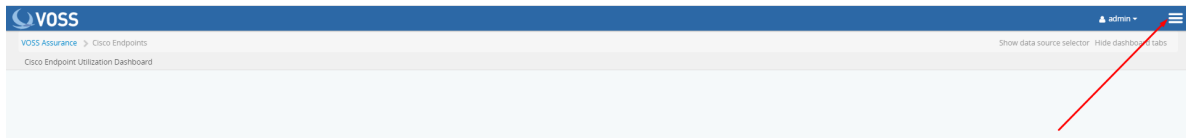
5.1. VOSS Automate Database Setup

1. Add a Database user - this is a Read only user

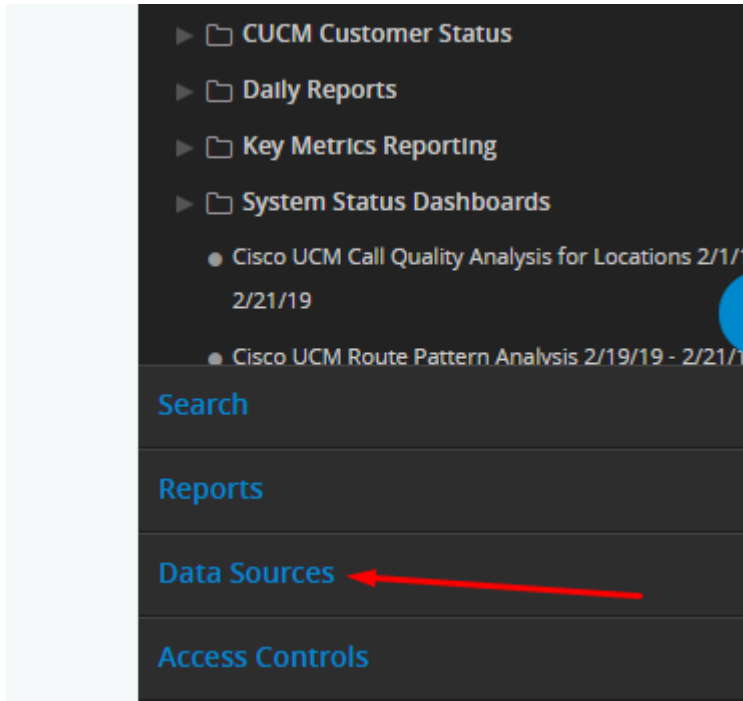
```
platform@gsr10-un1:~$ database user add 1.1.1.1 Analytix
```

IP Address of Dashboard Server

2. Take note of the username and password you have just configured
3. Now log in to the GUI on the Dashboard Server username admin — password admin
4. Click on the Hamburger Menu shown Below



5. Click on Data sources



6. Click on New Data Source

A screenshot of the 'Data Sources' configuration page. At the top, there is a dropdown menu showing '172.30.15.120'. Below it is a blue button labeled 'New Data Source' with a red arrow pointing to it. The form contains the following fields: 'Name' with the value '172.30.15.120', 'Data Source Type' with a dropdown menu showing 'Remote Arbitrator Postgres Database', and 'Host' with the value '172.30.15.120'.

7. Fill out the form presented.

Name	Name
<input type="text" value="test"/>	Enter a name for this data source.
Data Source Type	Data Source Type
<input type="text" value="Voss Mongo Database"/>	Select the data source type and fill in the fields below.
Ip	
<input type="text" value="localhost"/>	Set the IP Address of V4UC UNI
Port	
<input type="text" value="27020"/>	
Db	
<input type="text" value="VOSS"/>	
Username	
<input type="text" value="Analytix"/>	Username you set on V4UC
AuthSource	
<input type="text" value="VOSS"/>	Change the AuthSource From admin to VOSS
Password	
<input type="password" value="....."/>	Password you set on V4UC
Ssl	
<input type="text" value="true"/>	
Alias	
<input type="text"/>	

8. Repeat the process above to Add the Arbitrator as a Data Source

Name	Name
<input type="text"/>	Enter a name for this data source.
Data Source Type	Data Source Type
<input type="text" value="Remote Arbitrator Postgres Database"/>	Select the data source type and fill in the fields below.
Host	
<input type="text" value="localhost"/>	Set the IP Address of the Arbitrator
Port	
<input type="text" value="5432"/>	

5.2. Install Arbitrator System

5.2.1. Policy Configuration Files

Policies are a modular groupings of correlation rules, actions and response procedures that define how to respond to certain situations that happen on the monitored systems. Policies are usually system and manufacturer specific but can contain custom scripts for actions and response procedures. Each policy will also contain several correlation rules that are designed to create Alerts based on the best practices of that

particular system manufacturer.

The configuration files in this table are installed at the end of the installation process. The purpose of the components are:

- Controls

Controls are actions that the system can automate user actions to support data collection, analysis before presenting to an operational user as a alert to help reduce User input and provide information and actions faster.

- Turn a alarm a different colour
- Push alert to another system such as dashboard server or a correlation server
- Auto acknowledge alarms
- Email the alert to a destination
- Create a ticket with ServiceNow
- Pre scripted action based on a response

Other options that can be developed are:

- Using API send the data to another destination
- Interact with another system
- Run a script to collect additional information
- Run a script with actions to change state or configuration

- Probes

A probe is a script that is defined to poll a system to collect data from a remote system. This is important if the data required cannot be streamed from a system to the arbitrator to be ingested, the arbitrator and collect the data remotely by periodic probing of the system. Examples of probes that collect data

- AXL
- API
- CLI

- Response procedures

Contains group of controls that are assigned to the policies

- Policies

A policy is a set of rules for the data that is turned in a to an alert. It enables an alert to be generated and defines the alarm ID and the content of the alarm that gets presented to a user.

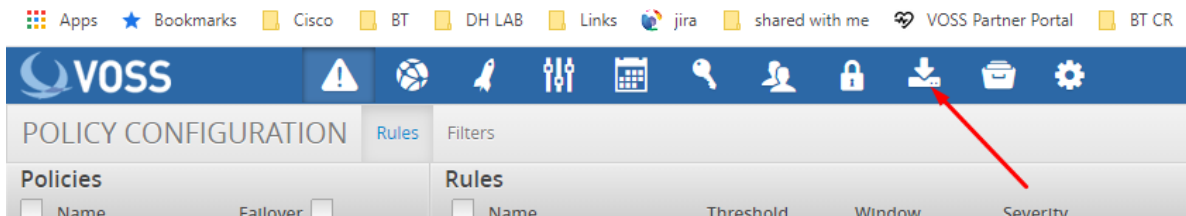
Component	Filename
Controls	STDCONTROLS.lxcfg
Probes	StandardDeploymentProbes.lxcfg PROBES.lxcfg
Response Procedures	
Policies	SiteStats_08122020.lxcfg POLICIESUCCE221020.lxcfg POLICIESCUCM221020.lxcfg POLICIESCUCIMP221020.lxcfg PINGMON.lxcfg

5.2.2. Installation Steps

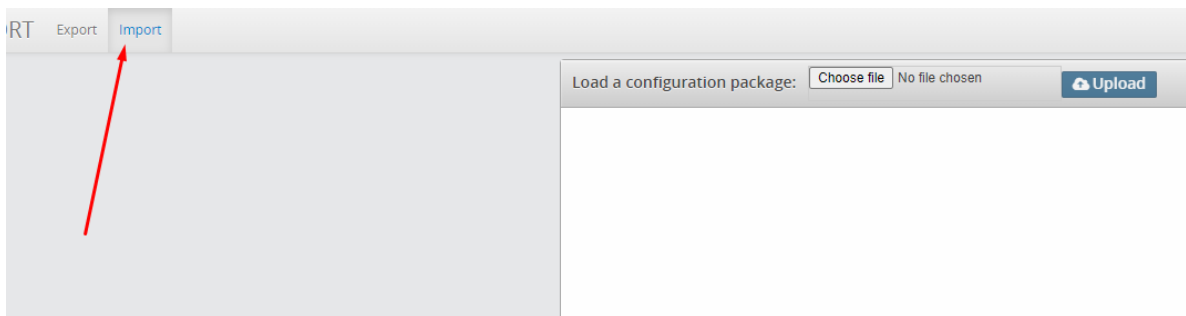
1. Log in to the Arbitrator: admin/admin
2. Click on the spanner icon



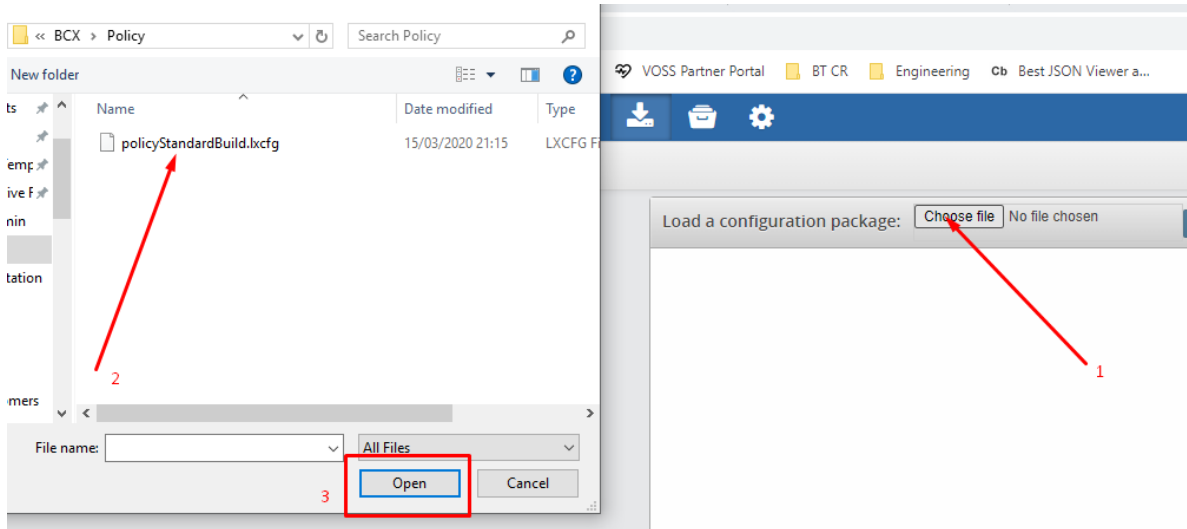
3. Click on the icon shown below



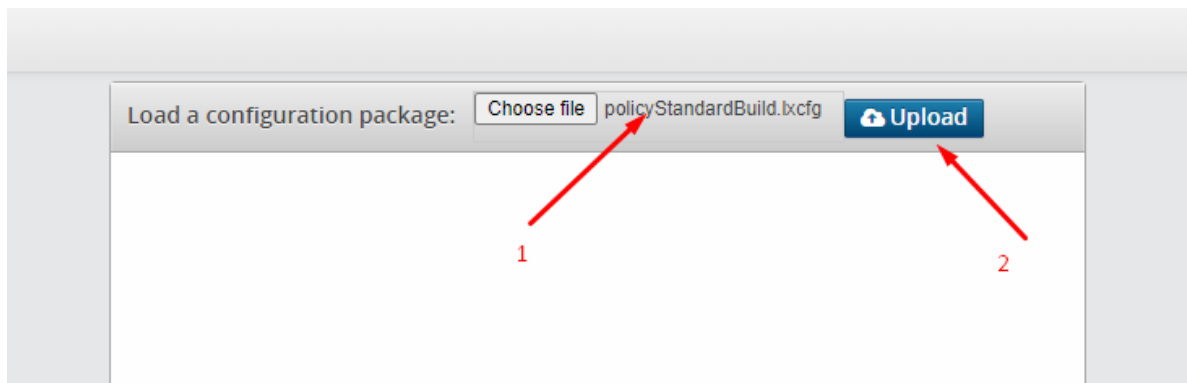
4. Click on **Import**



5. Click on **Choose file**, then select your file and click **OK**.



6. Ensure the file you have just selected shows next to choose file, then click **Upload**.



7. Once the file has uploaded click **Import**.

Load a configuration package: policyStandardBuild.lxcfg

Package Name:	policy153
Package Description:	policy153
Package Type:	backup
Package Date:	03/15/20 21:14

Updating Policy Module: Cisco CVP Alarms (Syslog)

Updating Policy Module: Cisco ICM Alarms (Syslog)

Updating Policy Module: Cisco UCCE - Error Events

Updating Policy Module: CUC_EvtCat

Updating Policy Module: CUC_LicCat

Updating Policy Module: CUC_SrmCat

Updating Policy Module: CUCM Media Resource Alarms

Updating Policy Module: Cucm_CmCat_Audit

Updating Policy Module: Cucm_CmCat_Capf

Updating Policy Module: Cucm_CmCat_Car

Updating Policy Module: Cucm_CmCat_CdrRep

Updating Policy Module: Cucm_CmCat_Cef

Updating Policy Module: Cucm_CmCat_CertMon

Updating Policy Module: Cucm_CmCat_Cm

Updating Policy Module: Cucm_CmCat_Cmi

Updating Policy Module: Cucm_CmCat_Ctlman

Updating Policy Module: Cucm_CmCat_Ils

Updating Policy Module: Cucm_CmCat_Ipvms

Updating Policy Module: Cucm_CmCat_Lbm

Updating Policy Module: Cucm_CmCat_Phone

Updating Policy Module: Cucm_CmCat_Tcdsrv

Updating Policy Module: Cucm_ImpCat_Upclstrsync

Updating Policy Module: Cucm_ImpCat_Uprepl

Updating Policy Module: Cucm_ImpCat_Upsconfig

Updating Policy Module: Cucm_ImpCat_Upspresence

Updating Policy Module: Cucm_ImpCat_Upsrecovery

8. Repeat this procedure for:

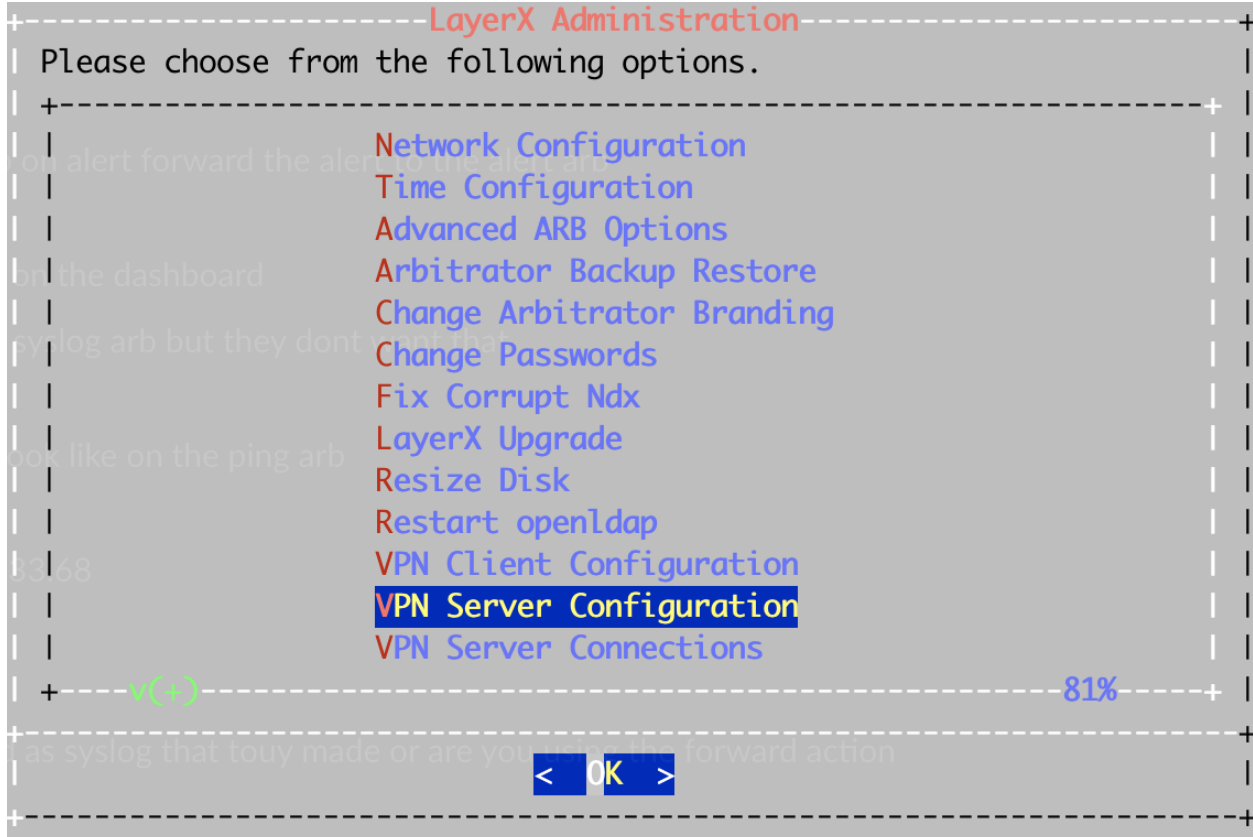
- **Controls**
- **Probes**

- **Response Procedures**
- **Policies**

See: *Policy Configuration Files*

5.3. Set up Arbitrator to Arbitrator Communication

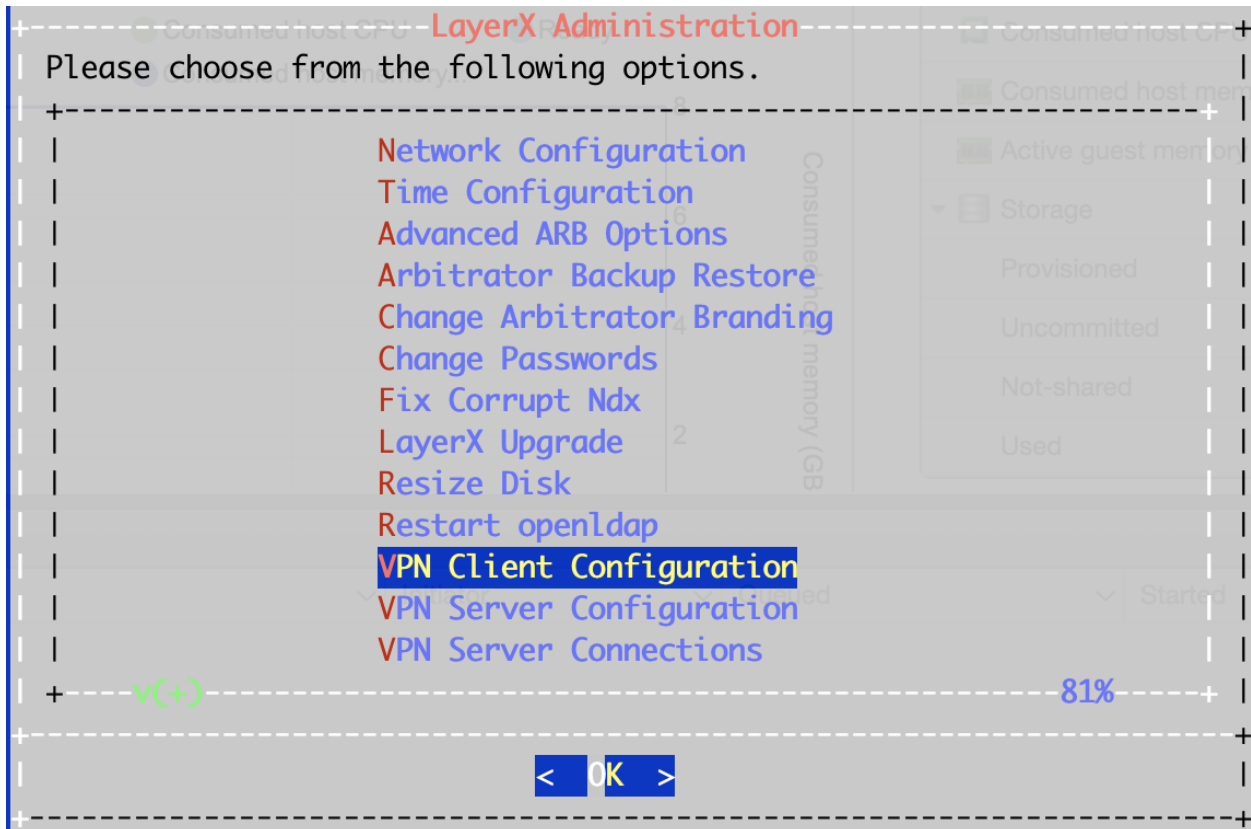
Log in as admin on the central/lead arbitrator and go to VPN Server Configuration



Then Clear Fabric Configuration, then reset this up:

- Set the Organization name
- Set The Public Ip Address (this is the address of the Arbitrator)
- Set Authorized Client Port to 62003
- Set the Negotiation Port to 62004
- Set the VPN Subnet (to a number between 1 and 150)
- Set the Ethernet Interface Number (Usually 0)

As shown in the example below:



1. Clear Fabric Configuration to remove any remnants of other tunnels
2. Then set the Server Address as the IP address of the Central/Lead Arbitrator
3. Ensure the Negotiation Port is set as 62004
4. Click **Done**.

A Tunnel will now be set up between the Arbitrators.

You can check this by running the following commands in CLI when logged in as root:

```
root@dharp1:~# netstat -ne | grep 3050
tcp        0      0 169.254.5.1:30501    169.254.5.6:18880    TIME_WAIT  0          0
tcp        0      0 169.254.5.1:30501    169.254.5.6:18920    ESTABLISHED 0        13090739
tcp        0      0 169.254.5.1:30501    169.254.5.6:18866    TIME_WAIT  0          0
tcp        0      0 169.254.5.1:23238    169.254.5.6:30503    TIME_WAIT  0          0
tcp        0      0 169.254.5.1:30501    169.254.5.6:18896    TIME_WAIT  0          0
tcp        0      0 169.254.5.1:23280    169.254.5.6:30503    ESTABLISHED 0        13097174
tcp        0      0 169.254.5.1:23166    169.254.5.6:30503    TIME_WAIT  0          0
root@dharp1:~#
```

The tunnel is setup using 169.253.x.x addresses:

```
root@dharp1:~# netstat -ne | grep 6200
tcp        0      0 192.168.58.42:62003  192.168.58.38:37680  ESTABLISHED 0        8520558
tcp        0      0 127.0.0.1:50688      127.0.0.1:62009     ESTABLISHED 0        24342
tcp        0      0 127.0.0.1:62009      127.0.0.1:50688     ESTABLISHED 0        19387
root@dharp1:~#
```

To set Alerts to be forwarded from the subordinate Arbitrators to the Central/Lead Arbitrator:

- On the Subordinate Arbitrator go to Response Procedures in the config area of the GUI:

Methods

Control Type: LinkIPToAlert ✎

Destination: As Event? Click here then click save

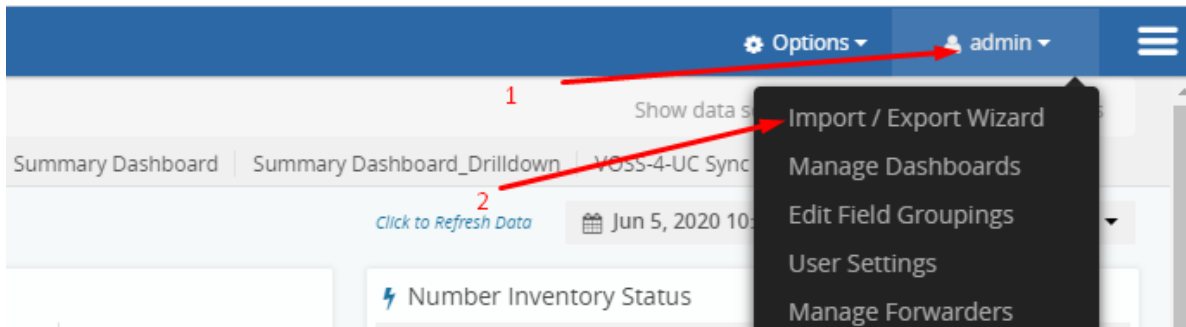
2. Insert the name of the Central ARB

Ensure as event is ticked

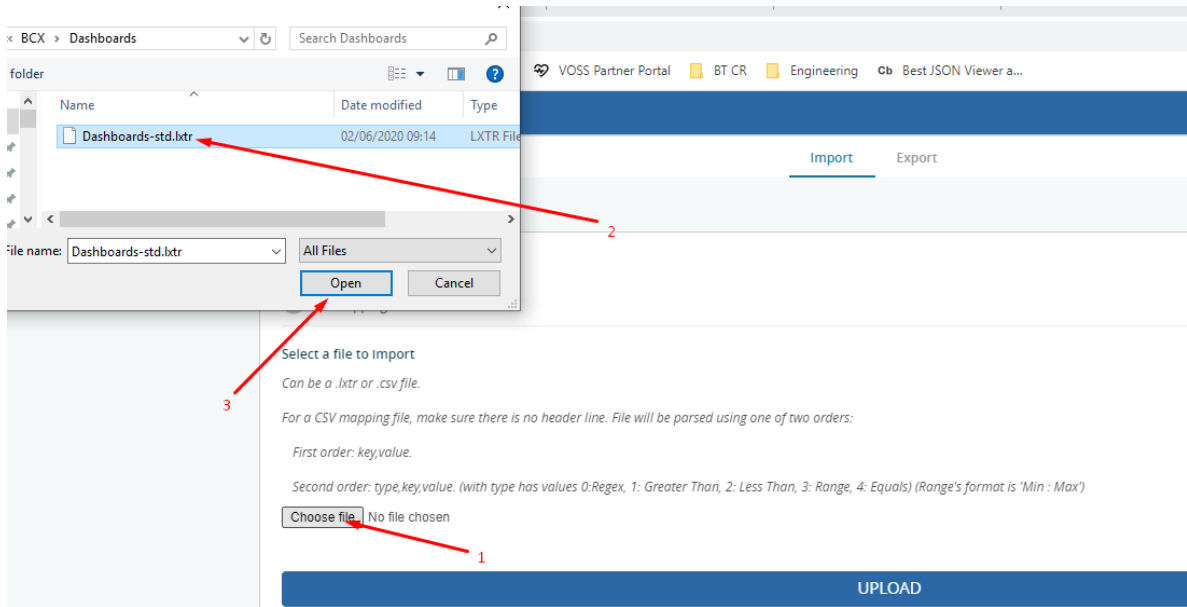
1. Click Forwarder to add

5.4. Install Dashboard System

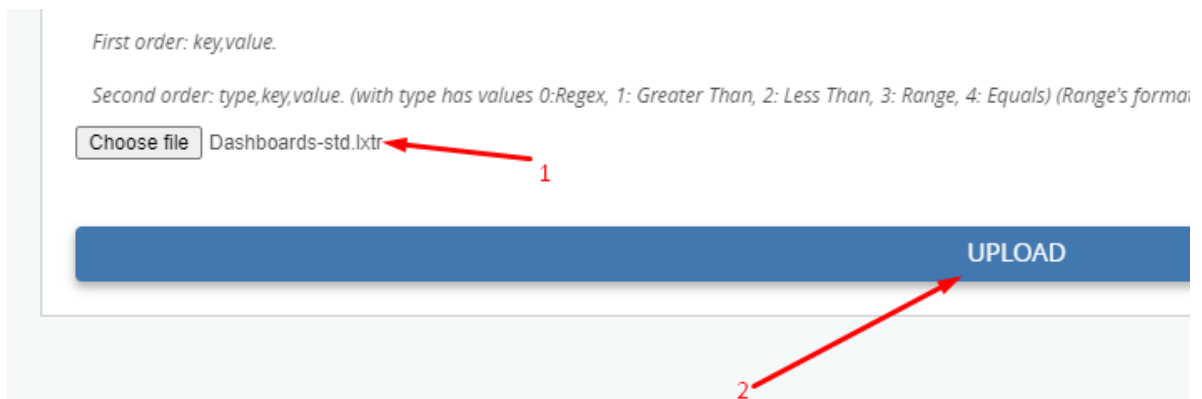
1. Access the Dashboard Server: `admin/admin`
2. In the top banner bar click on `admin`, then click on **Import/Export Wizard**.



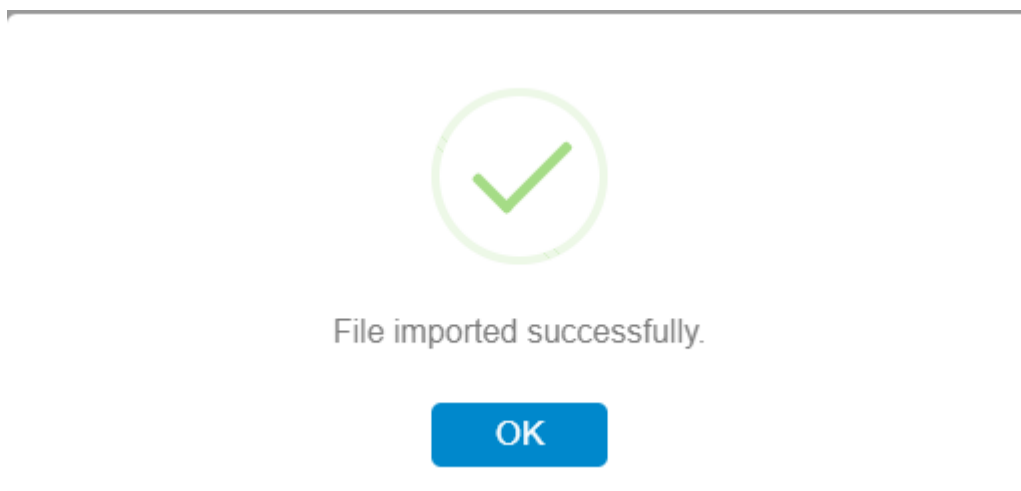
3. Click on **Choose file**, then navigate to the file you wish to import (dashboard files have the `.lxttr` file extension) then click **OK**.



4. Ensure your file is visible adjacent to **Choose file**, then click **Upload**.

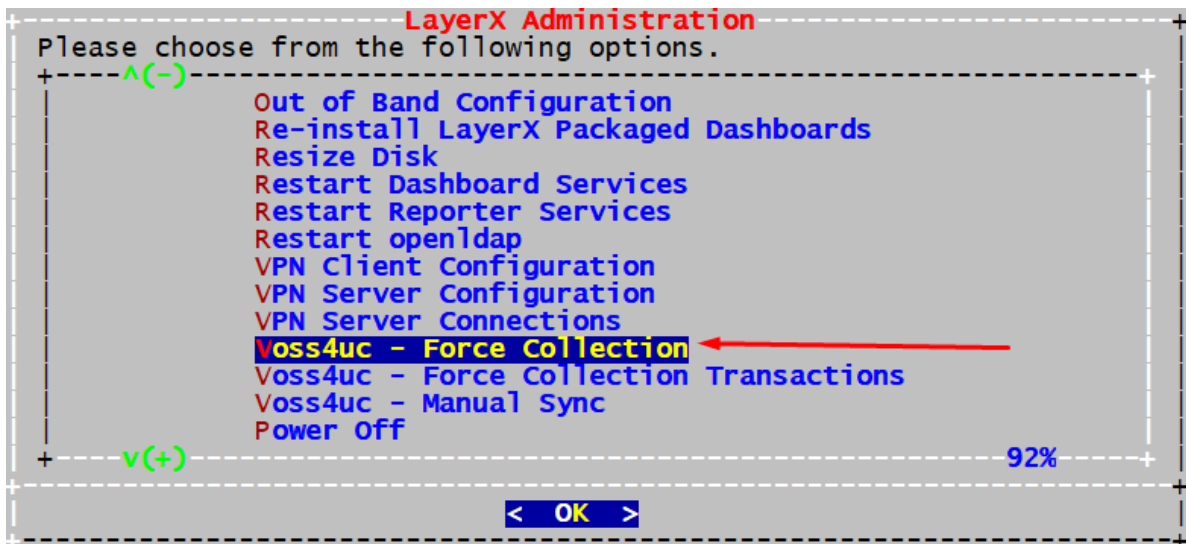


5. Your file will then upload, and you will see the below — click **OK**.



6. Log in to the Dashboard CLI as `admin/admin`.
7. Navigate down to **Voss4uc - Force Collection** and click **OK**. This will then sync VOSS Automate data

into the dashboard.



6. Certificates

6.1. Add Certificates

1. SCP the new `server.crt` and `server.key` files to the `etc/apache2/` directory on the system, overwriting the old certificate files.

Recommended: back up the current certificate files prior to overwriting them.

2. SSH to the system as `root` and restart the apache service using the **`sv restart apache`** command.
3. Clear browser cache.
4. Apache will now use the new signed certificate.

7. CUCM Asset Onboarding

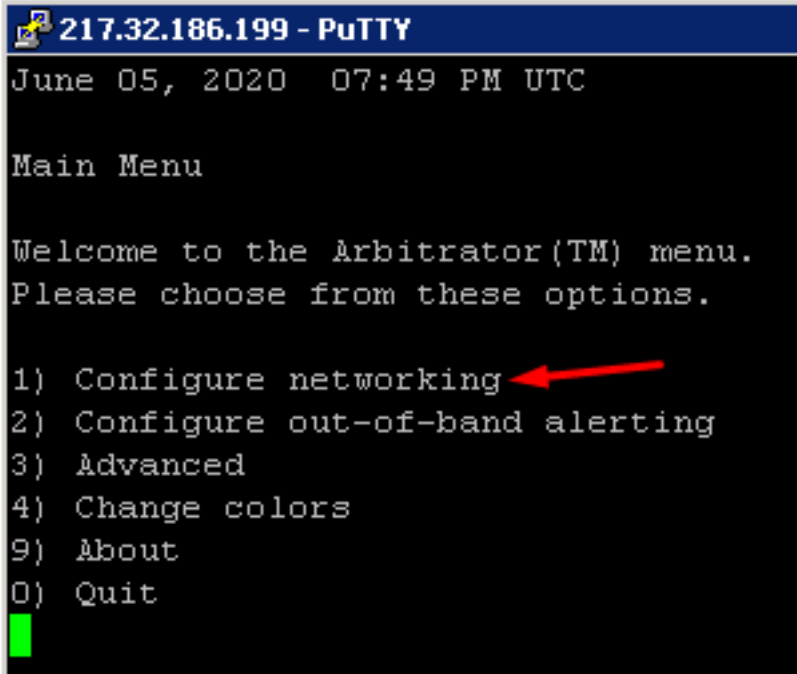
7.1. Customer Onboard

7.1.1. Add Customer CDR Folders

1. Log in via the command line interface to the Arbitrator selected to receive CDR data from the CUCM.
2. Use the admin credentials to log in.

```
-----LayerX Administration-----
Please choose from the following options.
-----
Network Configuration
Time Configuration
Advanced ARB Options
Arbitrator Backup Restore
Change Arbitrator Branding
Change Passwords
Fix Corrupt Ndx
LayerX Upgrade
Resize Disk
Restart openldap
VPN Client Configuration
VPN Server Configuration
VPN Server Connections
-----
v(+)                                     81%
-----
< OK >
```

3. Navigate to Advanced Arb Options (as shown above) and click ok.



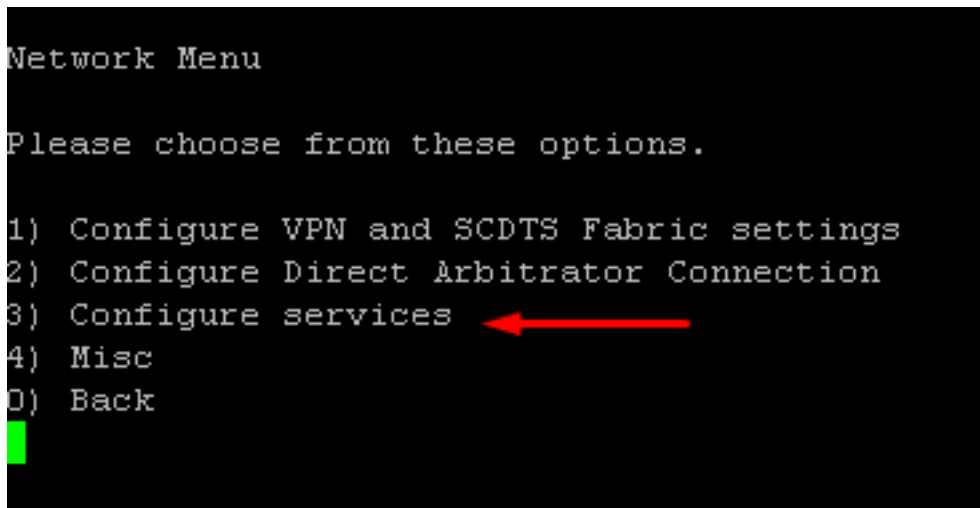
```
217.32.186.199 - PuTTY
June 05, 2020 07:49 PM UTC

Main Menu

Welcome to the Arbitrator(TM) menu.
Please choose from these options.

1) Configure networking
2) Configure out-of-band alerting
3) Advanced
4) Change colors
9) About
0) Quit
█
```

4. Now press 1.



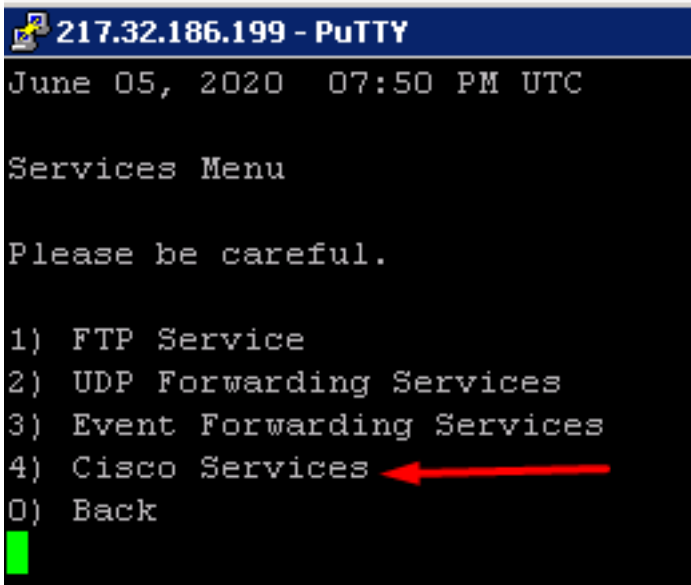
```
217.32.186.199 - PuTTY
June 05, 2020 07:49 PM UTC

Network Menu

Please choose from these options.

1) Configure VPN and SCDTS Fabric settings
2) Configure Direct Arbitrator Connection
3) Configure services
4) Misc
0) Back
█
```

5. Now press 3.



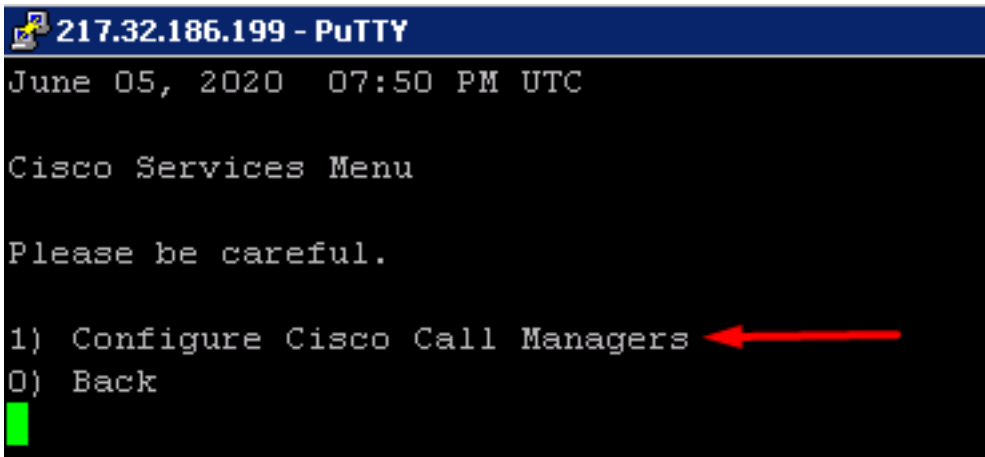
```
217.32.186.199 - PuTTY
June 05, 2020 07:50 PM UTC

Services Menu

Please be careful.

1) FTP Service
2) UDP Forwarding Services
3) Event Forwarding Services
4) Cisco Services
0) Back
```

6. Press 4.



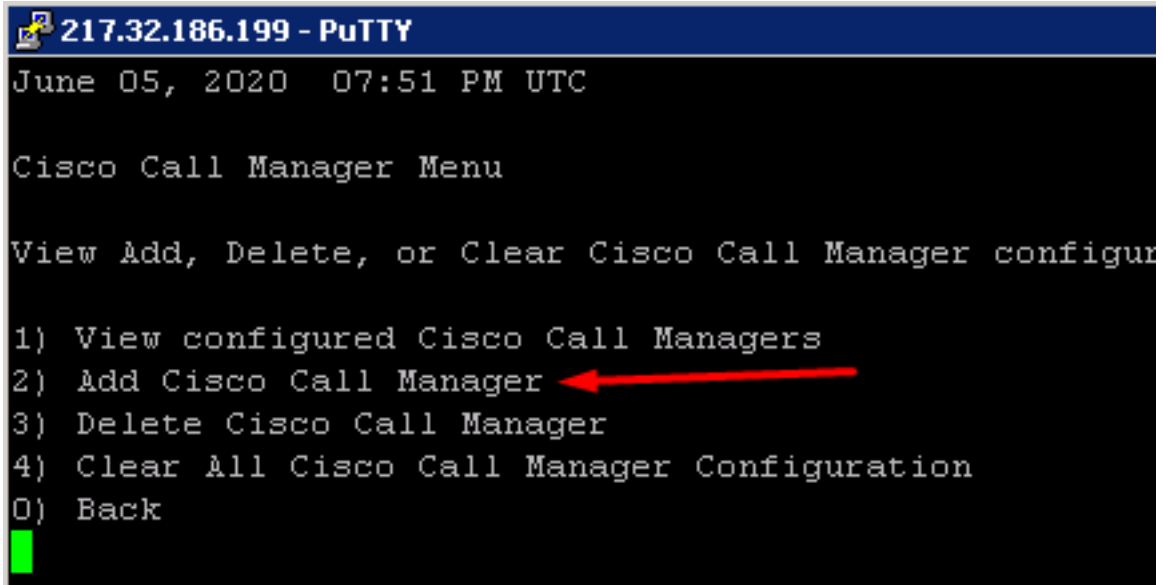
```
217.32.186.199 - PuTTY
June 05, 2020 07:50 PM UTC

Cisco Services Menu

Please be careful.

1) Configure Cisco Call Managers
0) Back
```

7. Press 1.



```
217.32.186.199 - PuTTY
June 05, 2020 07:51 PM UTC

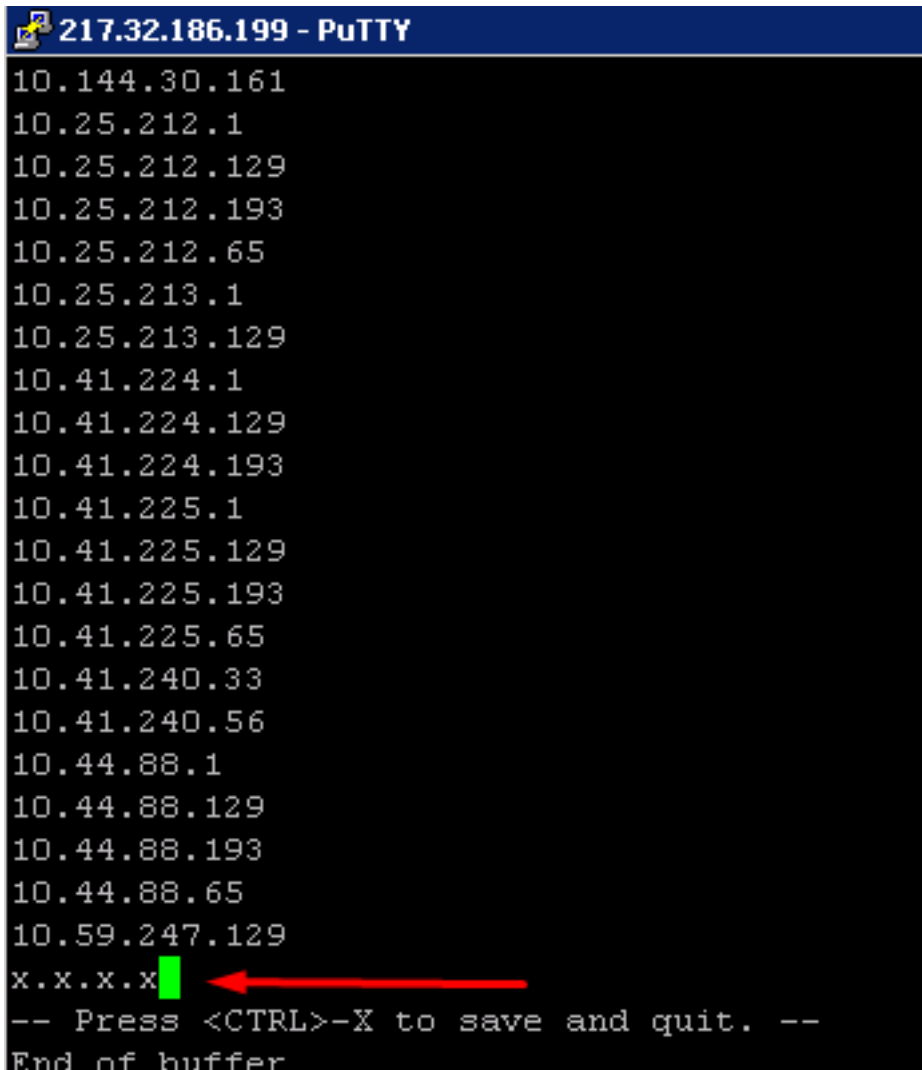
Cisco Call Manager Menu

View Add, Delete, or Clear Cisco Call Manager configur

1) View configured Cisco Call Managers
2) Add Cisco Call Manager
3) Delete Cisco Call Manager
4) Clear All Cisco Call Manager Configuration
0) Back
```

8. Press 2.

This will open the screen below.

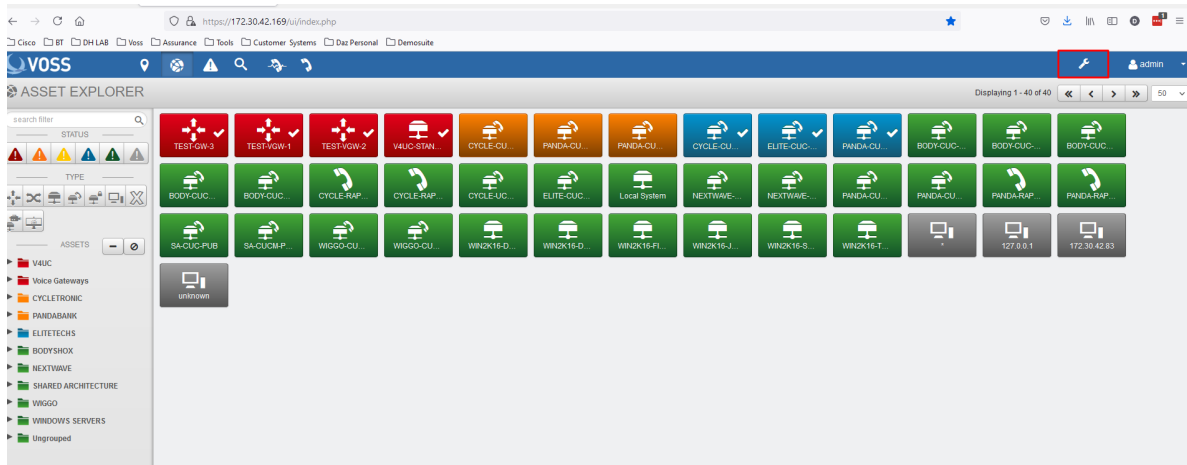


```
217.32.186.199 - PuTTY
10.144.30.161
10.25.212.1
10.25.212.129
10.25.212.193
10.25.212.65
10.25.213.1
10.25.213.129
10.41.224.1
10.41.224.129
10.41.224.193
10.41.225.1
10.41.225.129
10.41.225.193
10.41.225.65
10.41.240.33
10.41.240.56
10.44.88.1
10.44.88.129
10.44.88.193
10.44.88.65
10.59.247.129
x.x.x.x
-- Press <CTRL>-X to save and quit. --
End of buffer
```

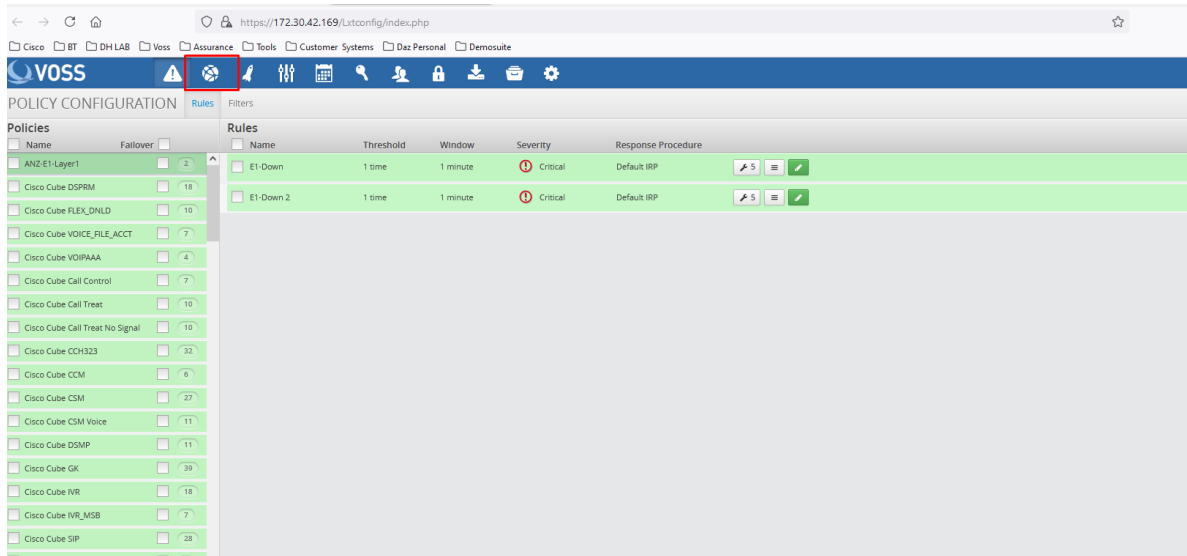
9. Add the IP Address of the call manager then press **<CTRL>-X** to save.

7.1.2. Add Customer Assets

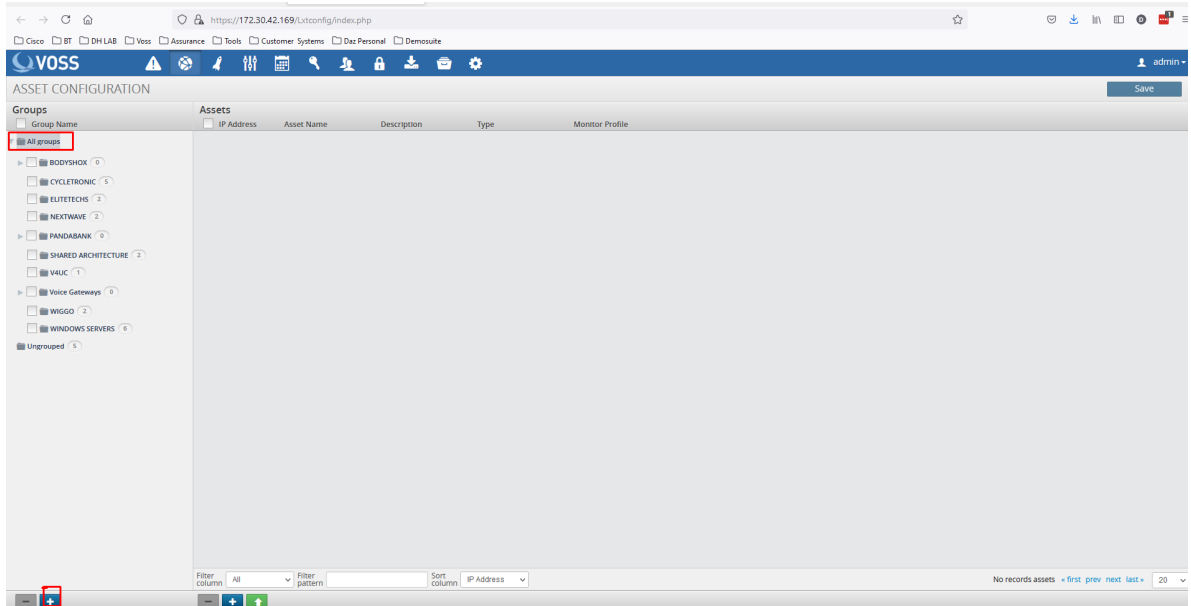
1. Log in to the Arbitrator as admin.



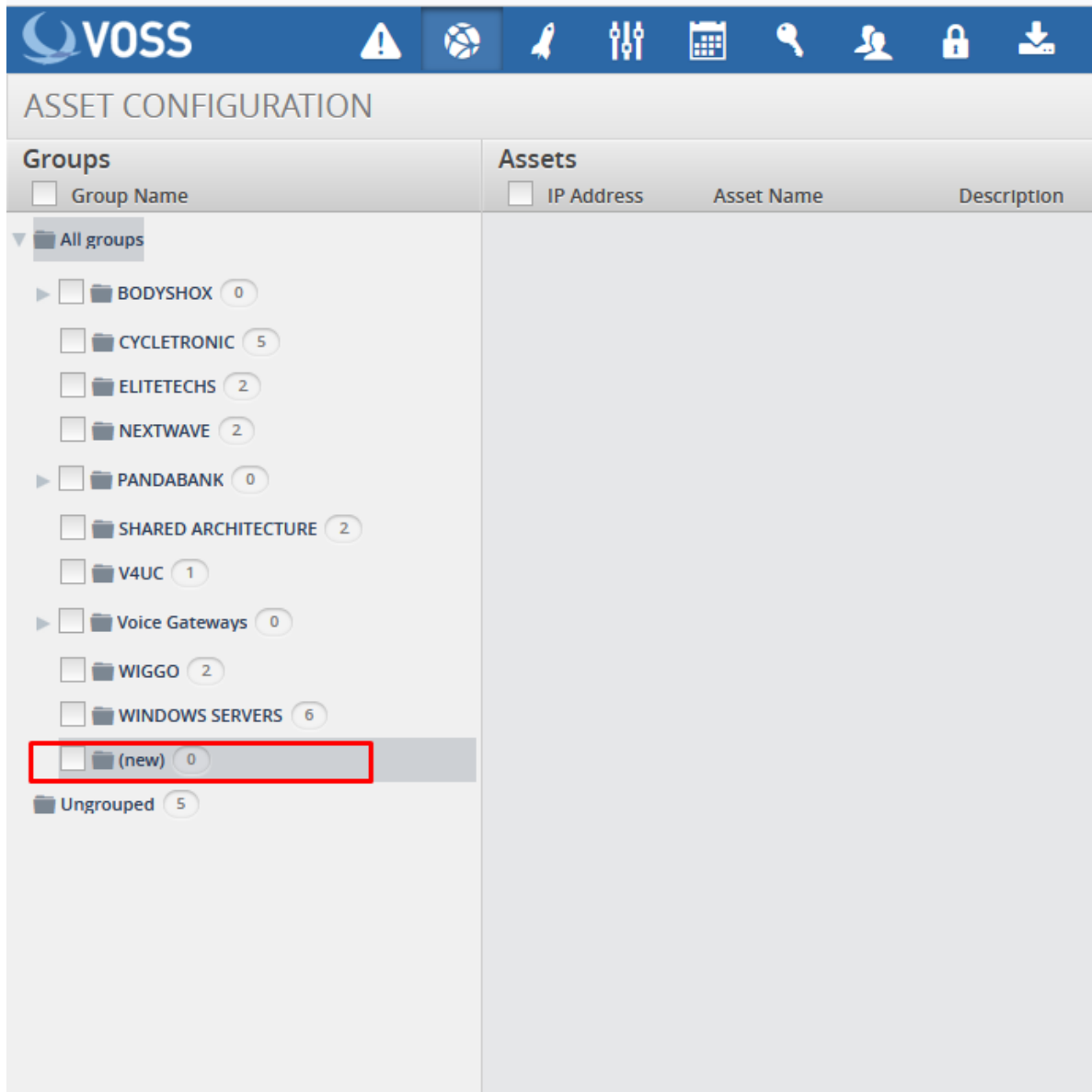
2. Click on the wrench icon (Highlighted in the red box)



3. Click on the Globe icon (as highlighted in the red box), this will then open the Asset Configuration screen.



4. With **All groups** selected, click the **+** icon



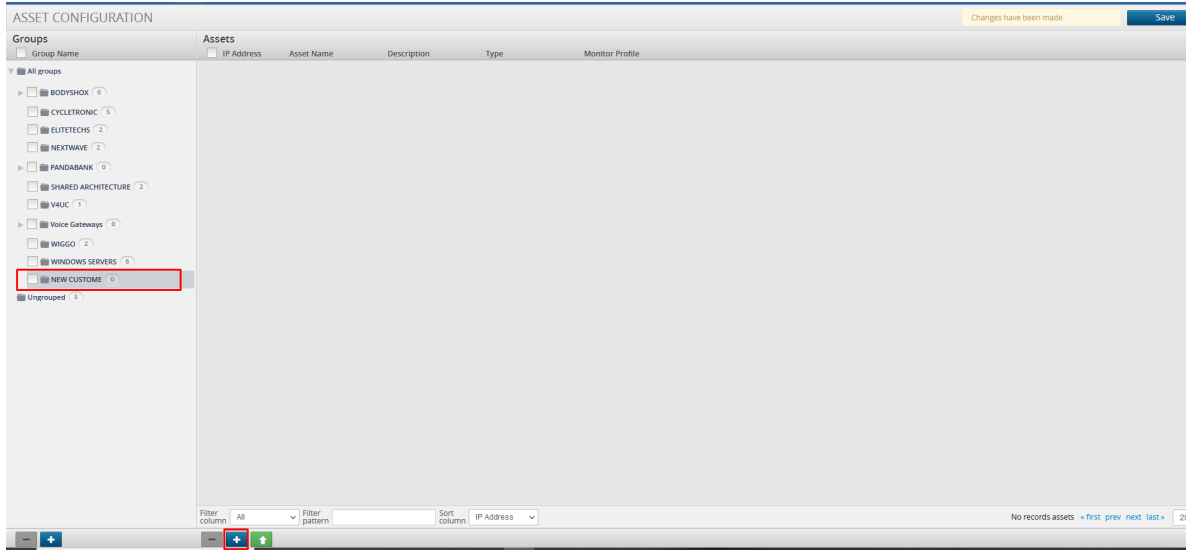
The screenshot displays the VOSS Asset Configuration interface. At the top, there is a blue header with the VOSS logo and several navigation icons. Below the header, the main content area is titled "ASSET CONFIGURATION" and is divided into two panels: "Groups" and "Assets".

The "Groups" panel shows a list of folders under "All groups". Each folder has a checkbox and a count in a circle. The folders listed are: BODYSHOX (0), CYCLETRONIC (5), ELITETECHS (2), NEXTWAVE (2), PANDABANK (0), SHARED ARCHITECTURE (2), V4UC (1), Voice Gateways (0), WIGGO (2), WINDOWS SERVERS (6), (new) (0), and Ungrouped (5). The "(new)" folder is highlighted with a red rectangular box.

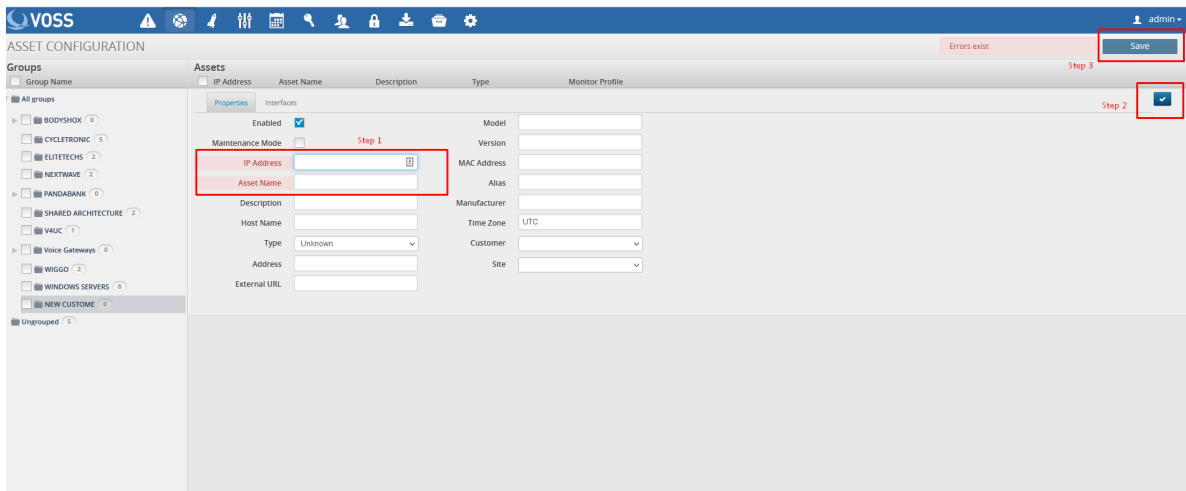
The "Assets" panel is currently empty and has a table header with columns: "IP Address", "Asset Name", and "Description".

This will create a new folder as shown above.

To rename this folder double click on it, rename and press **<Enter>**.




With the new folder (NEW CUSTOMER) highlighted, click the + in the right-hand pane.



- Step 1 – Enter IP Address (Mandatory)

Asset Name (Mandatory)

You may then enter any other information you have into the relevant fields.

- Step 2 – Click on 
- Step 3 – Click **Save**

Repeat the above for all assets you wish to monitor.

Alternatively, you can upload multiple assets using a CSV import.

CSV Import of Assets

It is possible to upload multiple assets using a CSV file.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	TEST-DEV1	Test	165.137.166.69	AA-AA:11:11:22:22	Cisco	CUCM	TEST-DEV1	NEW CUSTOME	voice server				
2	TEST-DEV2	Test	165.137.166.70	33:33:11:11:A2:22	Cisco	CUCM	TEST-DEV2	NEW CUSTOME	voice server				

The CSV file is available in the Google Drive.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	AE_NAME	DESC0	IP_ADDRE	MAC_ADD	VENDOR	MODEL	DESC1	HOST_NAI	DESC2	GROUP_N	RENDER_N	TIME_ZON	COMMENT	Physical Address	
2	MN_10RPI	MediaGat	165.137.166.69	Avaya	G450	MN_10RPP	NEWCUT	unknown	MG35	Saint Paul, MN					

Above is an example.

The mandatory fields are:

- AE_NAME
- IP_ADDRESS

You can also use this CSV to create the asset and the Asset group and place the asset into the group.

Note:

- Remove the header row before you try to upload.
- Mac Address field must be in the following format: XX:XX:XX:XX:XX:XX
- Renderer – This selects the icon seen on the Arbitrator. The options are:

```
unknown
router
firewall
switch
voice switch
switch voice
server
```


(continues on next page)


(continued from previous page)

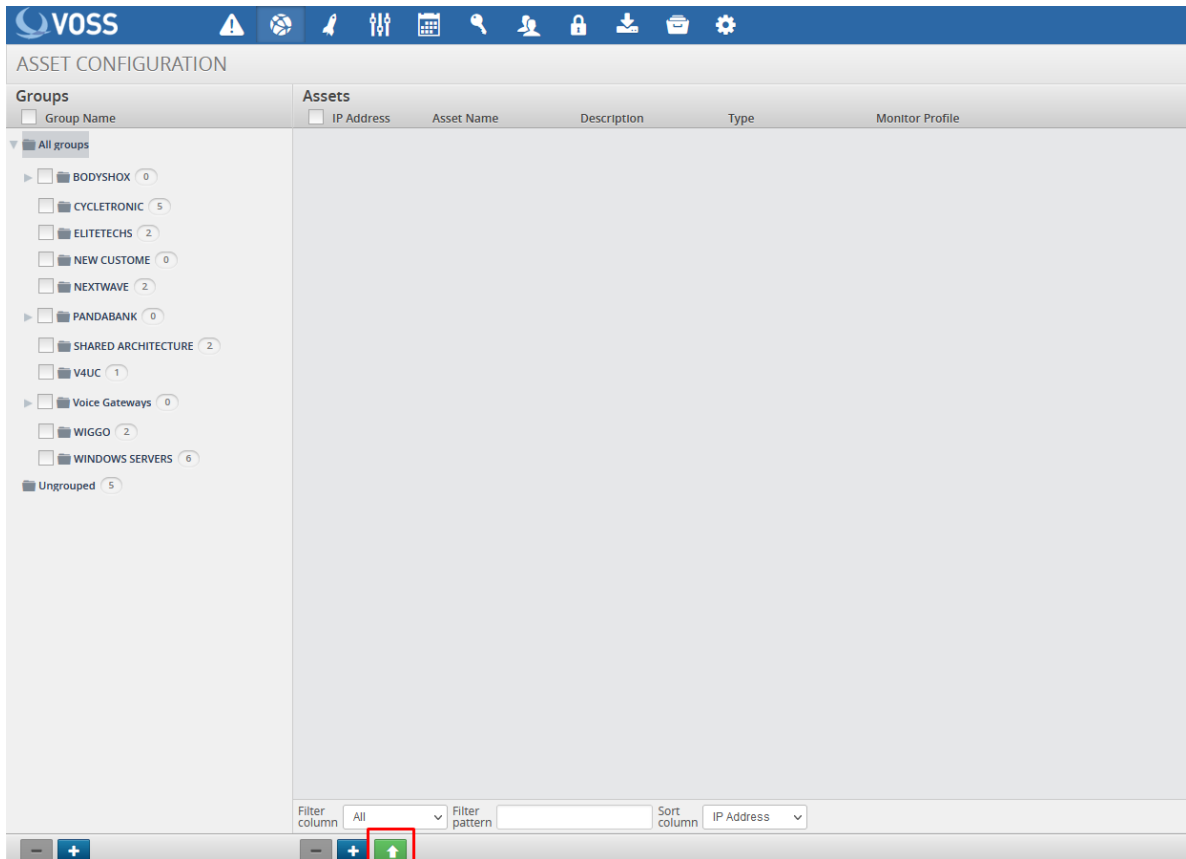
```
voice server
server voice
workstation
phone
```

How to Import using CSV


1. Log in to the Arbitrator with admin privileges.

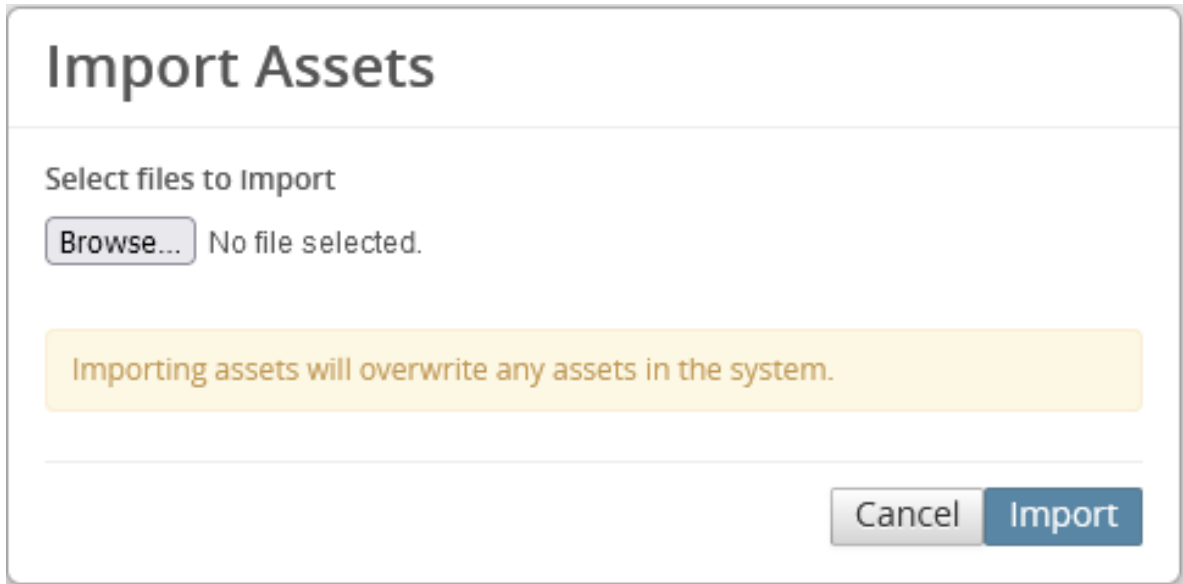
2. Click on the  to open the configuration screen.

3. Click on the  to open the Asset Configuration screen.

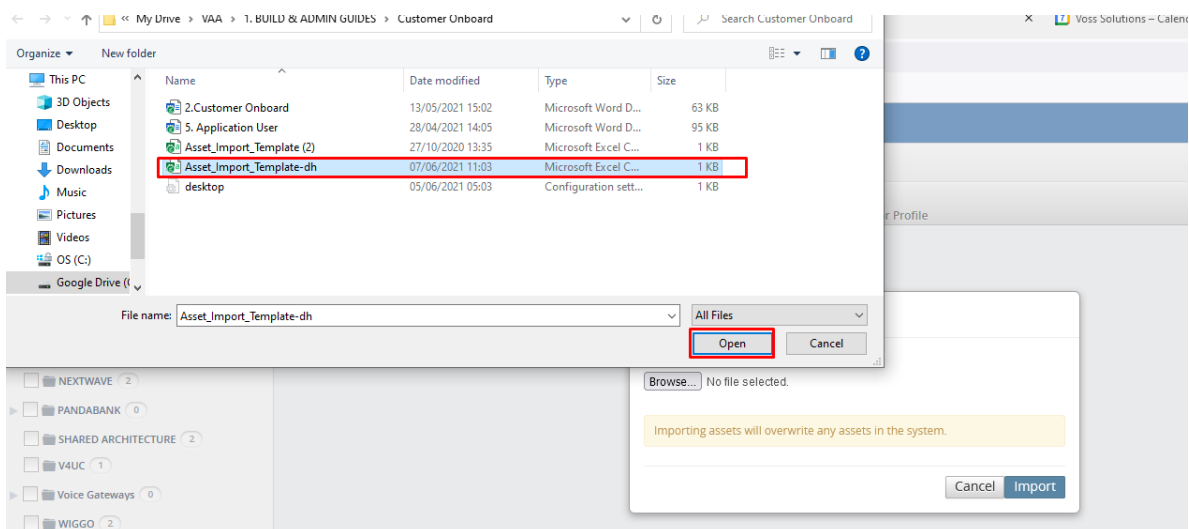


The screenshot displays the VOSS ASSET CONFIGURATION interface. The top navigation bar includes the VOSS logo and various icons. The main content area is divided into two sections: 'Groups' on the left and 'Assets' on the right. The 'Groups' section shows a tree view with several groups, each with a count in parentheses. The 'Assets' section is currently empty. At the bottom of the interface, there are filter and sort controls. A red box highlights a green plus icon in the bottom right corner of the table area.

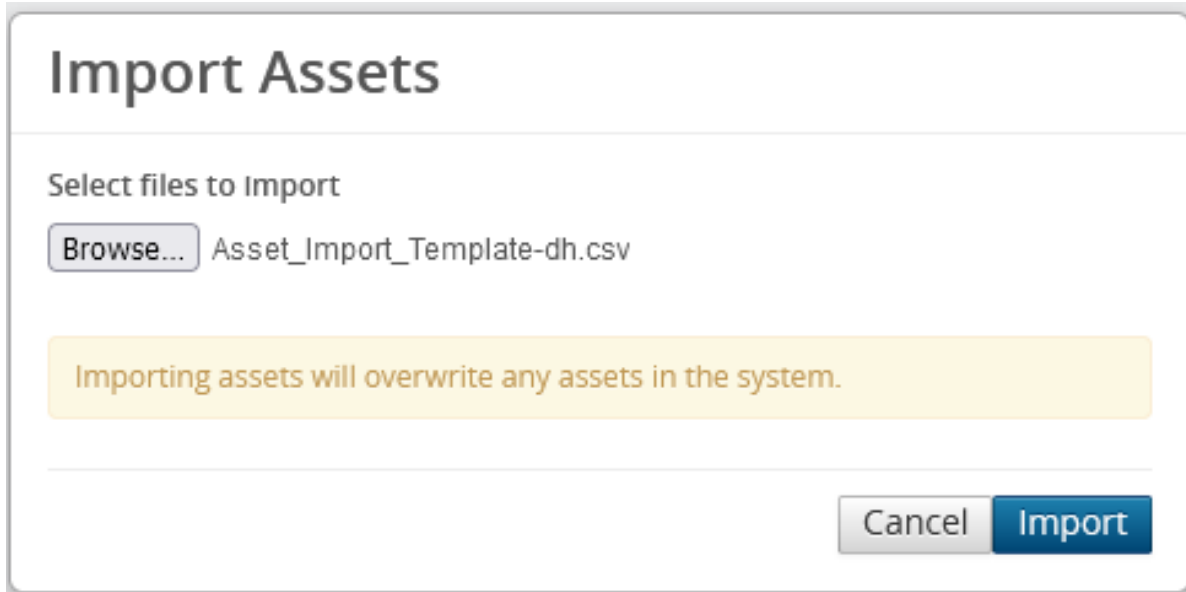
4. Click on the .
This will then open the below.



5. Browse to your csv file.

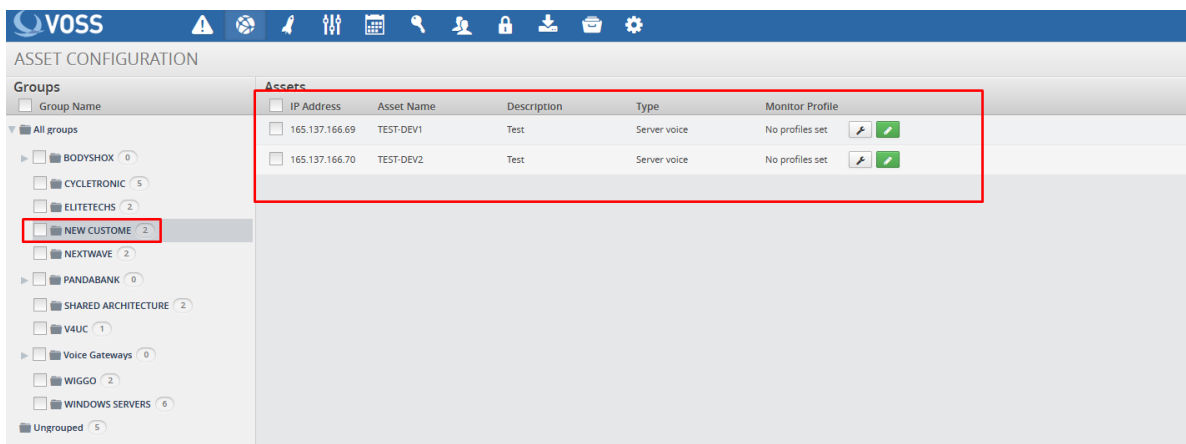


6. Click **Open**.



7. Click **Import**

Once the Import has completed check, the **Asset Configuration** screen to confirm your assets are present and in the correct location.



7.1.3. Assigning Probes to Assets


Assign Standard Probes

1. Log in to the Arbitrator with admin privileges.

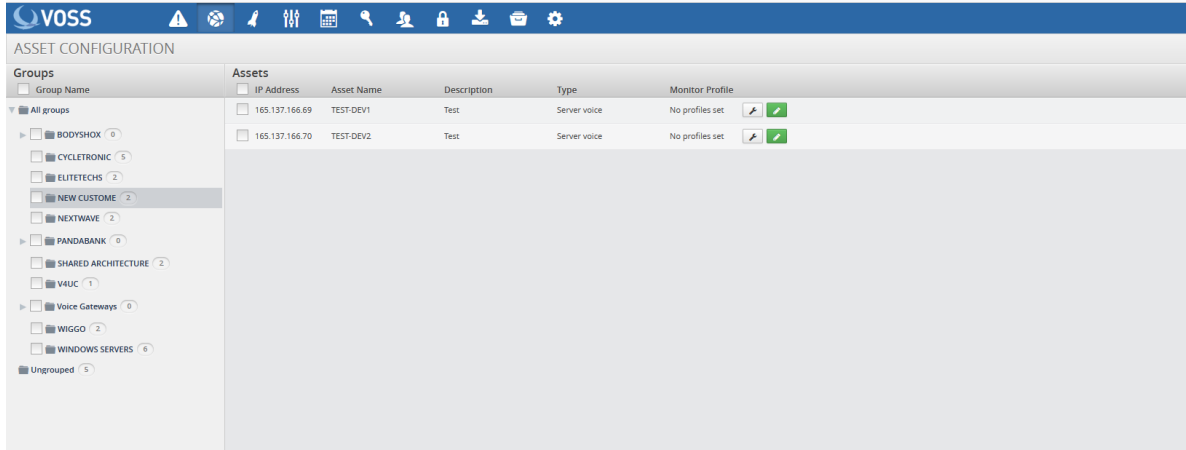


2. Click on the  to open the configuration screen.

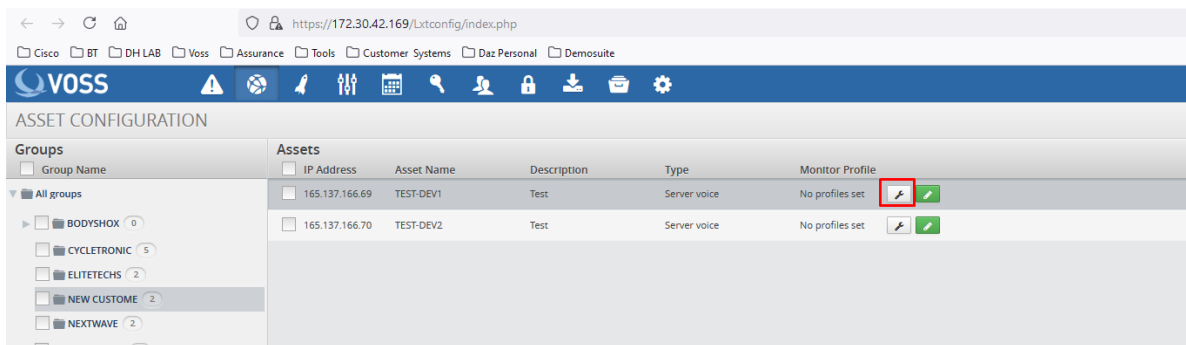


3. Click on the  to open the Asset Configuration screen.

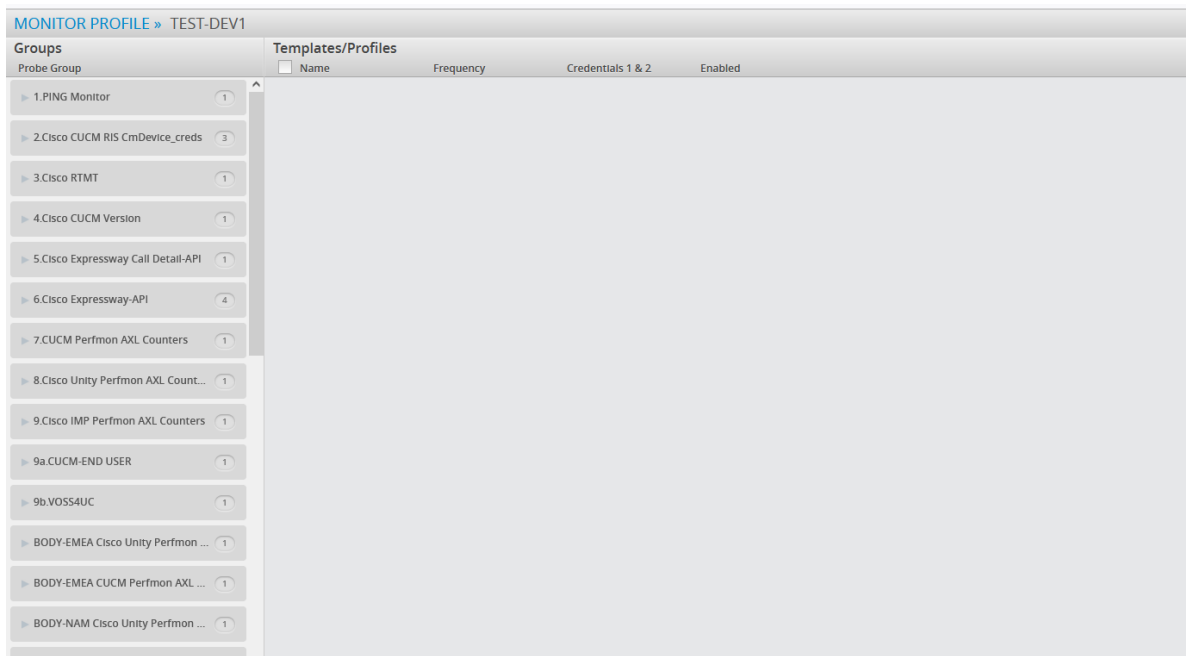
4. Select the Asset Group that contains the assets you wish to configure



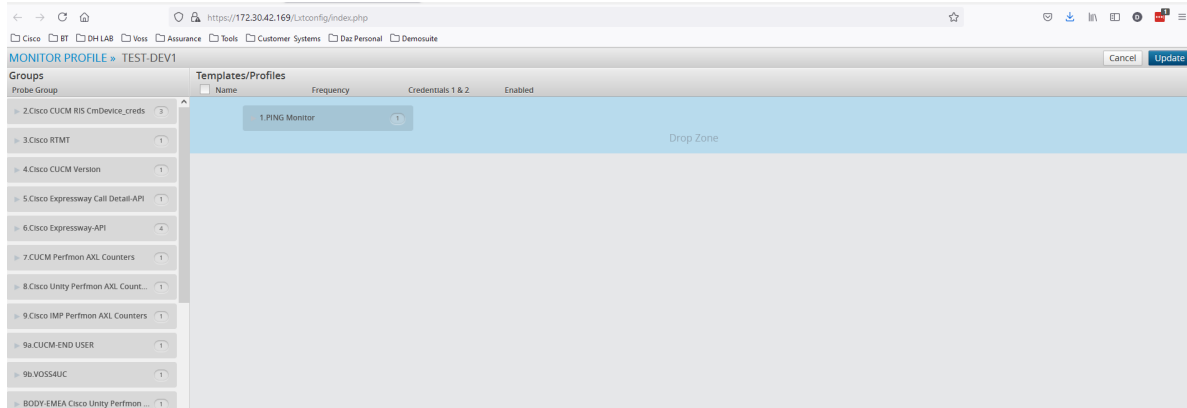
5. Click on the wrench icon as shown below.



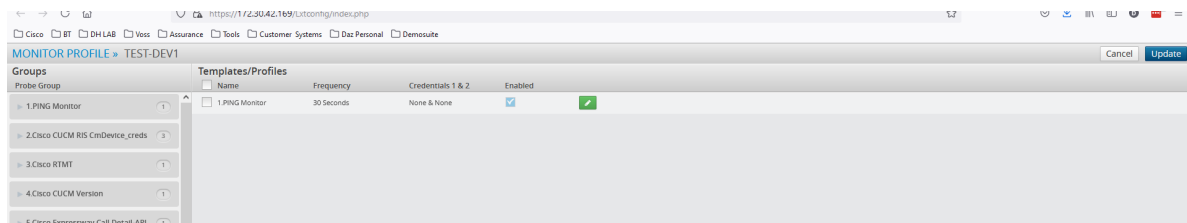
This will then open the Assignment screen.



6. You can now drag the required probe from the left pane to the right pane.



7. Ensure the Drop Zone (Blue Area) Reduces down before you drop.



8. If you then click on  you can set any time schedules / credentials required for this probe

9. Once finished click **Update** and then click **Save**.

Note: It is possible to assign multiple probes at the same time.

7.2. Call Manager Configuration

7.2.1. Application User

1. Create an Application User on the Call Manager, follow the standard Cisco documentation.
2. This user will need to have permissions granted.
3. Create a new Access Control Group named AXL-GROUP.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Access Control Group Configuration Relate

Save Delete Copy Add New

Status

Status: Ready

Access Control Group Information

Name*

Available for Users with User Rank as *

User

4. Add roles to this new group.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Access Control Group Configuration

Save

Status

Status: Ready

Access Control Group Information

Name* AXL-GRP

Role Assignment

Role

- Standard AXL API Access
- Standard AXL API Users
- Standard AXL Read Only API Access

Assign Role to Group

Delete Role Assignment

Save

*- indicates required item.

5. Edit the Application User you created and assign the following groups:

- **AXL-GROUP**
- **Standard CCM Server Monitoring**
- **Standard RealtimeAndTraceCollection**

7.2.2. Enterprise Parameters

In Enterprise Parameters navigate the section Cisco Syslog Agent and configure the IP address of the Arbitrator in one of the Remote Syslog Server Name fields.

Enterprise Parameters Configuration

Save Set to Default Reset Apply Config

[Reply Multicast Echo Request](#) * Off

Cisco Syslog Agent

[Remote Syslog Server Name 1](#) 62.7.201.25

[Remote Syslog Server Name 2](#) 217.32.186.230

[Remote Syslog Server Name 3](#)

CUCM Service Parameters

Ensure CDR Service Parameters are set:

- **CDR Enabled Flag** = True
- **CDR Log Calls with Zero Duration** = True
- **Call Diagnostic Enabled** = True

System

[CDR Enabled Flag](#) * True

[CDR Log Calls with Zero Duration Flag](#) * True

[Call Diagnostics Enabled](#) * Enabled Only When CDR Enabled Flag is True

CUCM Serviceability

1. Navigate to Cisco Call Manager Serviceability.
2. Select **Tools > CDR Management**

Alarm Trace Tools Snmp CallHome Help

CDR Management

Add new Delete Selected

General Parameters

Disk Allocation (MB)	High Water Mark (%)	Low Water Mark (%)	CDR / CMR Files Preservation Duration (Days)	Disable CDR/CMR Files Deletion Based on HWM	CDR Repository Manager Host Name	CDR Repository Manager Host Address
3000	80	40	30	<input type="checkbox"/>	CYCLE-CUCM-PUB	172.30.42.73

Click on any of the above parameters to update the General Parameters

Billing Application Server Parameters

<input type="checkbox"/>	Server Number	Host Name / IP Address*	User Name*	Protocol*	Directory Path*	Resend on Failure	Generate New Key
<input type="checkbox"/>	2	172.30.42.169	drop	SFTP	cucm/172.30.42.73/	<input checked="" type="checkbox"/>	Reset

Add new Delete Selected

Click on the Add New button to add a new Billing Application Server

Click on the corresponding Server Name to Update the Billing Application Server details

Select corresponding Checkbox and click on Delete Selected button to Delete Billing Application Server details. For the SFTP Billing server the Authentication keys will be deleted.

Click on the Reset Button to Generate new Keys and reset the connection to the SFTP server.

3. Fields:

- **Hostname/IP Address***: insert the arbitrator IP Address
- **User Name***: insert the username drop
- **Password***: insert your password for the user drop account.
- **Protocol**: SFTP
- **Directory Path***: cucm/ip address of call manager

Billing Application Server Parameters

Host Name / IP Address*	<input type="text" value="217.32.186.230"/>
User Name*	<input type="text" value="drop"/>
Password*	<input type="password" value="....."/>
Protocol*	<input type="text" value="SFTP"/> ▼
Directory Path*	<input type="text" value="cucm/10.41.165.193/"/>
Resend on Failure	<input checked="" type="checkbox"/>