



# VOSS Insights Arbitrator Install Guide

Release 23.2

Jul 31, 2023

## Legal Information

- Copyright © 2023 VisionOSS Limited.  
All rights reserved.
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

DOCUMENT ID: 20230731124403

# Contents

- 1 What's New** **1**
  - 1.1 Arbitrator Install Guide: Release 23.2 . . . . . 1
  
- 2 Insights Assurance Quickstart** **2**
  - 2.1 Insights Assurance Setup Overview . . . . . 2
  - 2.2 Arbitrator Setup . . . . . 3
  - 2.3 Arbitrator Integrations . . . . . 4
  - 2.4 Dashboard Setup . . . . . 5
  - 2.5 Assurance Solution Documentation . . . . . 5
  
- 3 Download** **7**
  - 3.1 Arbitrator Download . . . . . 7
  
- 4 VMWare Specification and Requirements** **8**
  - 4.1 Arbitrator VM Sizing Specifications . . . . . 8
  - 4.2 Arbitrator Correlation Consolidation VM Sizing Specifications . . . . . 9
  - 4.3 DS-9 NetFlow VM Sizing Specifications . . . . . 9
  - 4.4 Raptor Call Path Generation VM Sizing Specifications . . . . . 12
  - 4.5 Cloud Installation . . . . . 12
  
- 5 Port Requirements** **14**
  - 5.1 Arbitrator and Dashboard System Connectivity . . . . . 14
  - 5.2 Cisco UC Monitoring System Connectivity . . . . . 14
  - 5.3 MS Teams System Connectivity . . . . . 15
  - 5.4 NetFlow and DS9 Monitoring System Connectivity . . . . . 15
  - 5.5 VOSS Automate Port Usage . . . . . 16
  - 5.6 Skype for Business Monitoring System Connectivity . . . . . 17
  - 5.7 Avaya Call Manager Connectivity . . . . . 18
  
- 6 Deploy and Networking Setup** **19**
  - 6.1 Deploy and VM Installation . . . . . 19
  
- 7 Database and System Setup** **30**
  - 7.1 Install Arbitrator System . . . . . 30
  - 7.2 Set up Arbitrator to Arbitrator Communication . . . . . 33
  
- 8 Certificates** **37**
  - 8.1 Add or Update Certificates . . . . . 37
  
- 9 CUCM Asset Onboarding** **40**
  - 9.1 Customer Onboard . . . . . 40
  - 9.2 Call Manager Configuration . . . . . 53
  
- Index** **57**

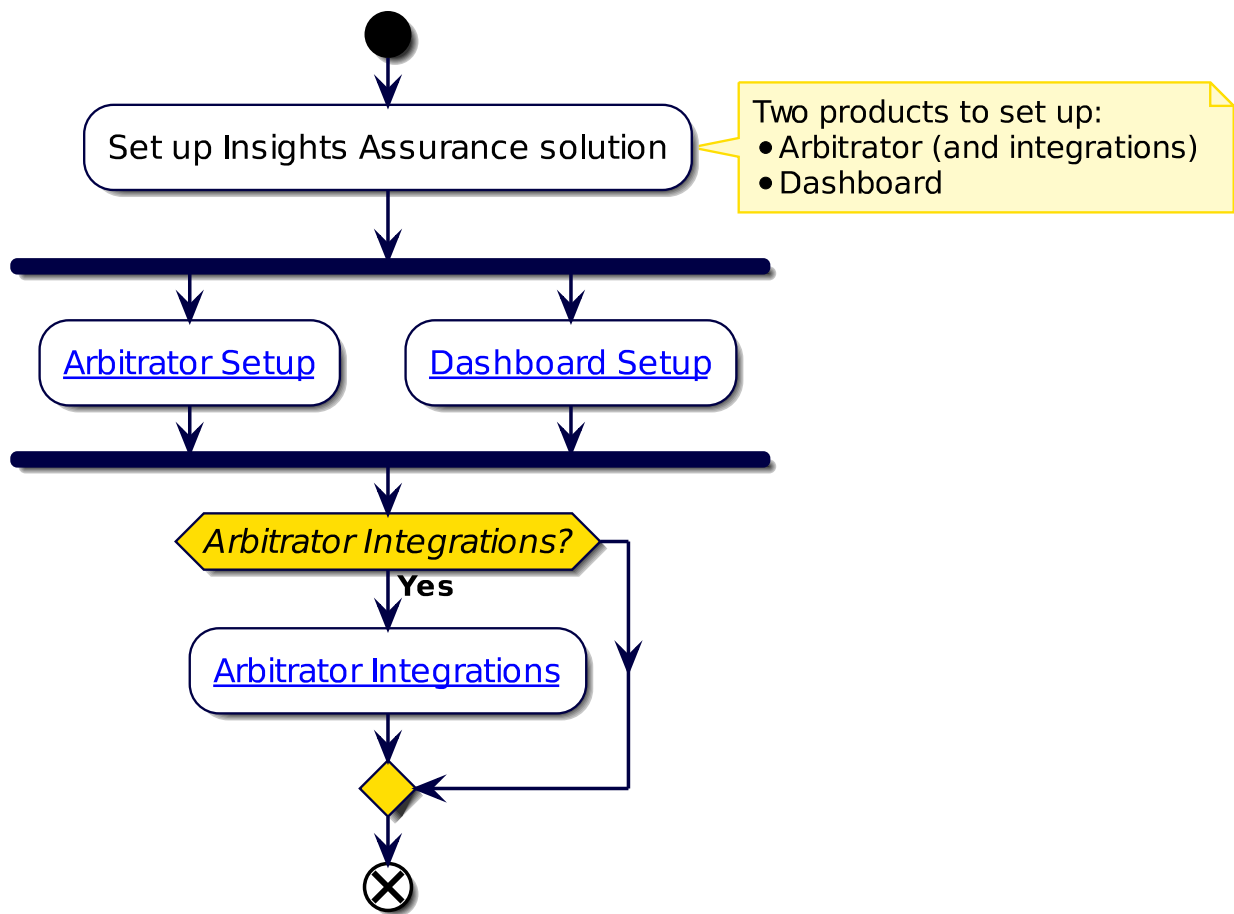
# 1. What's New

## 1.1. Arbitrator Install Guide: Release 23.2

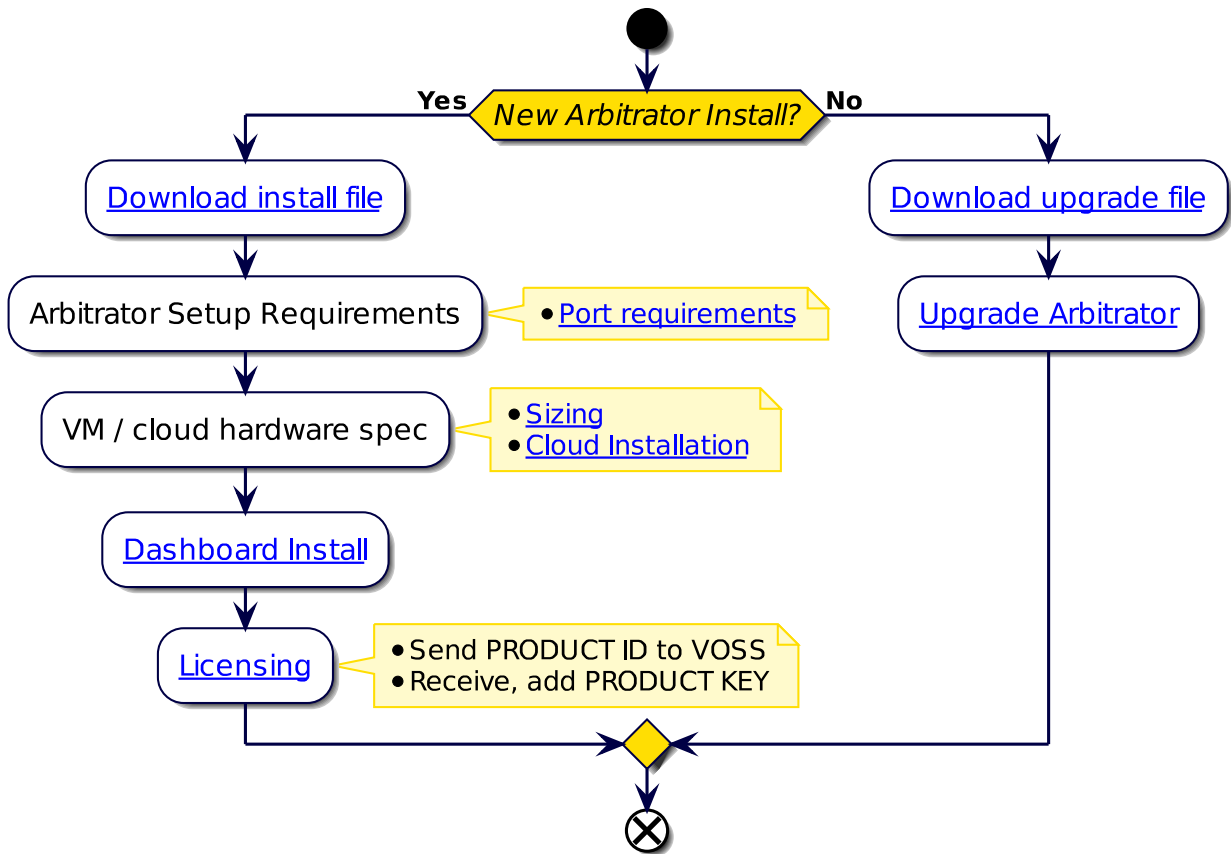
- EKB-16057: Vulnerable ftp-libopie - Arbitrator. See: *Deploy and VM Installation*  
Added a step to disable FTPD if it's not required.

## 2. Insights Assurance Quickstart

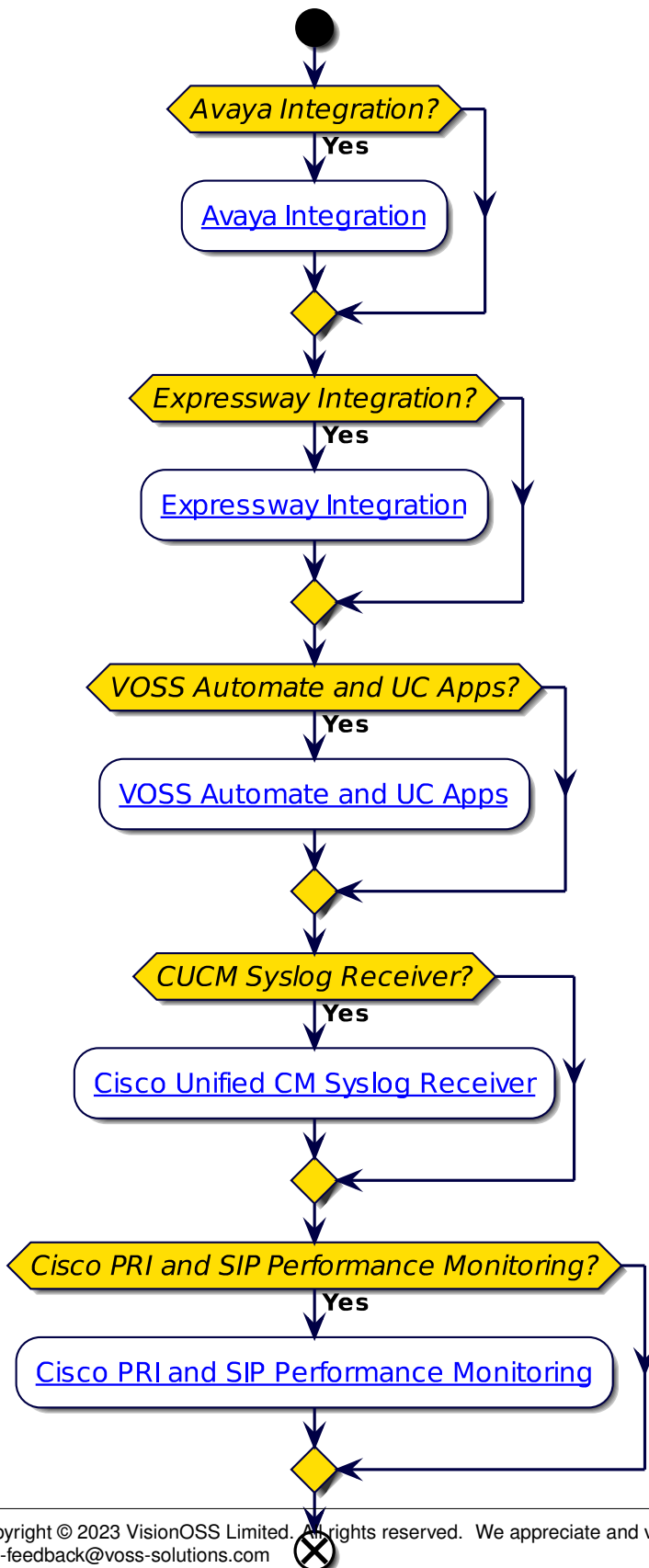
### 2.1. Insights Assurance Setup Overview



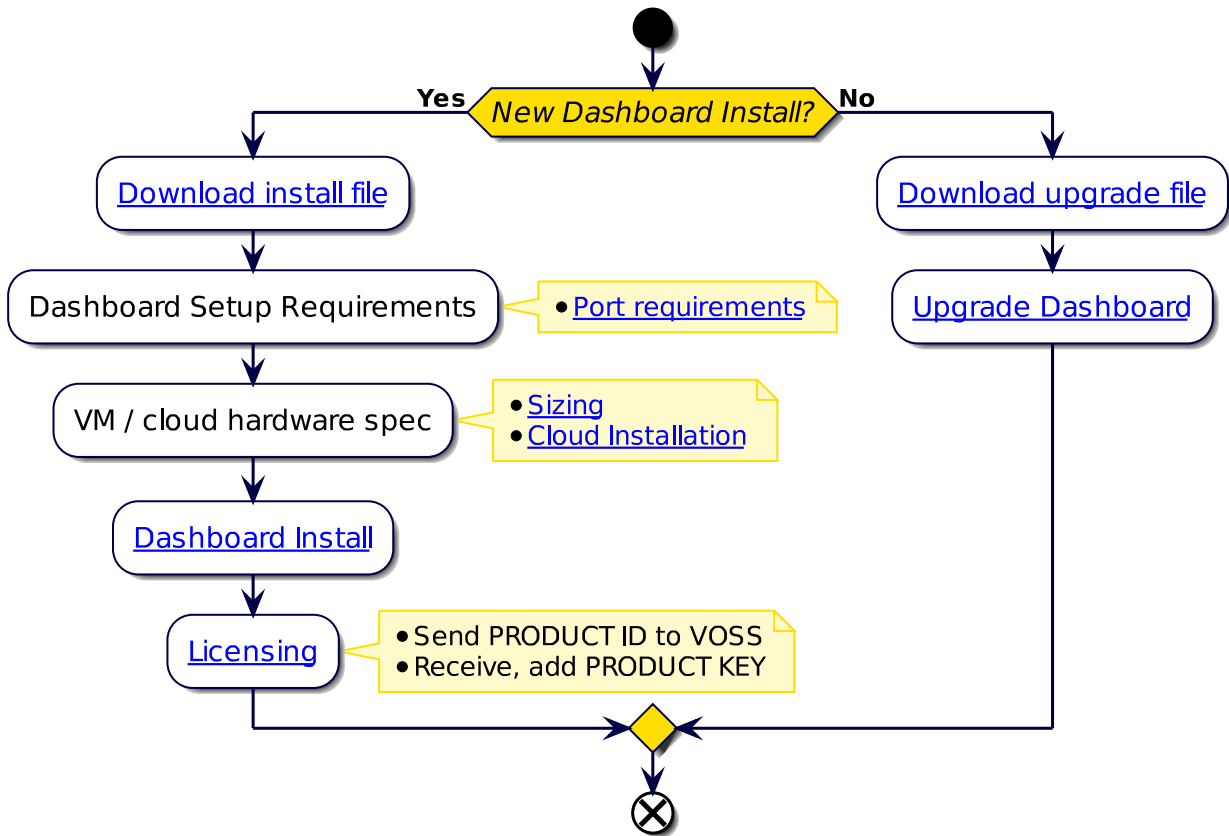
## 2.2. Arbitrator Setup



## 2.3. Arbitrator Integrations



## 2.4. Dashboard Setup



## 2.5. Assurance Solution Documentation

### 2.5.1. Additional Reference Documentation

- Arbitrator Release Notes
- Compatibility Matrix
- Arbitrator Install Guide
- Dashboard and Arbitrator Maintenance and Upgrade Guide
- Arbitrator Administration Guide
- Arbitrator API Guide
- Platform Guide
- Avaya Integration for Insights
- VOSS Assurance: Cisco Expressway monitoring set up
- VOSS Insights UC Apps License Sync Guide



- Cisco UCM syslog with VOSS Assurance as Receiver
- Arbitrator Probes to Monitor Cisco PRI and SIP Performance Monitoring
- Dashboard Release Notes
- Compatibility Matrix
- Dashboard Install Guide
- Dashboard and Arbitrator Maintenance and Upgrade Guide
- Dashboard Administration Guide
- Dashboard API Guide
- Platform Guide

## 3. Download

### 3.1. Arbitrator Download

- Arbitrator OVA file:
    1. Log in on the [VOSS Customer Portal](#)
    2. Go to **Downloads > VOSS Insights > Insights Arbitrator Hawaii > <release number> > New Installation.**
    3. Download the .ova file
    4. Verify that the original .sha256 checksums on the download site server match.
      - **system checksum media/<ova\_file>**Checksum: <SHA256>
  - Arbitrator upgrade file:
    - a. Log in on the [VOSS Customer Portal](#)
      - i. Go to **Downloads > VOSS Insights > Insights Arbitrator Hawaii > <release number> > Upgrade.**
      - ii. Download the .lxsp upgrade file
      - iii. Verify that the original .sha256 checksums on the download site server match.
        - **system checksum media/<lxsp\_file>**Checksum: <SHA256>
- or
- b. Use the direct link - for automated download mechanisms:
    - i. <http://www.layerxtech.com/downloads/arbitratorhawaii/updates/layerX-arbitrator-sp25-sp22.1.lxsp>To ensure continuity, the release updates will still be available from the LayerX download site, allowing customers to either download files manually, or via the automated download mechanisms from that location.

## 4. VMWare Specification and Requirements

### 4.1. 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 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

## 4.2. 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

## 4.3. DS-9 NetFlow VM Sizing Specifications

VOSS Insights DS9 for NetFlow sizing specifications are divided into small, medium and large solutions based on tiers related to the number of flows that need to be supported.

Each solution below includes the VM specifications for both the VOSS Insights DS9 server and the VOSS Insights Dashboard server.

### 4.3.1. Small NetFlow Solution

The three small tiers in Flows per Second:

- 1,000
- 5,000
- 10,000

Dashboard Server VM		DS9 NetFlow Collector VM	
Cores	12	Cores	16
Memory GB	32	Memory	64
Disc Storage GB	500	Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero		Disc 2 Storage in GB	500
		All Discs must be SSDs and Provisioned as Thick Eager Zero	

### 4.3.2. Medium NetFlow Solution

Two medium tiers in Flows per Second:

- > 10,000 but <= 25,000
- > 25,000 but <= 50,000

Dashboard Server VM		DS9 NetFlow Collector Bare Metal Server (Dell R740 or Equivalent)	
Cores	16	Cores	16
		CPU Needs to be Intel Gold or better.	
Memory GB	64	Memory	196
Disc Storage GB	500	Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero		Disc 2 Storage in TB	1,5
		Read Intensive SSDs required	
		Dual Intel 10GB NIC	1
		Intel Quad 1GB NIC	1
		iDRAC Enterprise or Equivalent	
		Dual Power Supplies	

### 4.3.3. Large NetFlow Solution

Two large tiers in Flows per Second:

- > 50,000 but <= 100,000
- > 100,000 but <= 200,000

**Note:** The DS9 Collector requires a minimum of 2 Bare Metal Servers to collect this volume in one location.

<b>Dashboard Server VM</b>		<b>DS9 NetFlow Collector Bare Metal Server 1 (Dell R740 or Equivalent)</b>	
Cores	16	Cores CPU Needs to be Intel Gold or better.	16
Memory GB	64	Memory	196
Disc Storage GB	500	Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero		Disc 2 Storage in TB	3
		Read Intensive SSDs required	
		Dual Intel 10GB NIC	1
		Intel Quad 1GB NIC	1
		iDRAC Enterprise or Equivalent Dual Power Supplies	
		Dual Power Supplies	

		<b>Bare Metal Server 2 (Dell R740 or Equivalent)</b>	
		Cores CPU Needs to be Intel Gold or better.	16
		Memory	196
		Disc 1 Storage in TB	3
		Disc 2 Storage in TB	3
		Disc 3 Storage in TB	3
		Read Intensive SSDs required	
		Dual Intel 10GB NIC	1
		Intel Quad 1GB NIC	1
		iDRAC Enterprise or Equivalent Dual Power Supplies	
		Dual Power Supplies	

**Note:**

- Larger than 200K flows per second requires special pricing and configuration.
- Distributed DS9 collection is available. This may reduce the compute required at each collection location.

## 4.4. Raptor Call Path Generation VM Sizing Specifications

### 4.4.1. Raptor Server

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

### 4.4.2. Raptor Client

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

## 4.5. Cloud Installation

The VMWare specification and requirements for each product can be used as guidelines when preparing for cloud installations.

For example, for the example minimum sizes below, the VM specifications are best matched by the cloud VM types indicated:

- Google Cloud products

Product	Size	Cloud VM Specification
Arbitrator	< 5k users	n2-standard-8
Dashboard	< 10k users	n2-standard-8
Raptor	N/A	custom
DS-9	< 1,000 flows/sec	n2d-standard-16

- Amazon Web Services

Product	Size	Cloud VM Specification
Arbitrator	< 5k users	t2.2xlarge
Dashboard	< 10k users	t2.2xlarge
Raptor	N/A	t2.small
DS-9	< 1,000 flows/sec	m6g.4xlarge

- Microsoft Azure

<b>Product</b>	<b>Size</b>	<b>Cloud VM Specification</b>
Arbitrator	< 5k users	B8ms
Dashboard	< 10k users	B8ms
Raptor	N/A	B1ms
DS-9	< 1,000 flows/sec	D16 v5



## 5. Port Requirements

### 5.1. Arbitrator and Dashboard System Connectivity

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

Source	Destination	Port / protocol	Notes
Arbitrator Server / Dashboard Server	Arbitrator 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
Arbitrator Server	Arbitrator 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
Arbitrator Server / Dashboard Server	Network Resources (NTP, DNS)	53, 123 UDP	Time and DNS
Client PC – GUI Interface and CLI Management Access	Arbitrator Server / Dashboard Server	443, 8443, 22, 80 TCP	User Interface Access
VOSS Automate	Dashboard Server	27020	Database access
Arbitrator Server / Dashboard Server	AD	389 636 TCP UDP	Authentication

### 5.2. 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

## 5.3. MS Teams System Connectivity

Source	Destination	Port / protocol	Notes
MS Teams - Cloud Agent	Cloud Arbitrator	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

## 5.4. NetFlow and DS9 Monitoring System Connectivity

### 5.4.1. Communication ports between NetFlow Source and DS9

Source	Destination	Protocol	Port	Direction	Description
NetFlow Source	DS9	UDP	4739	Unidirectional	IPFIX (Optional)
NetFlow Source	DS9	UDP	2055	Unidirectional	NetFlow v9 (Optional)
NetFlow Source	DS9	UDP	9996	Unidirectional	NetFlow v5 (Optional)
NetFlow Source	DS9	UDP	6343	Unidirectional	Sflow v5 (Optional)
DS9	NetFlow Source	UDP	161	Unidirectional	SNMP queries

### 5.4.2. Communication ports between Dashboard Server Users and Dashboard Server

Source	Destination	Protocol	Port	Direction	Description
Dashboard users	Dashboard Server	TCP	443	Unidirectional	HTTPS (GUI access)

### 5.4.3. 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	5432	Unidirectional	Data respository access
Dashboard Server	DS9	TCP	8082	Unidirectional	Data respository access
Dashboard Server	DS9	TCP	443	Unidirectional	DS9 System Stats and management
DS9	Dashboard Server	UDP	514	Unidirectional	DS9 System Logs

### 5.4.4. Communication ports that are required for remote management purposes

Source	Destination	Protocol	Port	Direction	Description
Admin users	DS9	TCP	22	Unidirectional	SSH (remote CLI access) and file transfer
Admin users	<b>Dashboard Server</b>	TCP	22	Unidirectional	SSH (remote CLI access) and file transfer
Admin users	<b>Dashboard Server</b>	TCP	443	Unidirectional	WEB access

## 5.5. 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

## 5.6. 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

## 5.7. Avaya Call Manager Connectivity

Source	Destination	Port / protocol	Notes
Avaya Call Manager	Insights Arbitrator	9000 TCP	To stream CDRs to the arbitrator

## 6. Deploy and Networking Setup

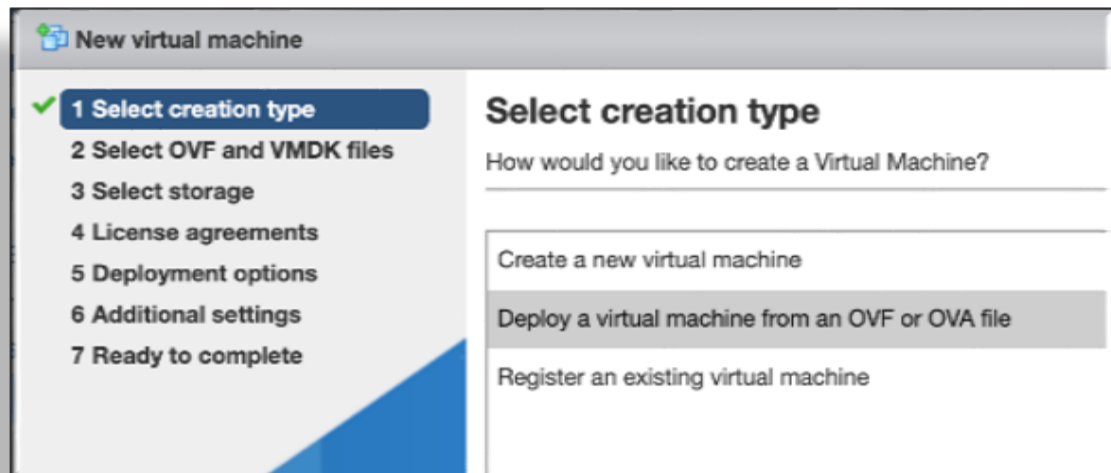
### 6.1. Deploy and VM Installation

#### 6.1.1. Base Install and Configuration

This procedure installs the base system, and involves the following tasks:

- Download the OVA.
- Deploy the OVA.
- Run the VM.
- Log in as admin.
- Change your password.
- Configure network settings.

1. Download the OVA for your system, to a directory accessible by the VM client.
2. Deploy the OVA:
  - 2.1. Select the downloaded OVA file, and choose a VM name.



- 2.2. At **Select storage**, configure storage settings, based on the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.

2.3. Configure the network mappings based on the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.

3. Run the VM, and monitor installation of the packages, which may take some time.

```

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/lsof.lxp
Info: install_package : Unpacking /mnt/cd/pkg/mdadm.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

```

Once all packages are installed, the VM is automatically powered off, confirmed via the auto-poweroff message on the console.

```

DHCPDISCOVER on eth8 to 255.255.255.255 port 67
DHCPDISCOVER on eth8 to 255.255.255.255 port 67
DHCPDISCOVER on eth8 to 255.255.255.255 port 67
DHCPDISCOVER on eth8 to 255.255.255.255 port 67
DHCPDISCOVER on eth8 to 255.255.255.255 port 67
DHCPDISCOVER on eth8 to 255.255.255.255 port 67
DHCPDISCOVER on eth8 to 255.255.255.255 port 67
DHCPDISCOVER on eth8 to 255.255.255.255 port 67
No DHCPOFFERS received.
Unable to obtain a lease on first try. Exiting.
useradd: user 'admin' already exists
umount: /mnt/target/dev: device is busy

```

The system reboots. Wait until you see the **About** console, which displays placeholder values for hostname, version, license, days licensed and remaining, and so on.

```

About
=====
Hostname: <hostname>
Version: <version>
Theme: <theme>

```

(continues on next page)

(continued from previous page)

```

    Flavor:
    License:  NNNNN-NNNNN-NNNNN-NNNNN-NNNNN
    Days Licensed:  nnnnn
    Days Remaining:  nnnnn
    Product Key:
    Website:  <website>
    Kernel:  Linux n.nn.nn-lxt-3 x86_64 GNU/Linux

<hostname> login:

```

#### 4. Log in:

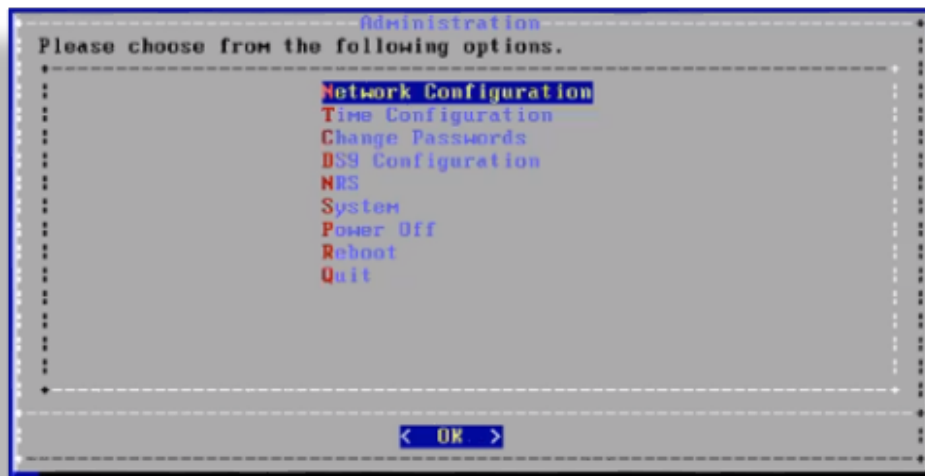
On the **About** console, at **<hostname> login:**, log in as **admin** and use as the password, the last 10 characters of the value at **License**, *excluding the dash*.

---

**Important:** The **License** key value is *only* displayed on the **About** console. When you *ssh* in, it is not visible, thus, you must copy the admin password from the **About** console.

---

Once you're logged in, the **Administration** menu displays (the image displays an example for DS9):



#### 5. Change your password:

On the **Administration** menu, select **Change Passwords**, then change your password.

---

**Note:** It is strongly recommended that you change your password immediately.

---

#### 6. Configure network settings.

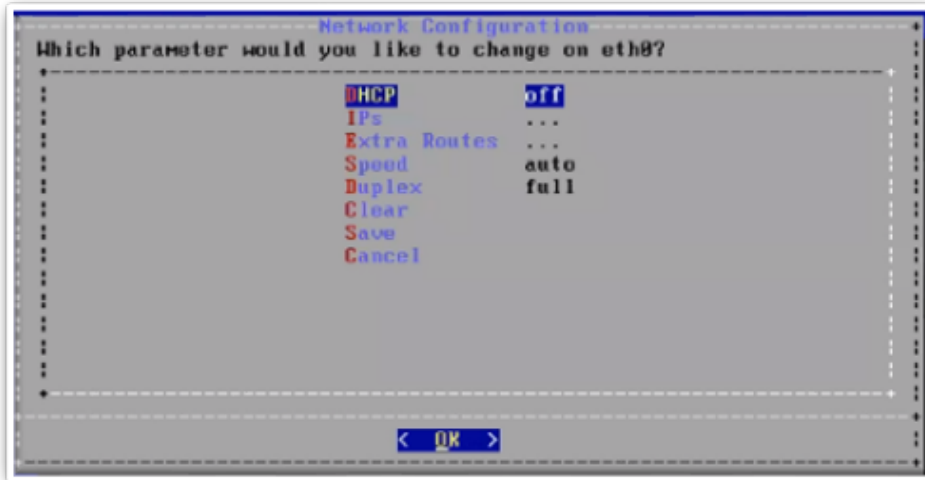
On the **Administration** menu, select **Network Configuration**, then:

##### 6.1 Configure interface settings:

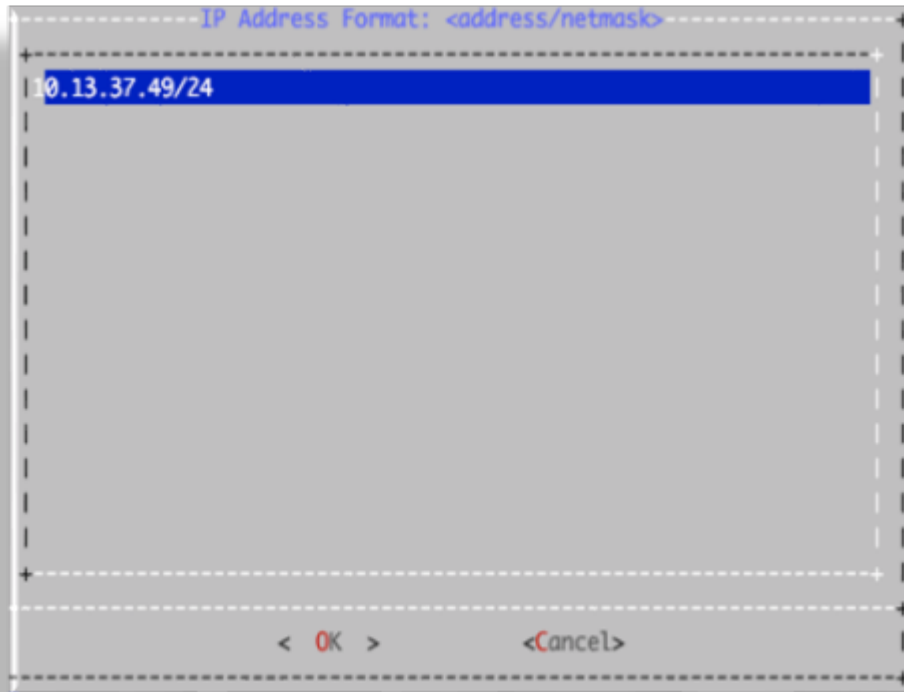
6.1.1 Select the **Interface Settings** menu, then select the interface to configure.

6.1.2 Modify the parameters for the selected interface:



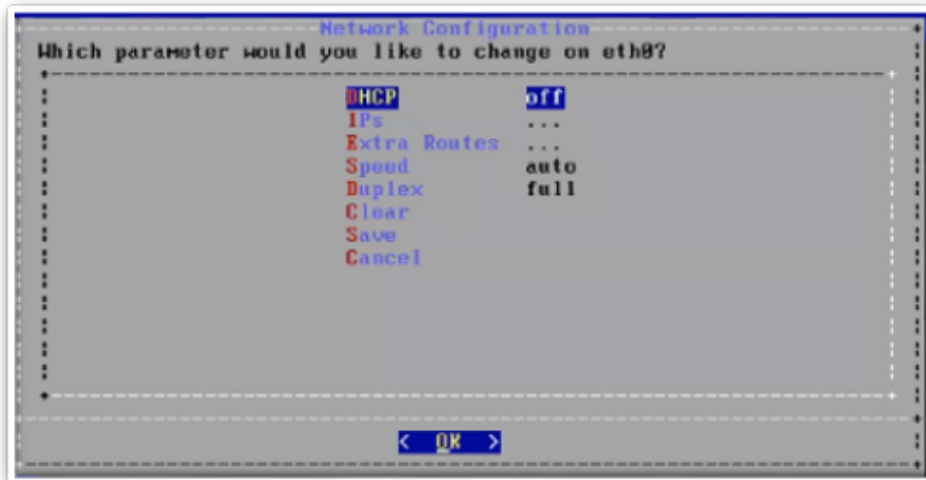


- Select **IPs**, then set the IP address and netmask in the format `nn.nn.nn.nn/24`.
- Save your changes.

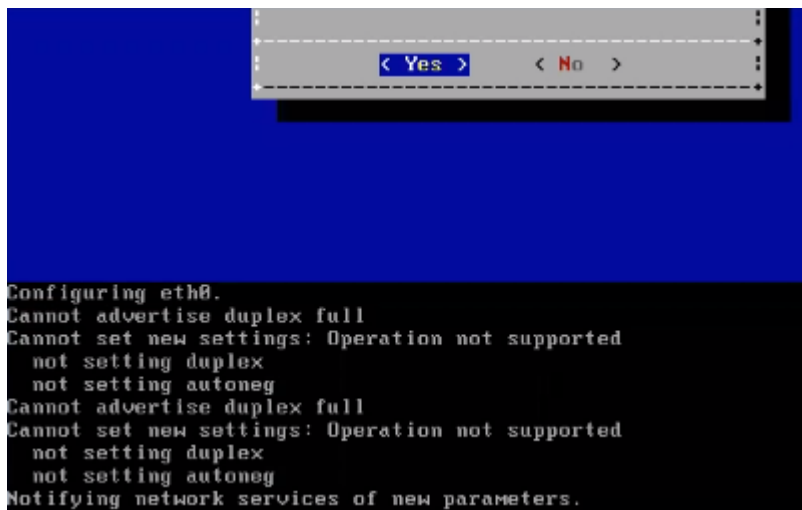


6.2 Configure the default gateway:

Select the **Extra Routes** menu:

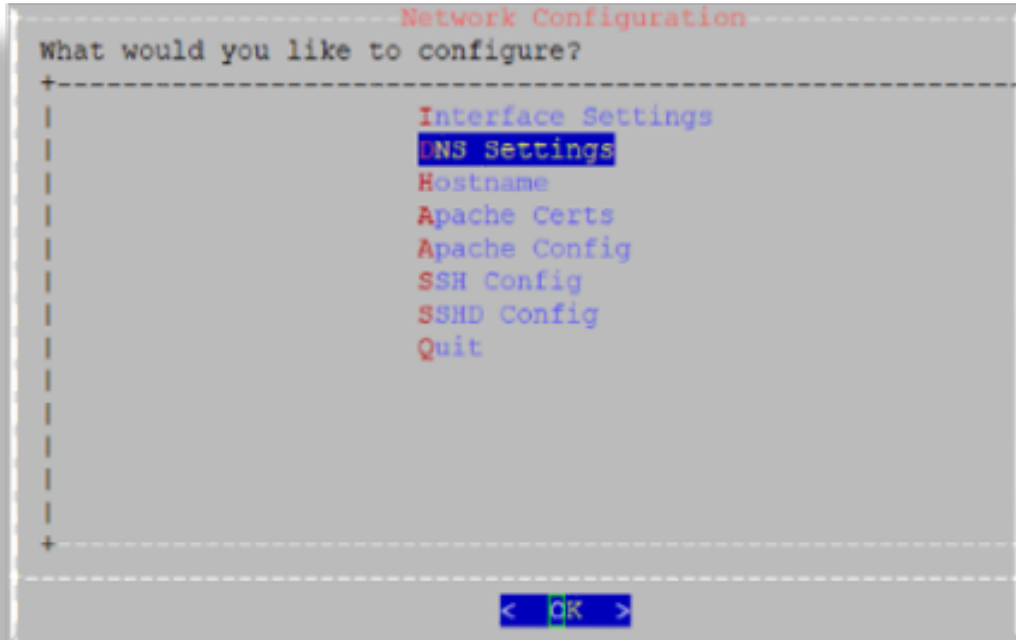


- Use the following format for the entry: `default <gateway IP address>`
- The word `default` is required. For additional route entries use the `<subnet> <gateway>` format. Similar to what would be done on a Linux system at the CLI.

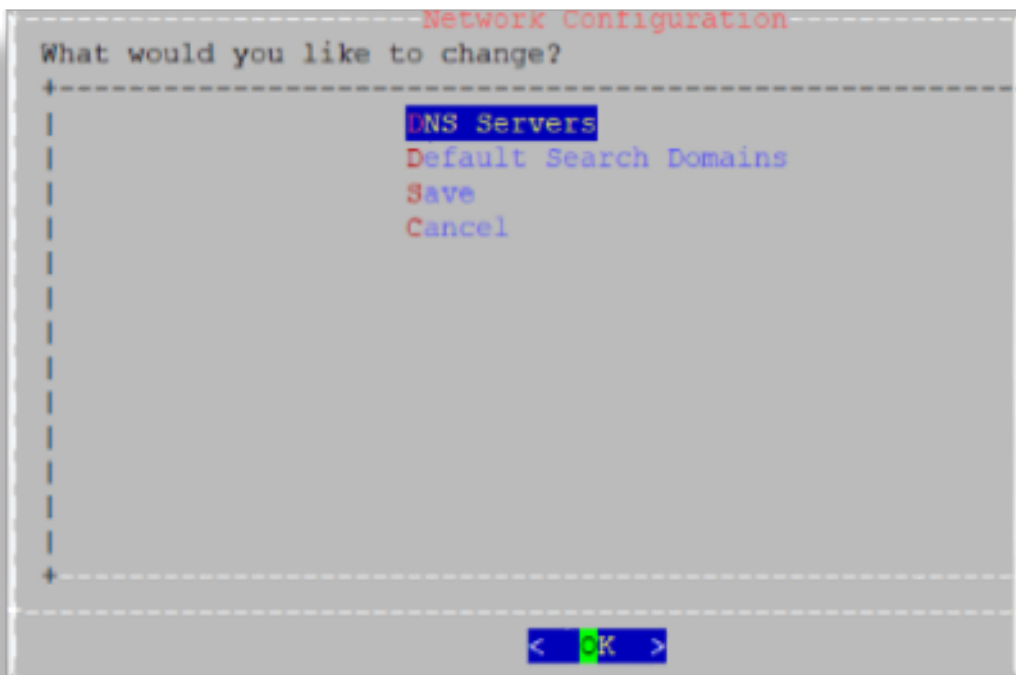


6.3 Configure DNS settings:

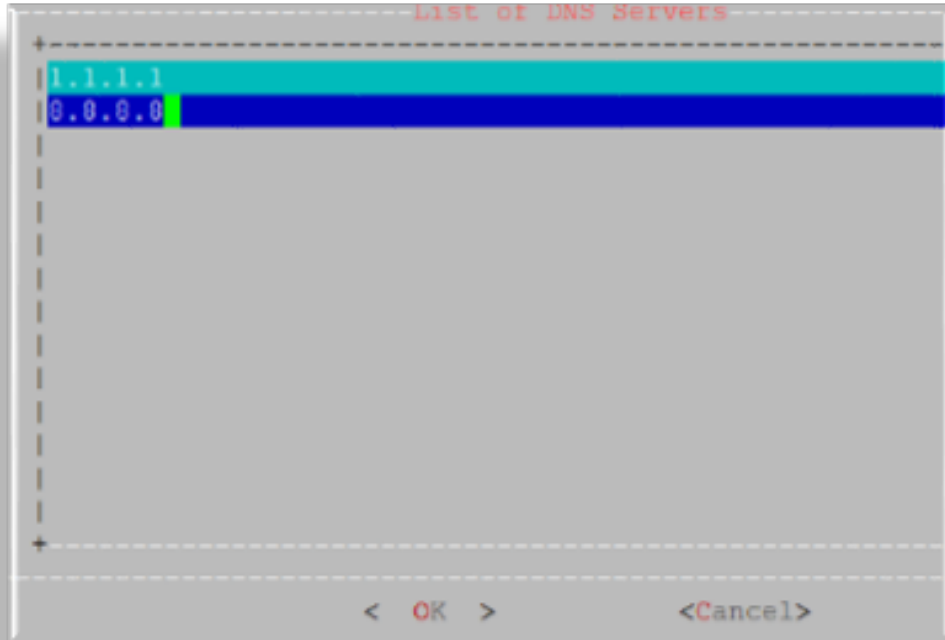
6.3.1 Select the **DNS Settings** menu.



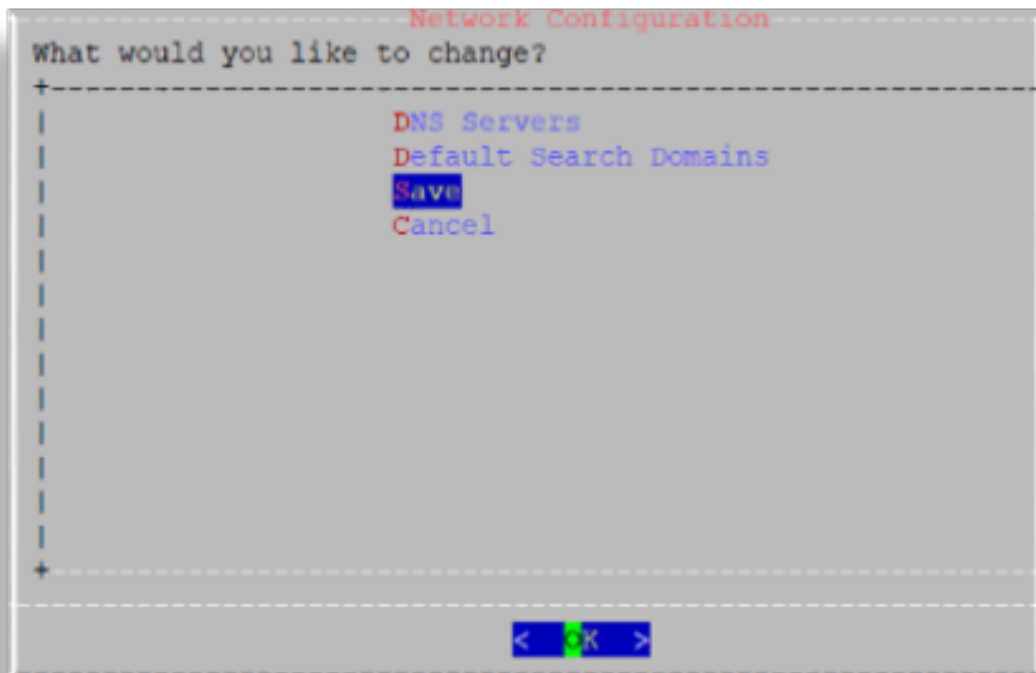
### 6.3.2 Select DNS Servers.



### 6.3.3 Add the IP address for each DNS server, one per line, then click **OK**.



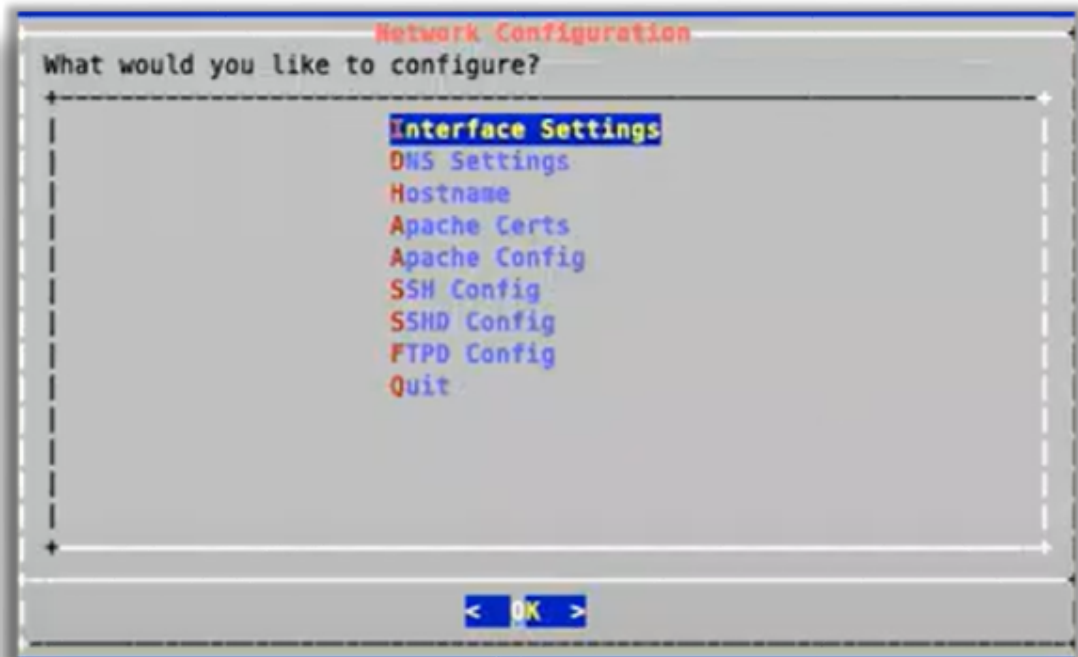
6.3.4 Click **Save**.



6.4 Configure the hostname:

6.4.1 Select the **Hostname** menu to configure settings.

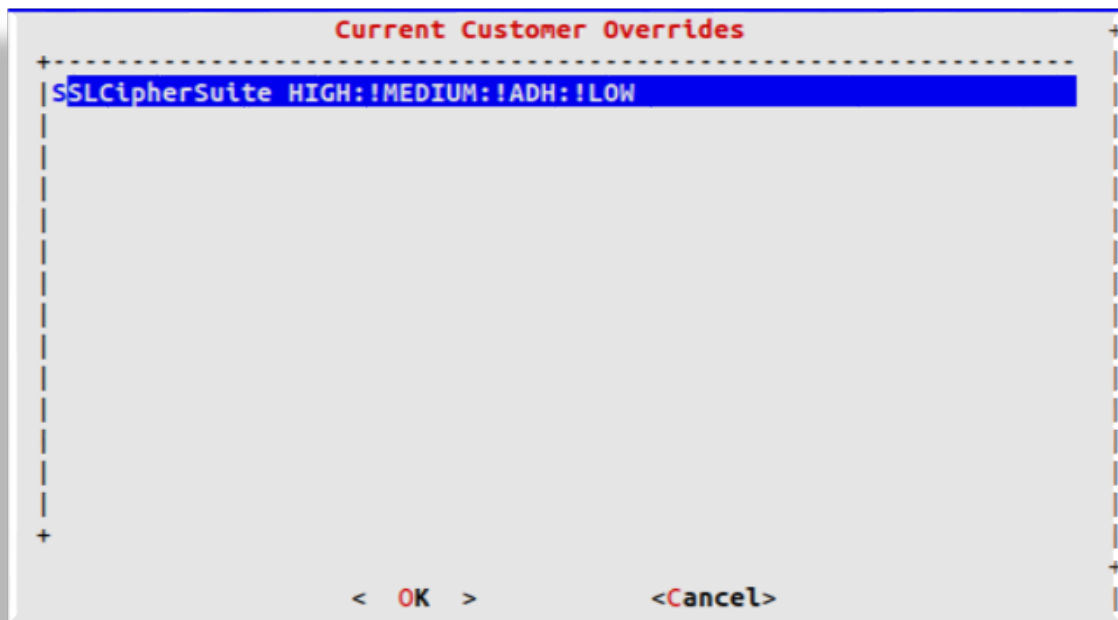
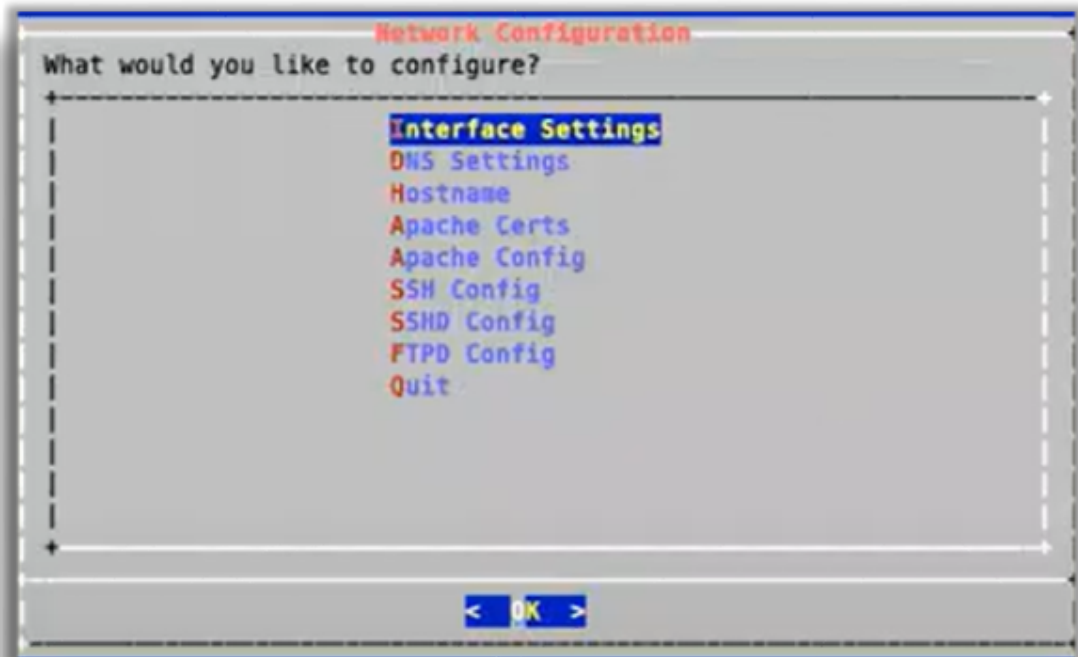
6.4.2 Save to trigger the update. The console displays a message, *Updating hosts*. This setup may take a few minutes.



6.5 Configure Apache. Select the **Apache Config** menu to configure settings.

**Note:**

- SSLCipherSuite defaults to HIGH encryption.
- For SSLProtocol, only TLSv1.2 is supported.
- OpenLDAP defaults to HIGH encryption.
- OpenSSH does not support weak ciphers.



### 6.6 Configure SSH.

Select the **SSH Config** menu to configure settings.

Custom entries can be added, if required. The following entries have been added:

```
kexalgorithms
```

(continues on next page)

(continued from previous page)

```
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
hostkeyalgorithms
ssh-rsa
```

### 6.7 Configure SSHD:

Select the **SSHD Config** menu to configure settings.

Multi-line entries can be added, if required. For example, for CUCM v11.5 support, see: [Multi-line CUCM Cipher Support](#).

**Note:** This step is relevant *only* to an Insights Assurance solution and its integration with Cisco UC systems.

This step is *not* relevant to the DS9 and Insights NetFlow solution.

### 6.8 Enable/disable FTPD, or restart the FTPD daemon:

On the **Administration** menu, select **Network Configuration**, then select **FTPD Config**.

**Important:** On new installs, the FTPD daemon is disabled by default.

It is strongly recommended that the FTPD daemon remains disabled, unless there is a good reason you need to use it. It has been seen that enabling the FTPD daemon may introduce a system vulnerability.

FTPD is typically *only* required in rare situations, where FTP is the only way to transfer files to the server. Instead of using FTPD, it is recommended that you use the drop account with SCP or SFTP.



## 7. Base system installation is now complete.

Select **Quit** to exit the **Administration** menu on the console and continue with product registration, and with the configuration of your system through the GUI:

- Insights Dashboard  
See the VOSS Automate Database Setup section in the VOSS Insights Install Guide.
- Insights Arbitrator (relevant only to an Insights Assurance solution and its integration with Cisco UC systems)

See the Install Arbitrator System section in the VOSS Insights Install Guide.

- Insights DS9

---

**Note:** Prior to opening the DS9 GUI, reboot the system.

---

See the DS9 Product Registration and Configuration on the Dashboard section in the VOSS Insights DS9 for NetFlow Install Guide.

### 6.1.2. Multi-line CUCM Cipher Support

This section provides details for the use of the **SSHD Config** menu option.

---

**Note:** This section is not relevant to the DS9 and Insights NetFlow solution. This solution is relevant only to an Insights Assurance solution and its integration with Cisco UC systems.

---

You can copy the keys into the screen in a comma separated list (without spaces).

For CUCM v11.5 support:

```
kexalgorithms diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-  
↪group-exchange-sha1  
ciphers aes128-cbc,3des-cbc,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,  
↪aes256-gcm@openssh.com  
macs hmac-md5,hmac-sha1,hmac-sha2-256,hmac-sha1-96,hmac-md5-96  
hostkeyalgorithms ssh-rsa,ssh-dss
```



## 7. Database and System Setup

### 7.1. Install Arbitrator System

#### 7.1.1. 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 table describes the purpose of the components:

Component	Purpose	Filename
Controls	<p>Controls are actions that the system can automate, user actions to support data collection, analysis before presenting to an operational user as an alert to help reduce user input and provide information and actions faster.</p> <ul style="list-style-type: none"> <li>• Turn an alarm a different color</li> <li>• Push alert to another system such as dashboard server or a correlation server</li> <li>• Auto acknowledge alarms</li> <li>• Email the alert to a destination</li> <li>• Create a ticket with ServiceNow</li> <li>• Pre scripted action based on a response</li> </ul> <p>Other options that can be developed:</p> <ul style="list-style-type: none"> <li>• Using API send the data to another destination</li> <li>• Interact with another system</li> <li>• Run a script to collect additional information</li> <li>• Run a script with actions to change state or configuration</li> </ul>	STDCONTROLS.lxcfg
Probes	<p>A script to poll a system to collect data from a remote system. This is important if the data required can't be streamed from a system to the Arbitrator to be consumed, the Arbitrator and collect data remotely by periodic probing of the system. Examples of probes that collect</p> <ul style="list-style-type: none"> <li>• AXL</li> <li>• API</li> <li>• CLI</li> </ul>	StandardDeploymentProbes.lxcfg PROBES.lxcfg
Response procedures	Contains group of controls that are assigned to the policies.	
Policies	A set of rules for the data that is turned into 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.	SiteStats_08122020.lxcfg POLICIESUCCE221020.lxcfg POLICIESCUCM221020.lxcfg POLICIESCUCIMP221020.lxcfg PINGMON.lxcfg

## 7.1.2. Installation Steps

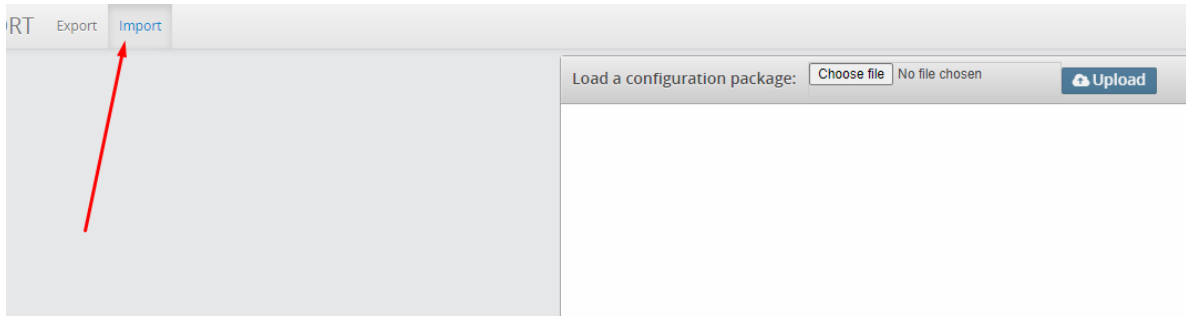
1. Log in to the Arbitrator: admin/admin
2. Click the Wrench icon.



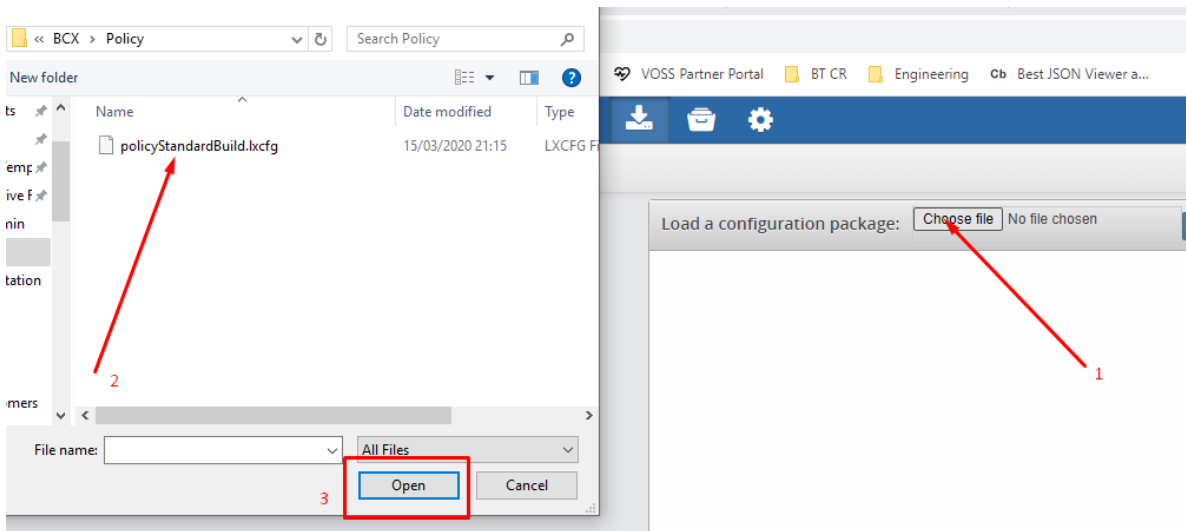
3. Click on the icon shown below



4. Click **Import**,



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



6. Ensure the name of the file you selected displays adjacent to **Choose file**, then click **Upload**.

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

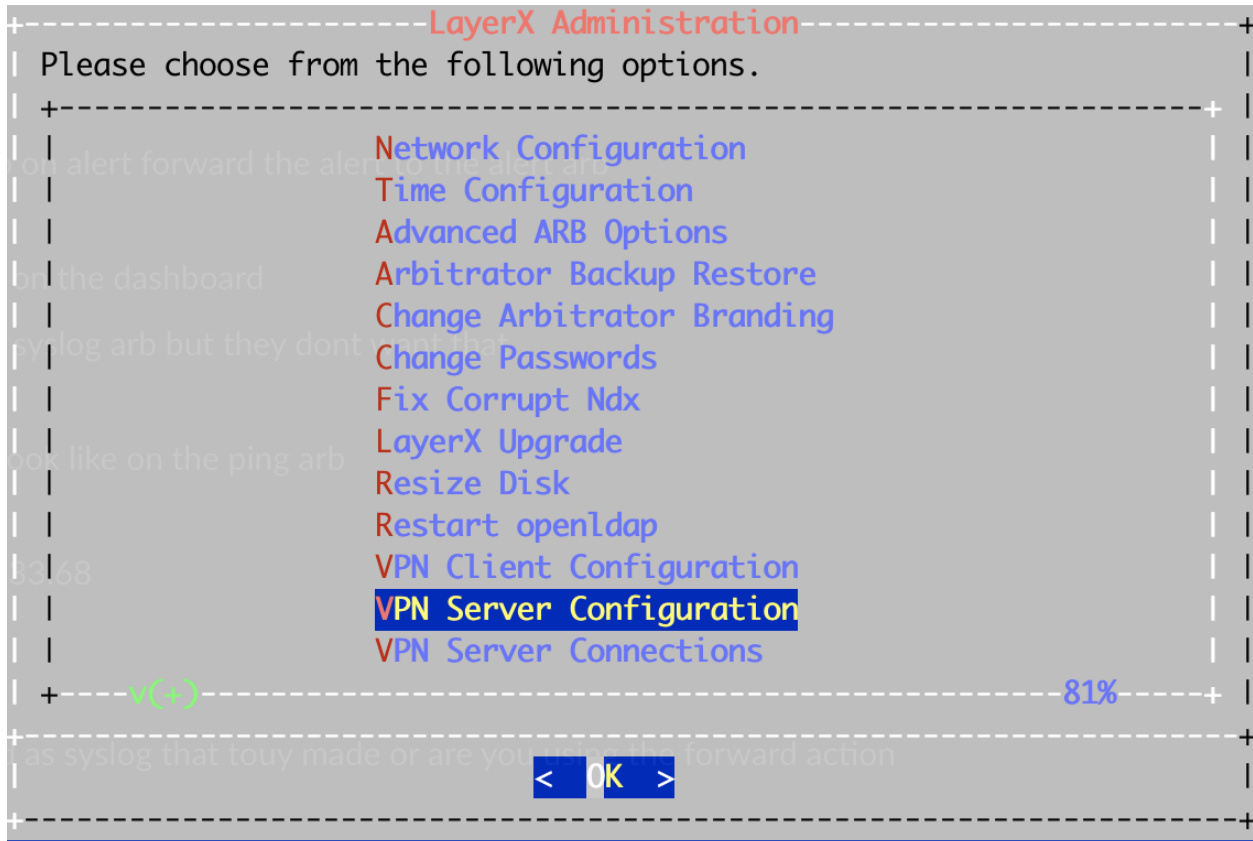
8. Repeat this procedure for the following:

- **Controls**
- **Probes**
- **Response Procedures**
- **Policies**

See: *Policy Configuration Files*

## 7.2. Set up Arbitrator to Arbitrator Communication

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



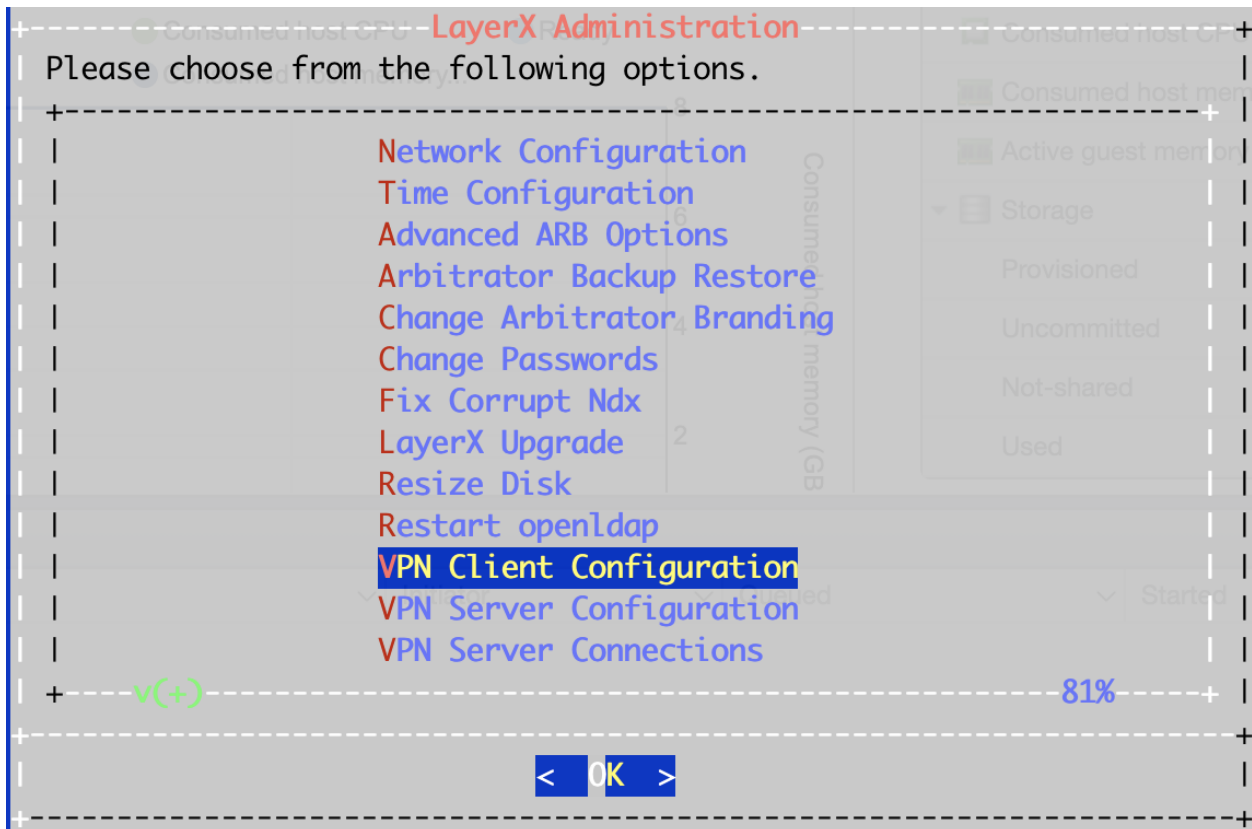
Then Clear Fabric Configuration, then reset this up:

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

As shown in the example below:

```
-----LayerX System Configuration-----+
| Please choose from the following options. |
|-----+
| | Organization Name | LAYERX |
| | Public Address | 192.168.103.17 |
| | Authorized Client Port | 62003 |
| | Negotiation Port | 62004 |
| | VPN Subnet | 2 |
| | Ethernet Interface Number | 0 |
| | Clear Fabric Configuration |
| | Done |
| | |
| | |
|-----+
|-----+
| < OK > |
|-----+
|-----+
```

On the subordinate Arbitrator log in as admin and navigate to VPN Client Configuration



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?

2. Insert the name of the Central ARB      Click here then click save

Ensure as event is ticked

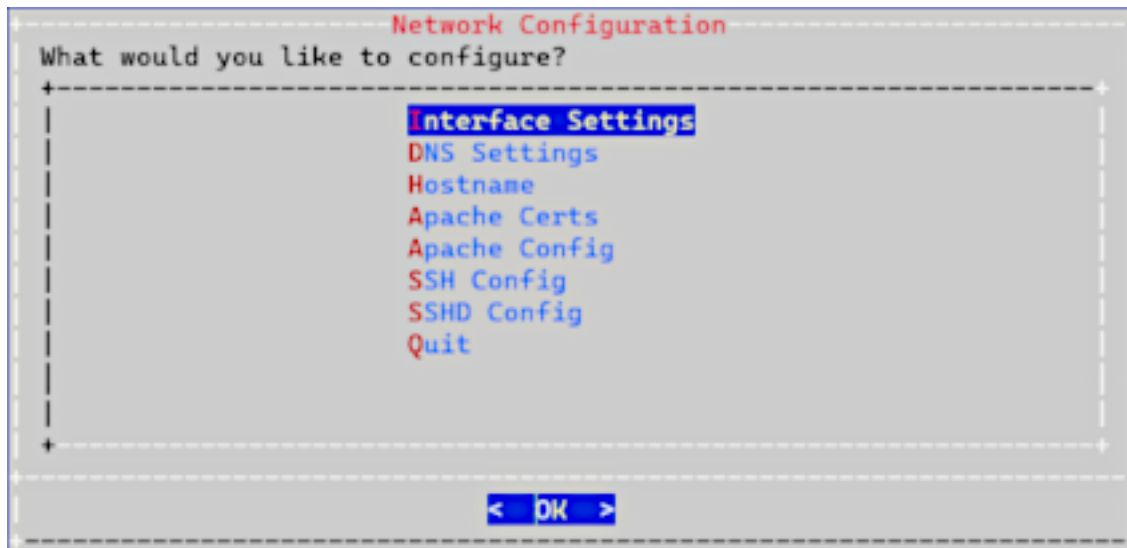
1. Click Forwarder to add

---

## 8. Certificates

### 8.1. Add or Update Certificates

Users can now update SSL Certificates and SSL keys from the Admin console menu.



#### 8.1.1. Add Certificates

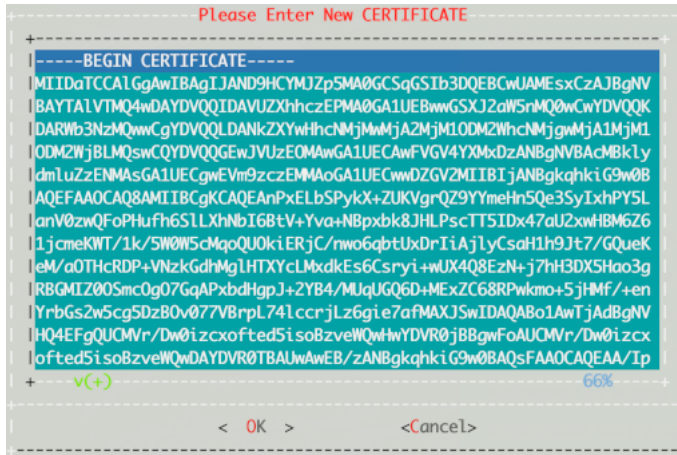
To add your own certificate, you will need both the certificate and private key.

1. SSH to the system using admin account
2. Select **Network Configuration**
3. Select **Apache Certs**
4. Select **Insert Cert**
5. Paste in customer certificate

A certificate has the following header and footer

```
--BEGIN CERTIFICATE--  
--END CERTIFICATE--
```





#### 6. Select **Insert Private Key**

#### 7. Paste in customer private key

A private key has the following header and footer

```
--BEGIN PRIVATE KEY--
--END PRIVATE KEY--
```



#### 8. Select **Display Cert Details** to view certificate details.

#### 9. Select **Back** and exit the menu.

#### 10. Refresh the browser. The system should be using the new certificate.

### 8.1.2. Update Certificates

If you want to generate a new unsigned certificate or to reset a certificate and private key:

1. SSH to the system using admin account
2. Select **Network Configuration**
3. Select **Apache Certs**
4. Select **Generate New Unsigned Cert**

5. When prompted, fill in the information requested.

```
Generating a 2048 bit RSA private key
.....+
.....+
writing new private key to '/etc/apache2/server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

6. Select **Back** and exit the menu.
7. Refresh browser. The system should be using the new unsigned certificate.

## 9. CUCM Asset Onboarding

### 9.1. Customer Onboard

#### 9.1.1. Add Customer CDR Folders

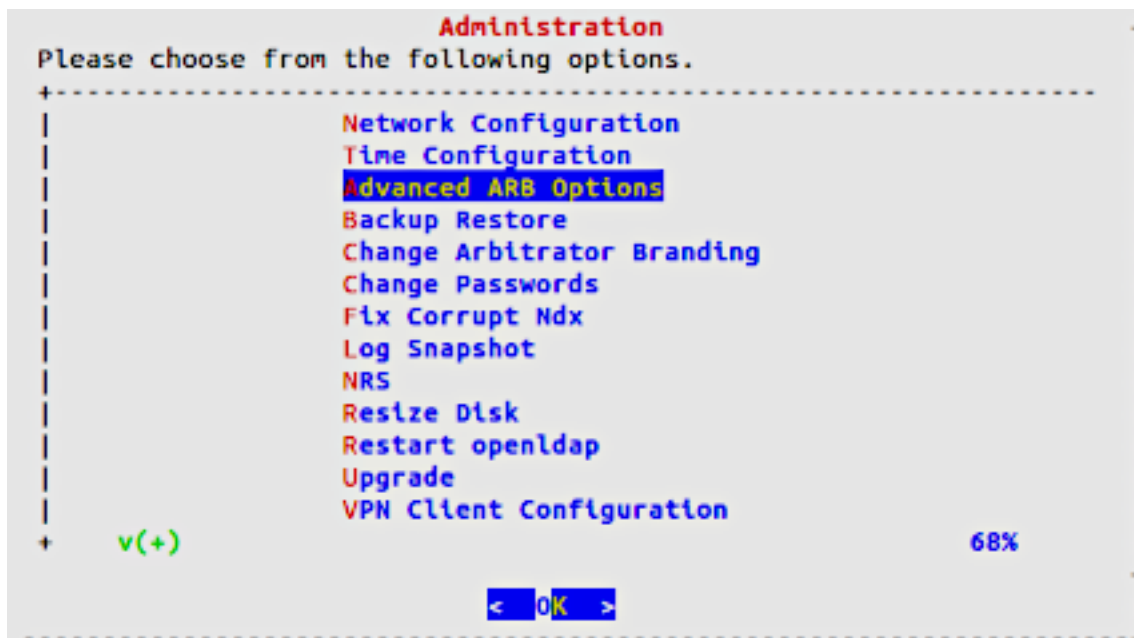
1. Log in via the command line interface to the Arbitrator selected to receive CDR data from call managers:

- Cisco UCM
- Oracle Call Manager

The entered call manager IP address name serves as a CDR folder name for incoming CDRs.

The steps below show the menus for the selected call manager to be configured.

2. Use the admin credentials to log in and navigate to Advanced Arb Options.



```
March 03, 2023 09:31 AM 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
```

3. Select **Configure networking**

```
March 03, 2023 09:31 AM 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
```

4. On the **Network Menu**, select **Configure services**.

```
March 03, 2023 09:32 AM UTC
Services Menu

Please be careful.

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

5. Select the required service to configure:

```
March 03, 2023 09:33 AM UTC
Cisco Services Menu
Please be careful.
1) Configure Cisco Call Managers
0) Back
```

```
March 03, 2023 09:32 AM UTC
Oracle Services Menu
Please be careful.
1) Configure Oracle Call Managers
0) Back
```

6. On the selected service, select the required Call Manager.

```
March 03, 2023 09:34 AM UTC
Cisco Services Menu
Please be careful.
1) Configure Cisco Call Managers
0) Back
```

```
March 03, 2023 09:33 AM UTC
Oracle Services Menu
Please be careful.
1) Configure Oracle Call Managers
0) Back
```

7. On the selected Call Manager menu, choose to add a Call Manager.

```

March 03, 2023 09:34 AM UTC

Cisco Call Manager Menu

View Add, Delete, or Clear Cisco Call Manager configuration here.

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

```

```

March 03, 2023 09:35 AM UTC

Oracle Call Manager Menu

View Add, Delete, or Clear Oracle Call Manager configuration here.

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

```

8. In the editor, add the IP Address of the call manager then press **<CTRL>-X** to save.

```

# Any line that begins with a # will be ignored.
#
# Enter a unique ip address or customer name, one cisco call manager per line.
# This will create a directory under the "cucn" and "cme" directories for
# each respective cisco call manager.
# This identifier can be used for multitenancy purposes. Choose wisely.
#
# On the cisco call manager, the location to use would be similar to the following:
#   sftp://<arbitrator ip address>:cucn/<name>

-- Press <CTRL>-X to save and quit. --

```

```

# Any line that begins with a # will be ignored.
#
# Enter a unique ip address or customer name, one oracle call manager per line.
# This will create a directory under the "sbc" and "sbc" directories for
# each respective oracle call manager.
# This identifier can be used for multitenancy purposes. Choose wisely.
#
# On the oracle call manager, the location to use would be similar to the following:
#   sftp://<arbitrator ip address>:sbc/<name>

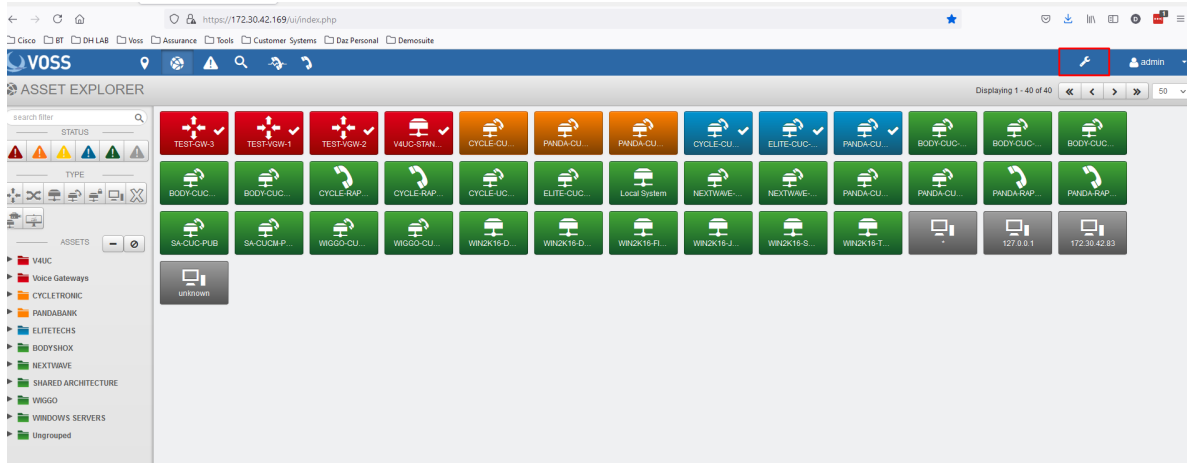
-- Press <CTRL>-X to save and quit. --

```

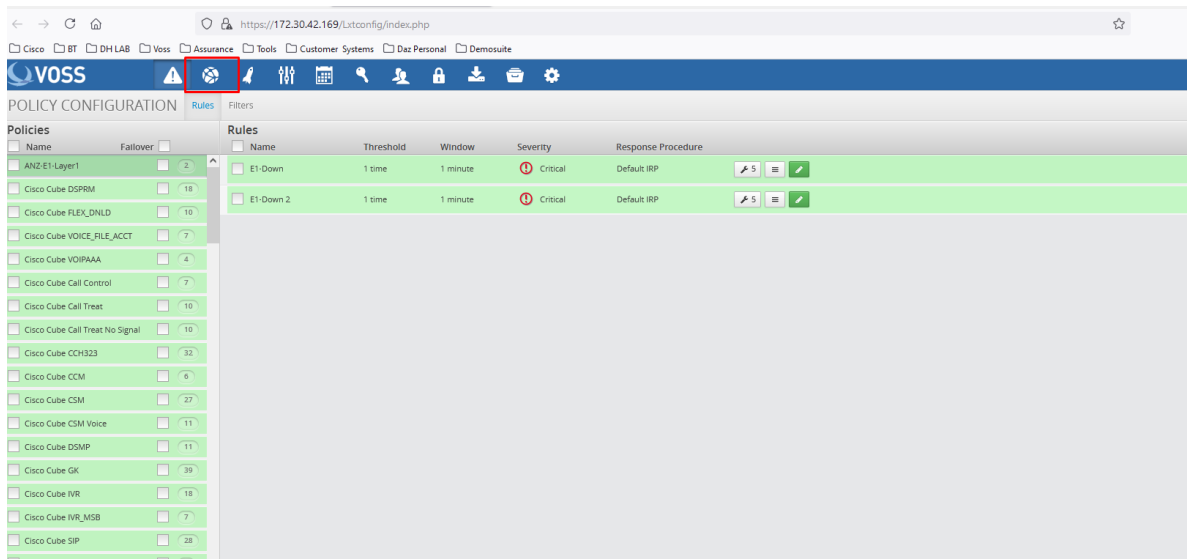
For Collect setup in Arbitrator, see the "Configuration -> Collect" topic in the Arbitrator Administration Guide.

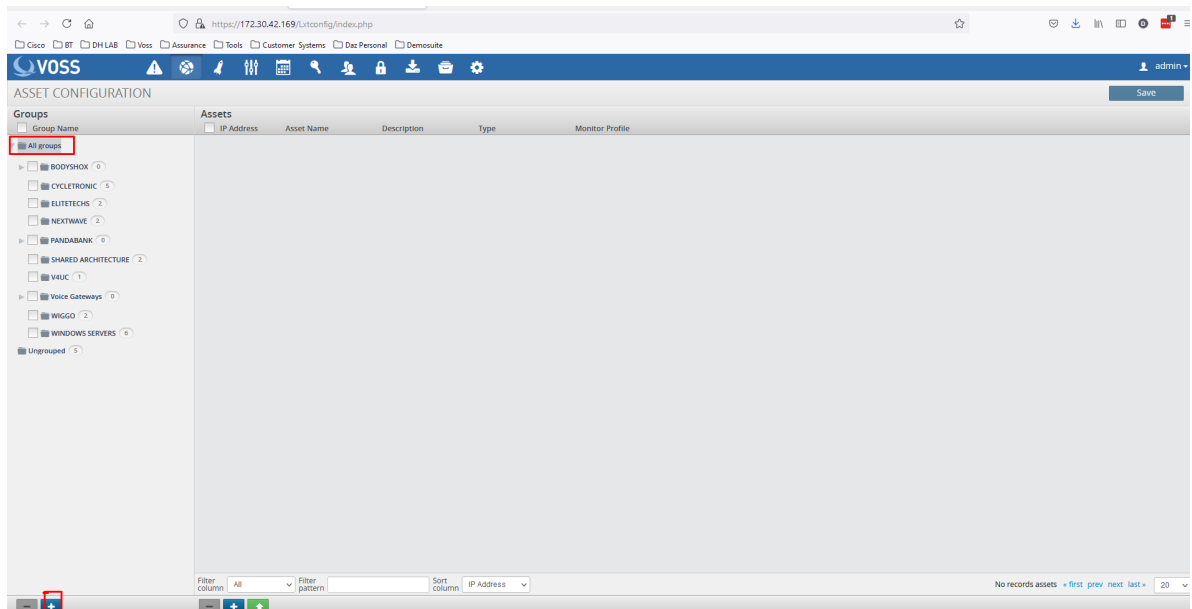
## 9.1.2. Add Customer Assets

1. Log in to the Arbitrator as admin.
2. Click the Wrench icon on the toolbar.



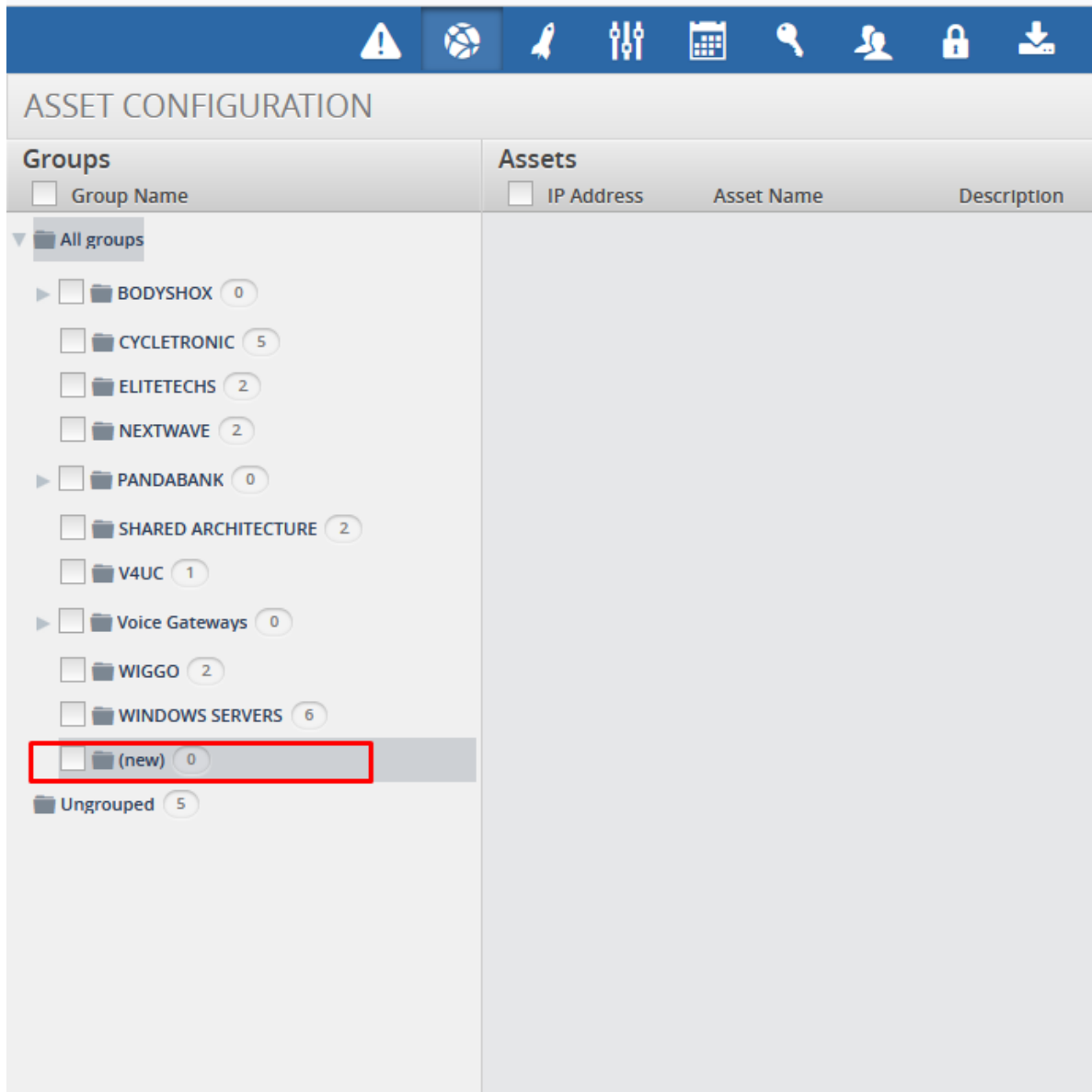
3. Click the Globe icon on the toolbar to open the **Asset Configuration** screen.





4. Select **All groups**, then select the Plus (+) icon to add a new folder.



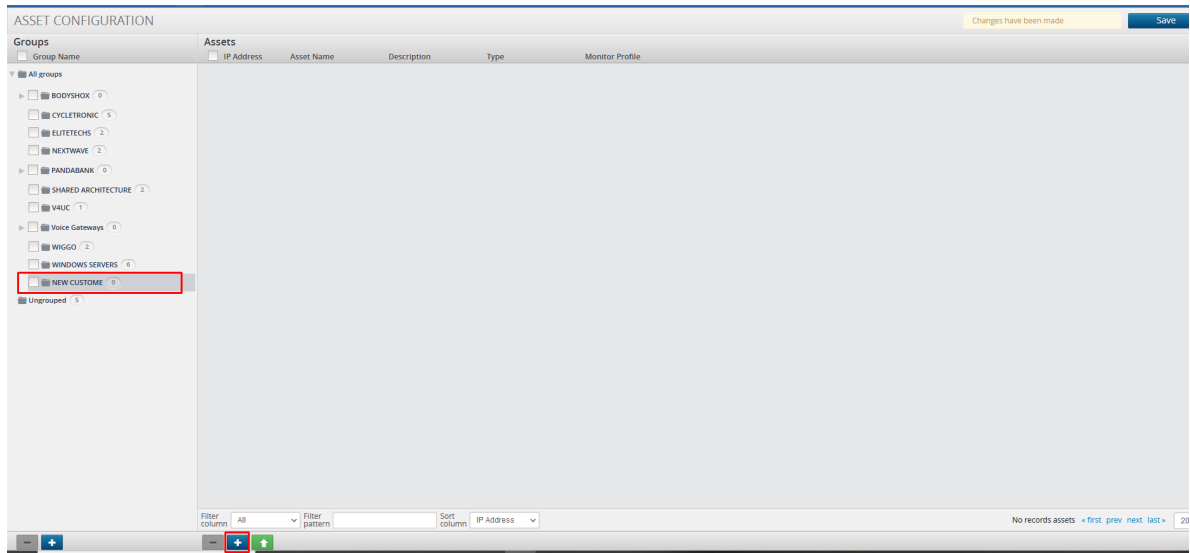


The screenshot displays the 'ASSET CONFIGURATION' interface. At the top, there is a blue navigation bar with several icons: a warning triangle, a globe, a rocket, a wrench and screwdriver, a calendar, a key, a person, a lock, and a download arrow. Below the navigation bar, the main content area is divided into two sections: 'Groups' and 'Assets'.

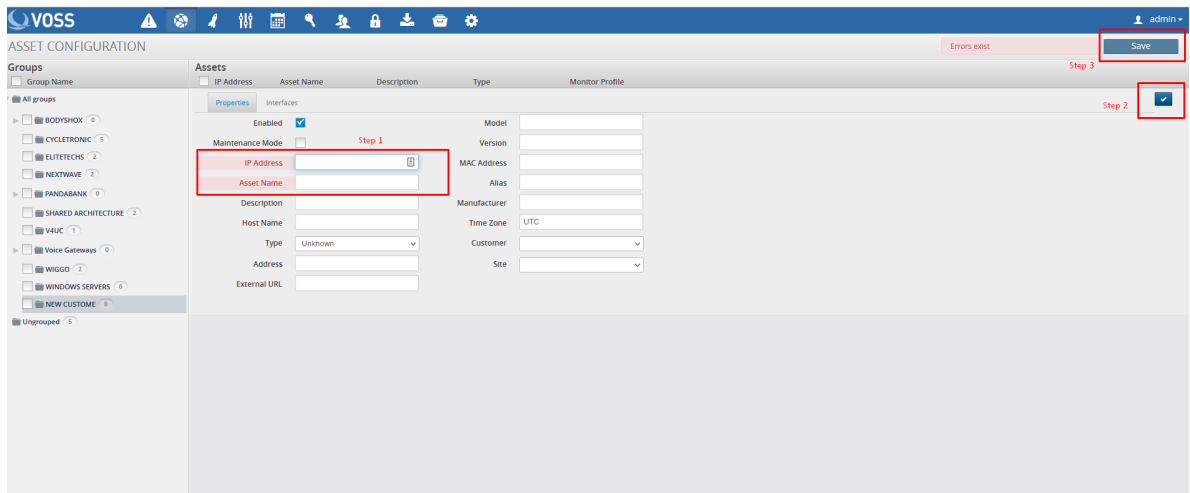
The 'Groups' section has a sub-header 'Group Name' and a list of folders. Each folder has a checkbox, a folder icon, a name, and a count in a circle. The folders are: 'All groups' (expanded), 'BODYSHOX' (0), 'CYCLETRONIC' (5), 'ELITETECHS' (2), 'NEXTWAVE' (2), 'PANDABANK' (0), 'SHARED ARCHITECTURE' (2), 'V4UC' (1), 'Voice Gateways' (0), 'WIGGO' (2), 'WINDOWS SERVERS' (6), '(new)' (0), and 'Ungrouped' (5). The '(new)' folder is highlighted with a red rectangular border.


The 'Assets' section has a sub-header 'IP Address' and a table with columns for 'Asset Name' and 'Description'. The table is currently empty.

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



5. Select the new folder, and click the Plus icon (+) in the right pane.



- Fill out the IP address (mandatory).
- Fill out the asset name (mandatory).
- Fill out any other information you have into the relevant fields.
- Click the Checkmark .
- Click **Save**.

6. Repeat the above for all assets you wish to monitor. Alternatively, you can upload multiple assets using a CSV import.

## CSV Import of Assets

See also the Asset Configuration section in the Arbitrator Administration Guide.

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	NTIME	ZON	COMMEN	Physical Address
2	MN_10RPP	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
```

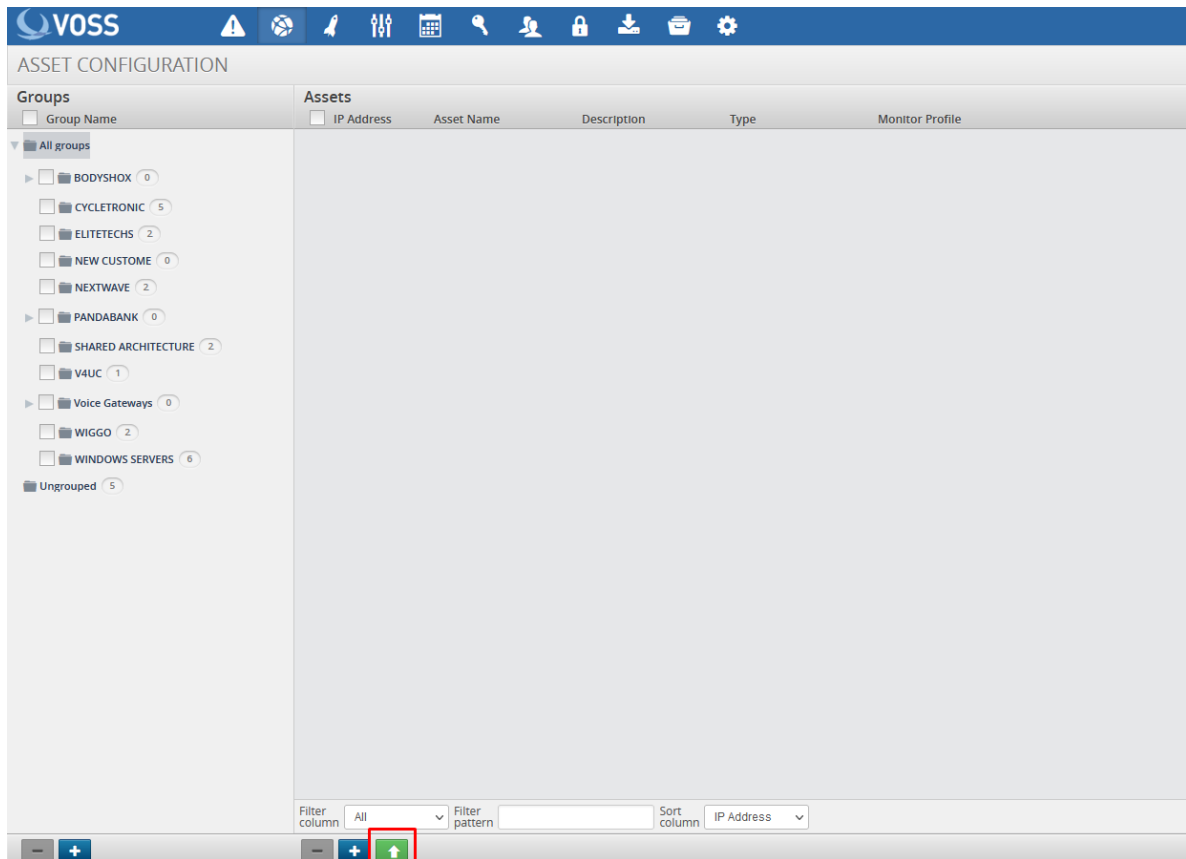
(continues on next page)

(continued from previous page)


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

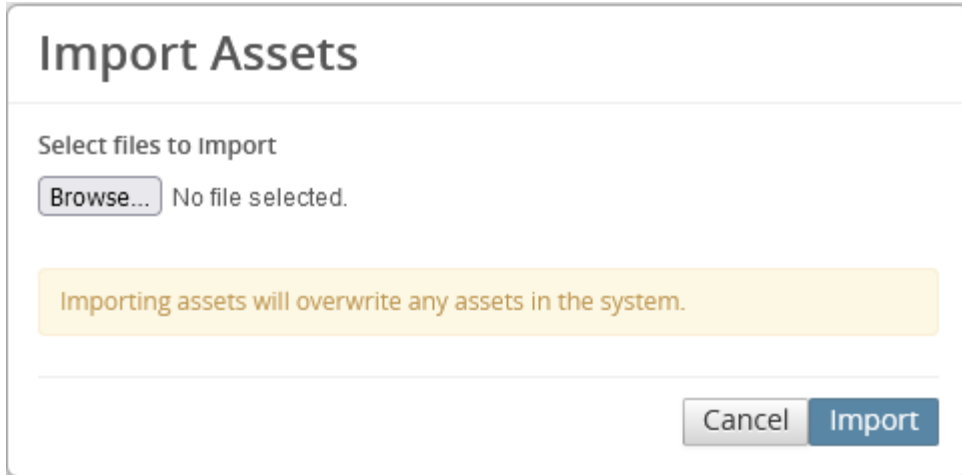
## How to Import using CSV

1. Log in to the Arbitrator with admin privileges.
2. Click the Wrench icon  to open the configuration screen.
3. Click the Globe icon  to open the Asset Configuration screen.

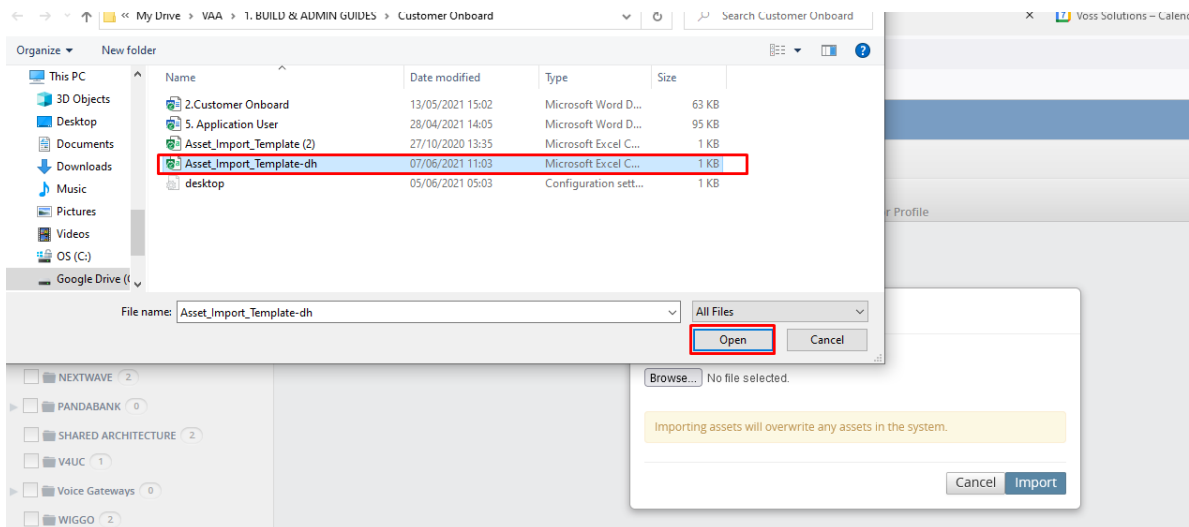


The screenshot displays the VOSS ASSET CONFIGURATION interface. The top navigation bar includes the VOSS logo and several icons. The main content area is divided into two sections: 'Groups' on the left and 'Assets' on the right. The 'Groups' section shows a tree view of asset groups, including 'All groups', 'BODYSHOX', 'CYCLETRONIC', 'ELITETECHS', 'NEW CUSTOME', 'NEXTWAVE', 'PANDABANK', 'SHARED ARCHITECTURE', 'V4UC', 'Voice Gateways', 'WIGGO', 'WINDOWS SERVERS', and 'Ungrouped'. The 'Assets' section is currently empty. At the bottom of the interface, there are filter and sort options. A red box highlights the 'Up Arrow' icon in the bottom right corner of the interface.

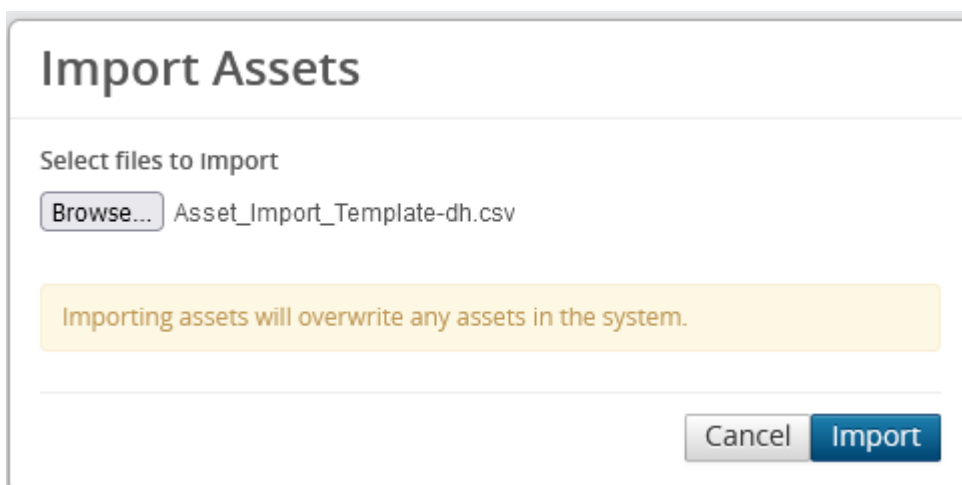
4. Click the Up-arrow  to open the **Import Assets** dialog.



5. Browse to your csv file.



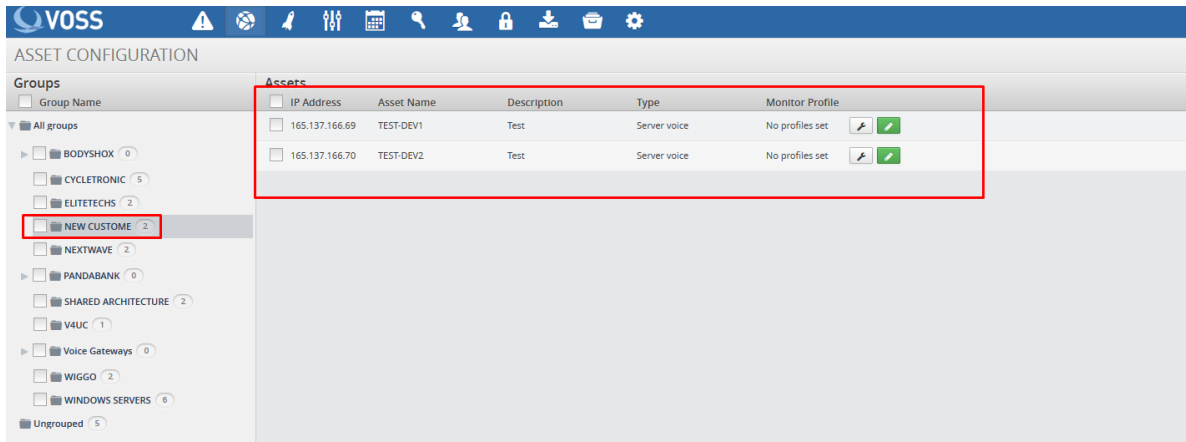
6. Click **Open**.



7. Click **Import**



Once the Import is complete, check the **Asset Configuration** screen to confirm your assets are

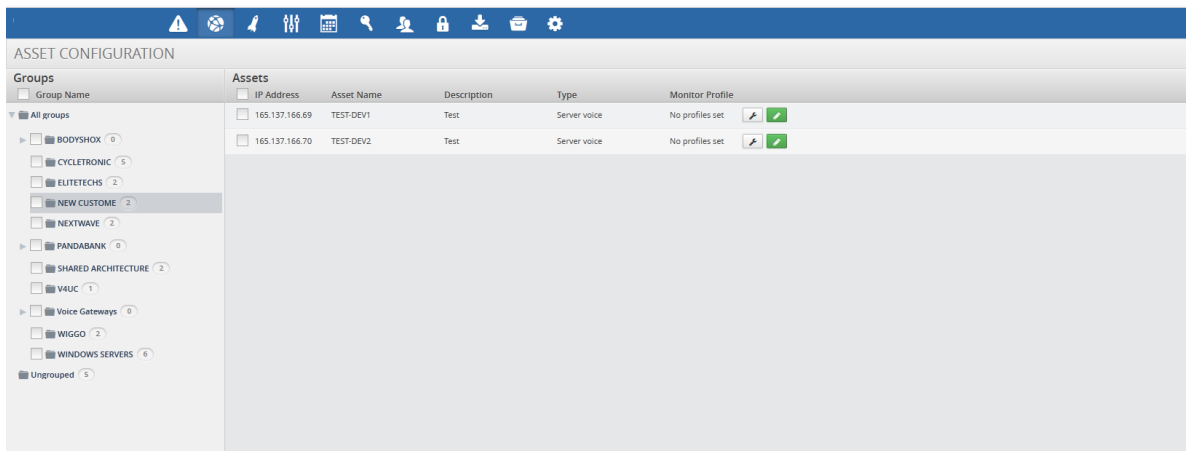
present and in the correct location.



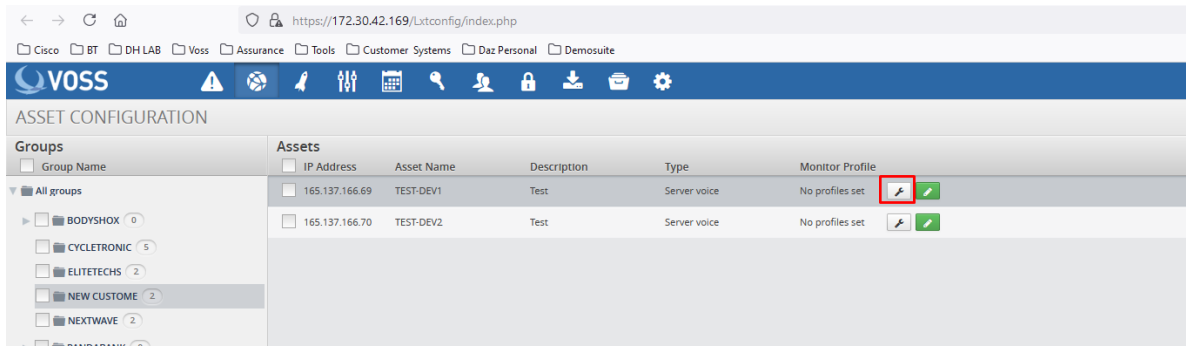
### 9.1.3. Assigning Probes to Assets

#### Assign Standard Probes

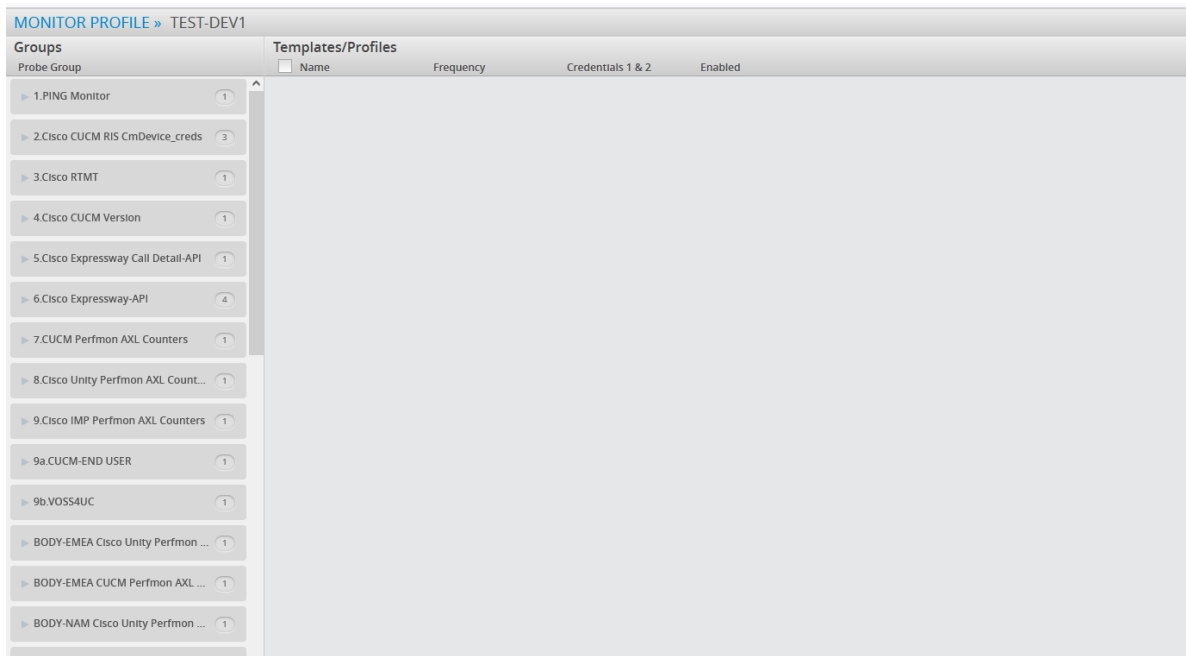
1. Log in to the Arbitrator with admin privileges.
2. Click on the  to open the configuration screen.
3. Click on the  to open the Asset Configuration screen.
4. Select the Asset Group that contains the assets you wish to configure



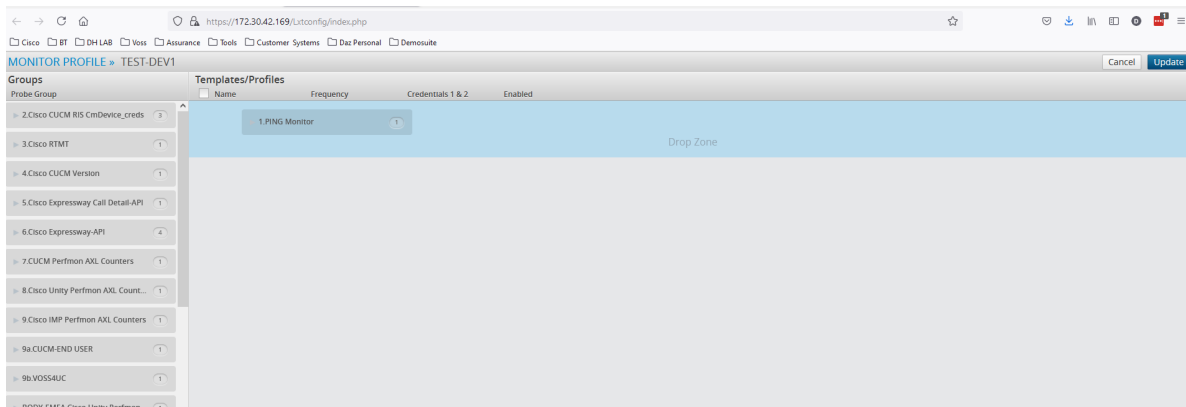
5. Click on the wrench icon as shown below.



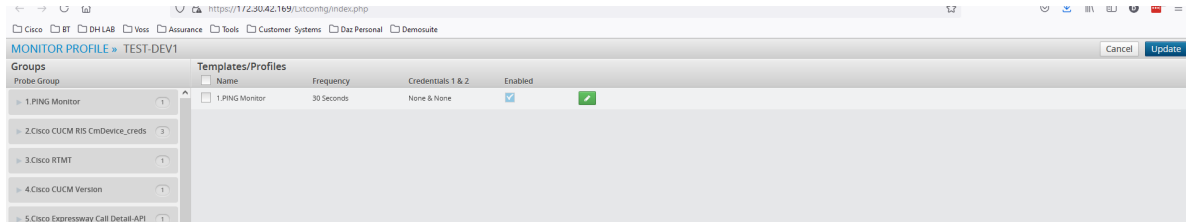
This will then open the Assignment screen.




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.



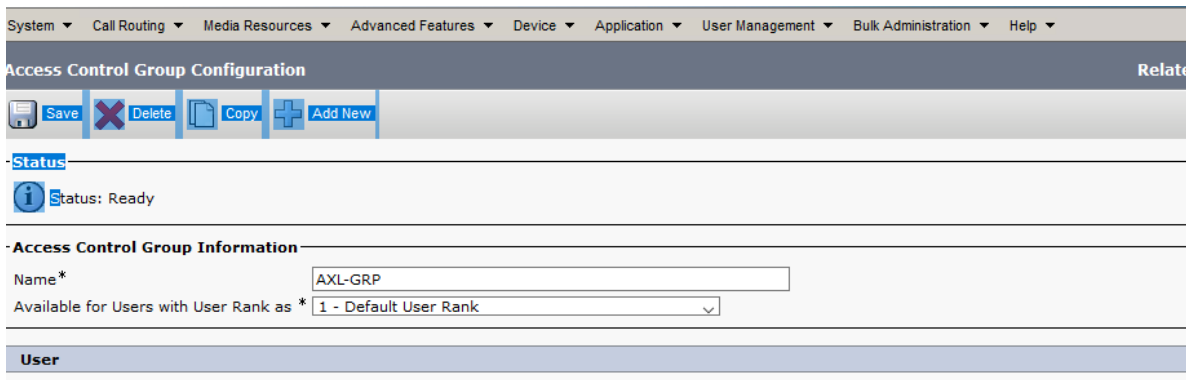
8. If you then click on  you can set any time schedules / credentials required for this probe
9. Once finished click **Update** and then click **Save**.

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

## 9.2. Call Manager Configuration

### 9.2.1. 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.



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

Save

\*- indicates required item.

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

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

## 9.2.2. 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](#) \*

**Cisco Syslog Agent**

<a href="#">Remote Syslog Server Name 1</a>	62.7.201.25
<a href="#">Remote Syslog Server Name 2</a>	217.32.186.230
<a href="#">Remote Syslog Server Name 3</a>	

## 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	
<a href="#">CDR Enabled Flag</a> *	True
<a href="#">CDR Log Calls with Zero Duration</a> *	True
Clusterwide Parameters (Device - General)	
<a href="#">Call Diagnostics Enabled</a> *	Enabled Only When CDR Enabled Flag is True

## CUCM Serviceability

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

Alarm ▾ Traces ▾ 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"/>	<a href="#">Reset</a>

[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"/>

# Index

## F

### Flowchart

- Insights Arbitrator for Assurance Setup,  
3
- Insights Arbitrator Integration for  
Assurance, 4
- Insights Assurance Setup Overview, 2
- Insights Dashboard for Assurance Setup,  
5