VOSS Insights
Arbitrator Install Guide

Release 25.2

August 27, 2025

Legal Information

DOCUMENT ID: 20250827112631

Contents

1. What's New

1.1. Arbitrator Install Guide: Release 25.2

- EKB-24083: Remove default admin:admin user created as part of Insights installation. See: *Deploy and VM installation*

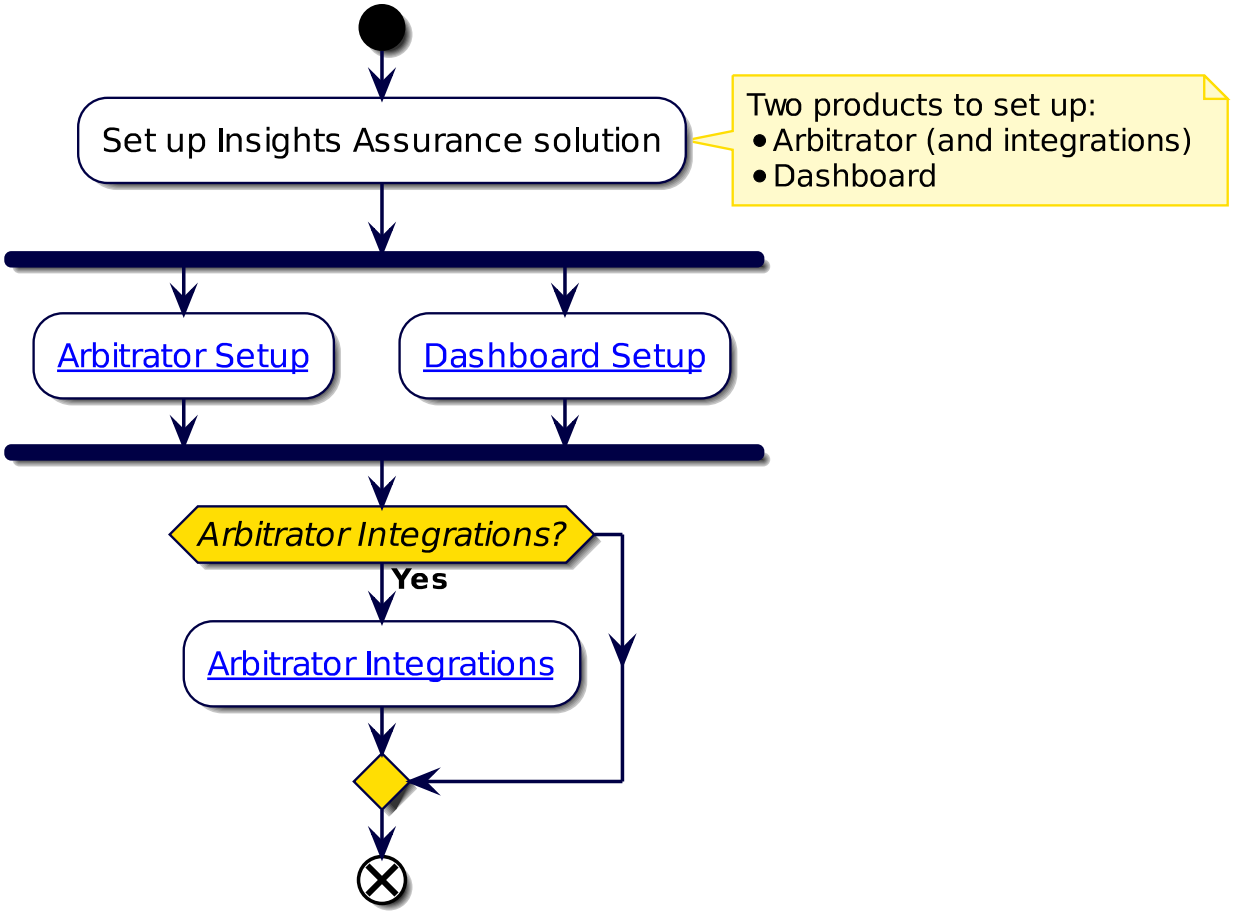
  Added steps for creating GUI admin passwords for Arbitrator and Dashboard.

- EKB-25315: Insights server certificate upload to support SSL certificates using 4096-bit encryption. See: *Add or update certificates*

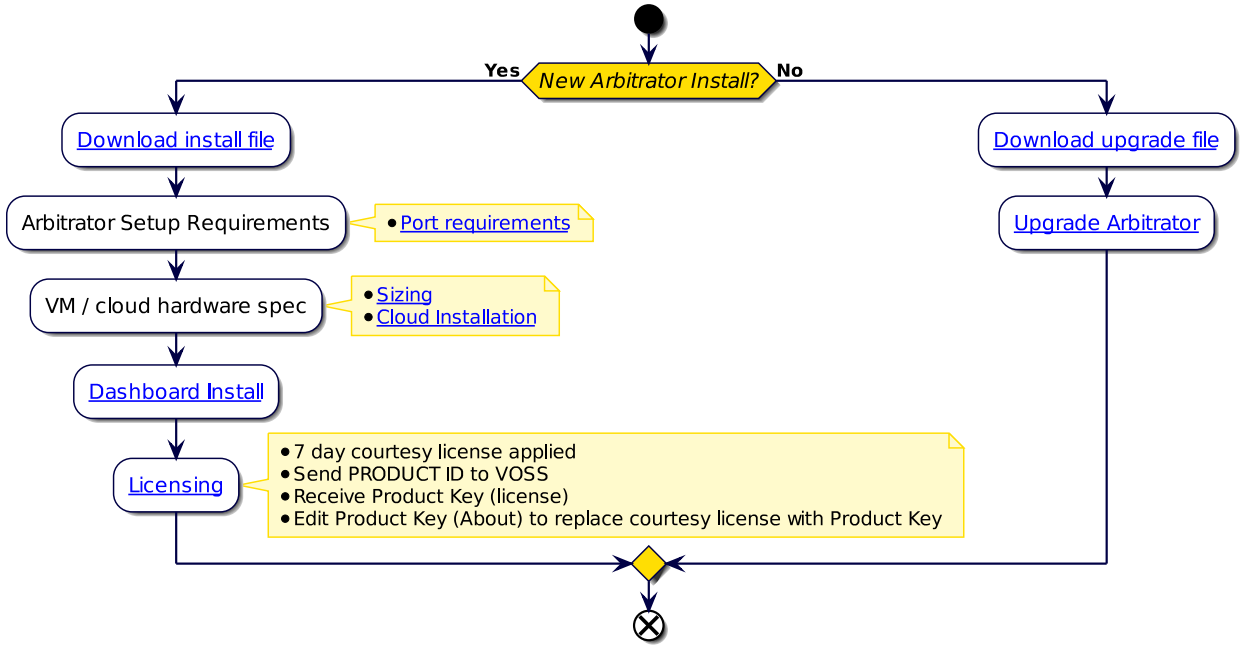
  Added details on the support for SSL certificates using 4096-bit encryption.

2. Insights Assurance Quickstart

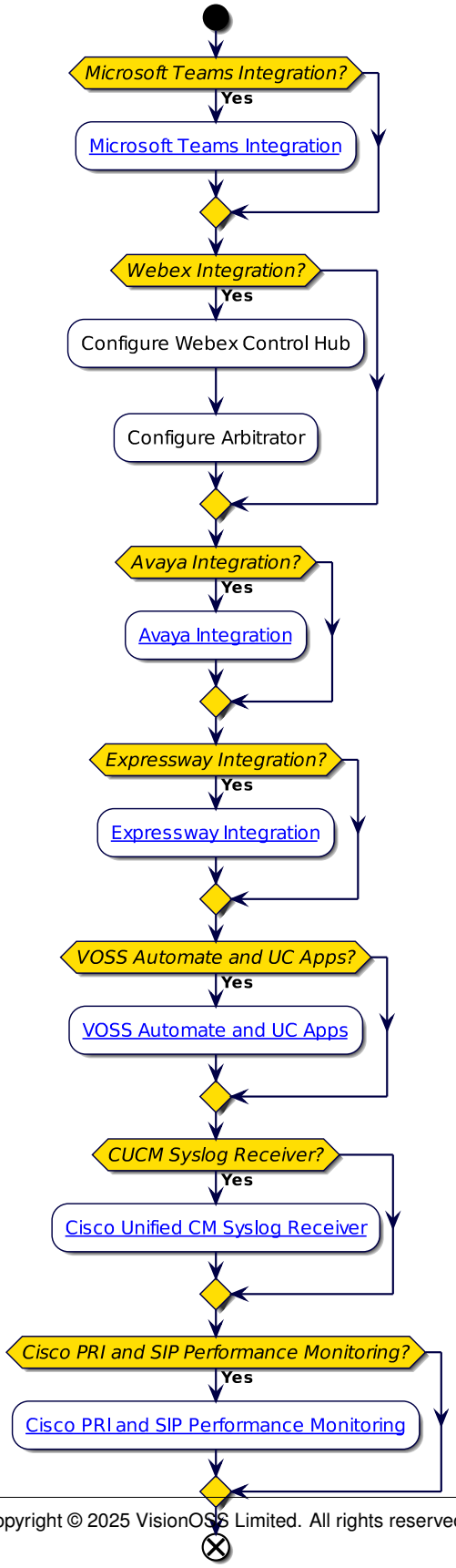
2.1. Insights Assurance Setup Overview



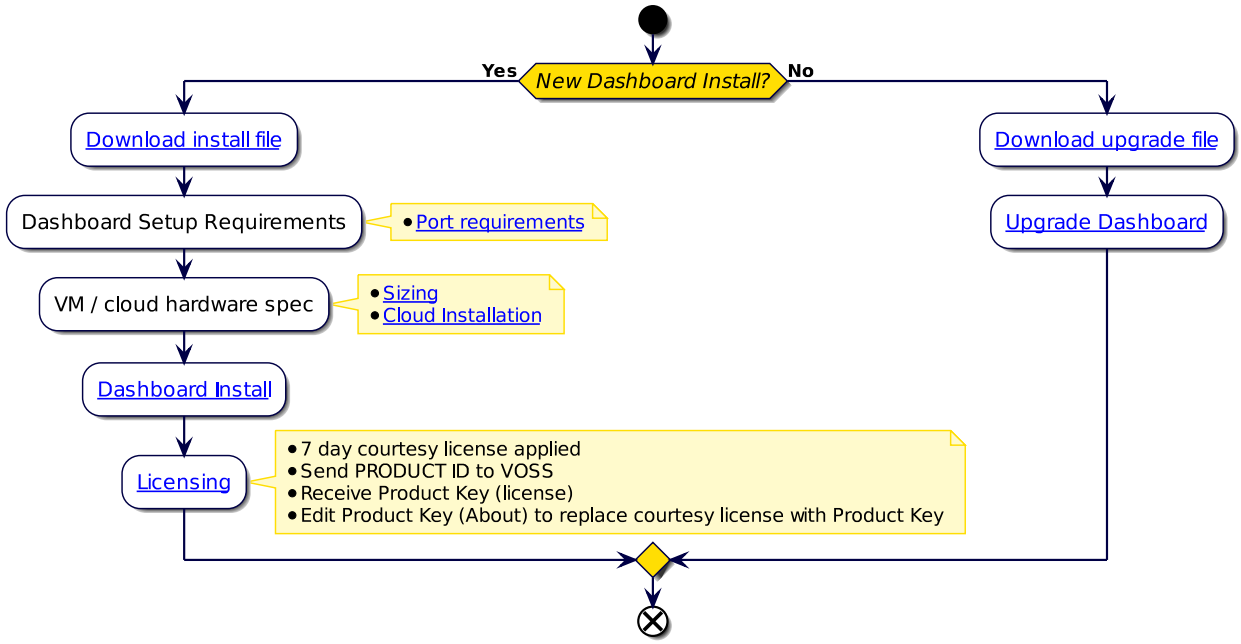
2.2. Arbitrator Setup



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
- Microsoft Teams 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:
  1. Log in on the VOSS Customer Portal
  2. Go to **Downloads > VOSS Insights > Insights Arbitrator Hawaii > <release number> > Upgrade**.
  3. Download the `.lxsp` upgrade file.
  4. Verify that the original `.sha256` checksums on the download site server match.

     system checksum media/<lxsp_file>

     `Checksum: <SHA256>`

4. VMWare Specification and Requirements

4.1. Arbitrator VM Sizing Specifications

Size	Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Stor-age (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.

Dashboard Server VM		**DS9 NetFlow Collector Bare Metal Server 1 (Dell R740 or Equivalent)**	
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	

		Bare Metal Server 2 (Dell R740 or Equivalent)	
		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

Product	Size	Cloud VM Specification
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, 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	443, 5432, 5000, 60514, 64514, 64515, 65515, 65516, 64005, 64004, 62009, (all TCP)	Intra-system communication and queries - Bi-directional
Arbitrator Server	Arbitrator Server	62002, 62003, 62004, 62005, 62006, 11501,30501, 30503, 40501, 40503 (all TCP)	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

Note: LDAP ports: 389 and 636 for TCP/UDP are not available for the Arbitrator and Dashboard server. If these ports are required for Dashboard server communication, refer to the configuration settings for LDAP in the **Configuration** chapter the *Dashboard Administration Guide*.

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
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
Arbitrator	Microsoft (https://graph.microsoft.com/v1.0)	443 TCP	The Arbitrator pulls the full call record details directly from Microsoft, using the https://graph.microsoft.com/v1.0 API.

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 repository access
Dashboard Server	DS9	TCP	8082	Unidirectional	Data repository 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	**Dashboard** Server	TCP	22	Unidirectional	SSH (remote CLI access) and file transfer
Admin users	**Dashboard** Server	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:

1. *Step 1: Download OVA*
2. *Step 2: Deploy the OVA*
3. *Step 3: Run the VM*
4. *Step 4: Log in to the Administration console*
5. *Step 5: Change the admin user password*
6. *Step 6: Configure network settings*
7. *Step 7: Create GUI admin password for Arbitrator and Dashboard*

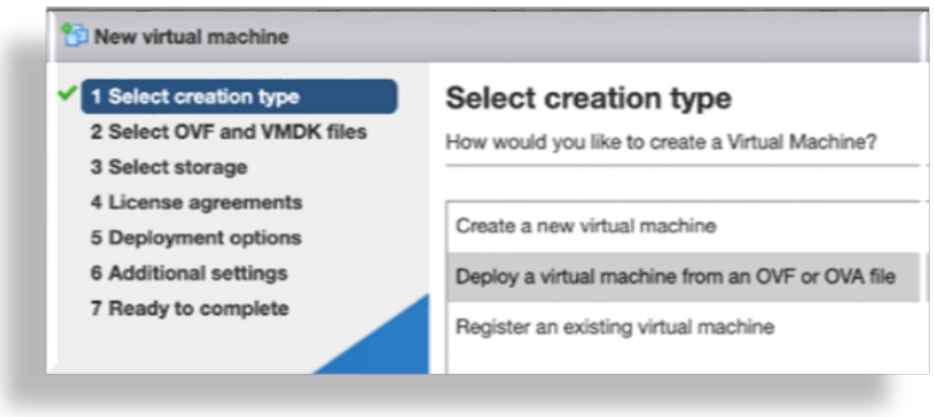
Step 1: Download OVA

1. Download the OVA for your system to a directory accessible by the VM client.

Step 2: Deploy the OVA

To deploy the OVA:

1. Select the downloaded OVA file, and choose a VM name.



2. On the **Select storage** menu, configure storage settings based on the recommended hardware specifications for the required configuration.

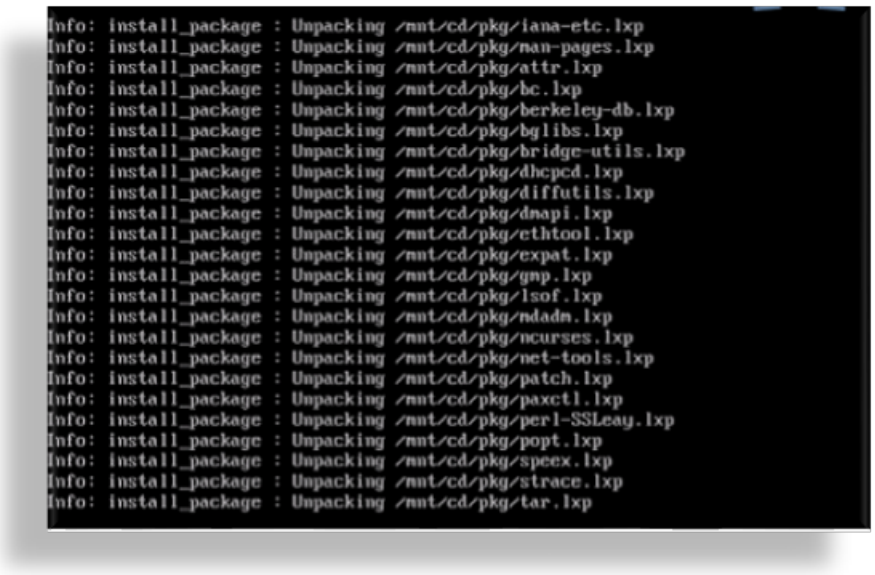
   See the *VMWare Specification and Requirements* for your system.

3. Configure the network mappings based on the recommended hardware specifications for the required configuration.

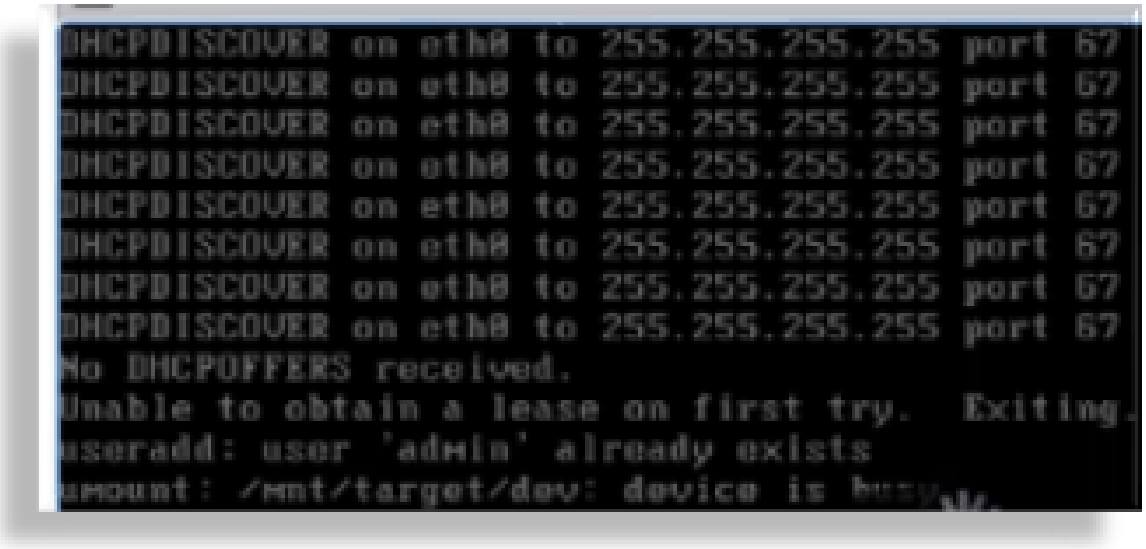
   See the *VMWare Specification and Requirements* for your system.

Step 3: Run the VM

1. Run the VM, and monitor installation of the packages (this may take some time).



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



2. 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>
        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:
```

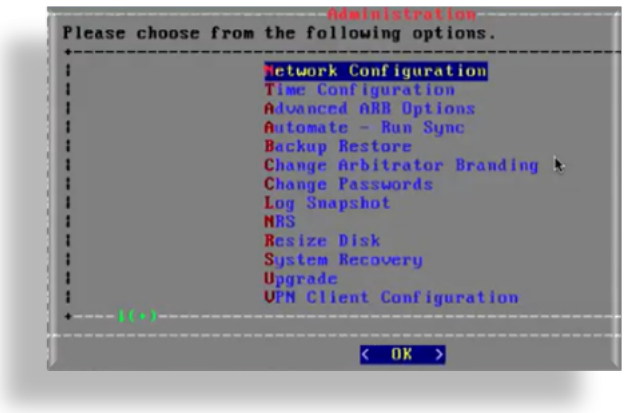
Step 4: Log in to the Administration console

Once the system reboots, you'll need to provide admin user credentials to log in.

1. On the **About** console, at **<hostname> login:**, fill out username `admin`.
2. For the password, use the last *10 characters* of the value at **License**, *excluding the dash*.

> **Important:** The **License** key value displays *only* on the **About** console. When you *ssh* in, it is not visible. For this reason, copy the admin password from the **About** console.
>
> For security purposes, it is recommended that you update this admin password prior to configuring the VMs networking address.

3. View the **Administration** menu, which displays once you're logged in.



Step 5: Change the admin user password

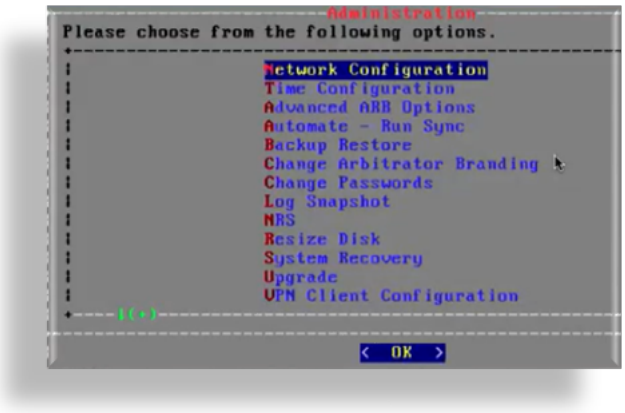
This procedure updates the admin password that is set during the installation process, using the last 10 digits of your license key.

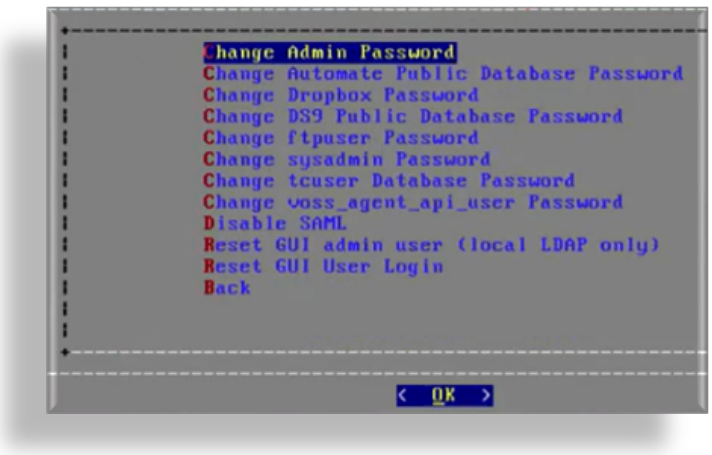
Note: The admin password will need to be updated for all Insights products you install. For security purposes, it is recommended that you update this admin password prior to configuring the VM networking address.

Once you update the password, it is strongly recommended that you make a written or digital copy of any system passwords and share the copies with trusted team members or store them in a secure location from where they may be retrieved if needed.

---

1. On the **Administration** menu, select **Change Passwords**.



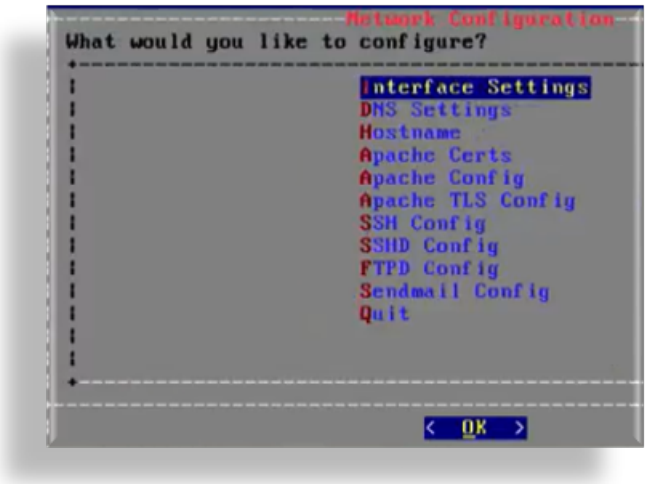


2. Select **Change Admin Password**.
3. Fill out a new password.
4. Save your changes.

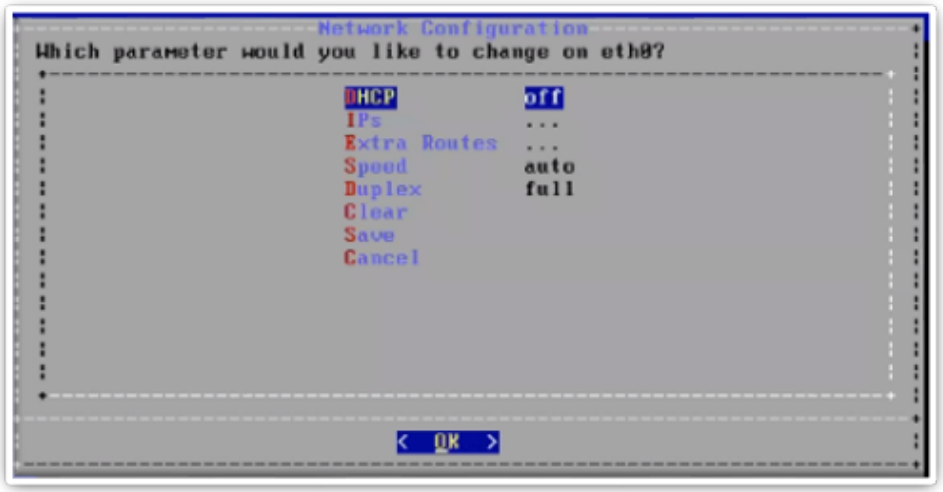
Important: It is strongly recommended that you make a written or digital copy of any system passwords and share the copies with trusted team members or store them in a secure location from where they may be retrieved if needed.

Step 6: Configure network settings

1. On the **Administration** menu, select **Network Configuration**.

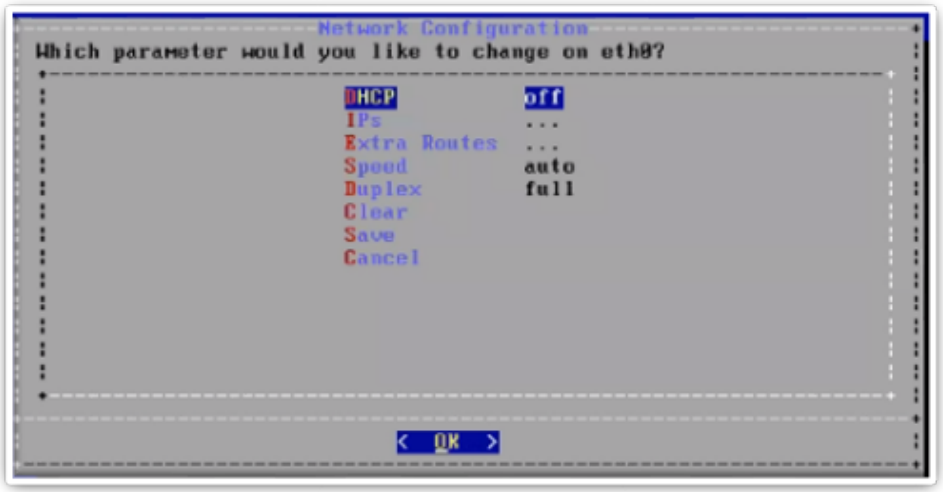


2. Configure interface settings:
   i. Select **Interface Settings**.
   ii. Select the relevant interface.

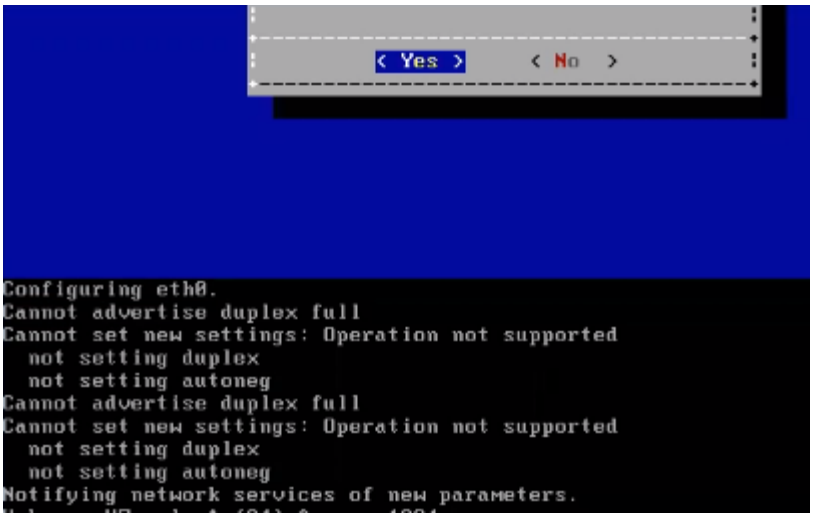


iii. Select **IPs**. Set the IP address and netmask in the format `nn.nn.nn.nn/24`. Click **OK**.

iv. Select **Extra Routes** to configure the default gateway.



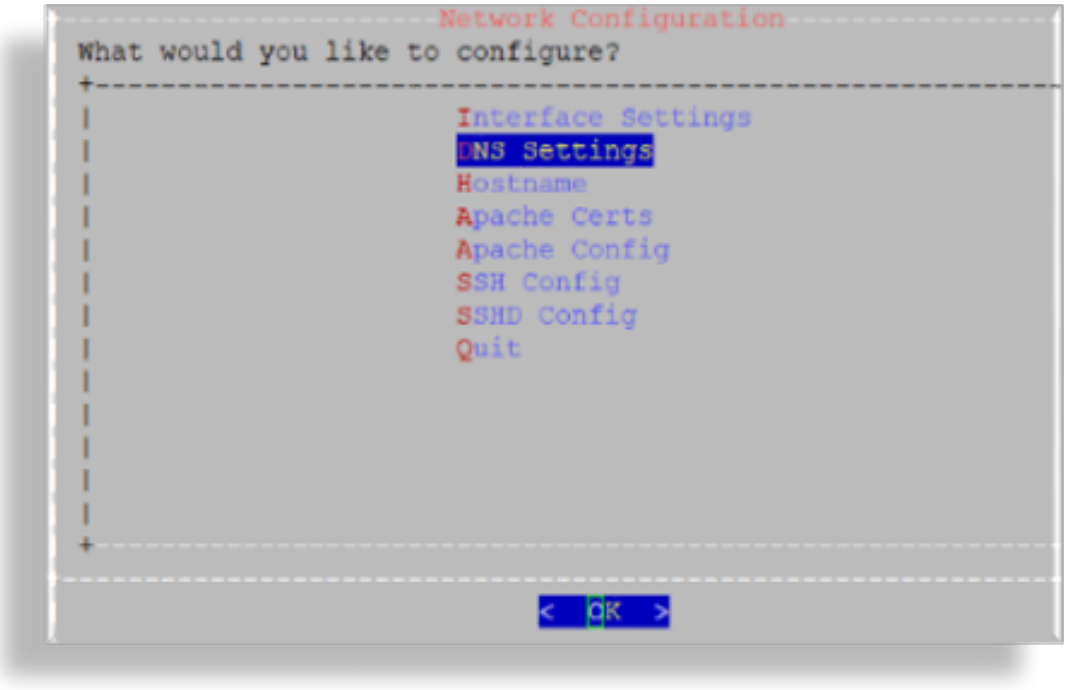
- Use the following format for the entry: *default <gateway IP address>*
- The word *default* is required. For additional route entries use the *<subnet> < gateway>* format. Similar to what would be done on a Linux system at the CLI.



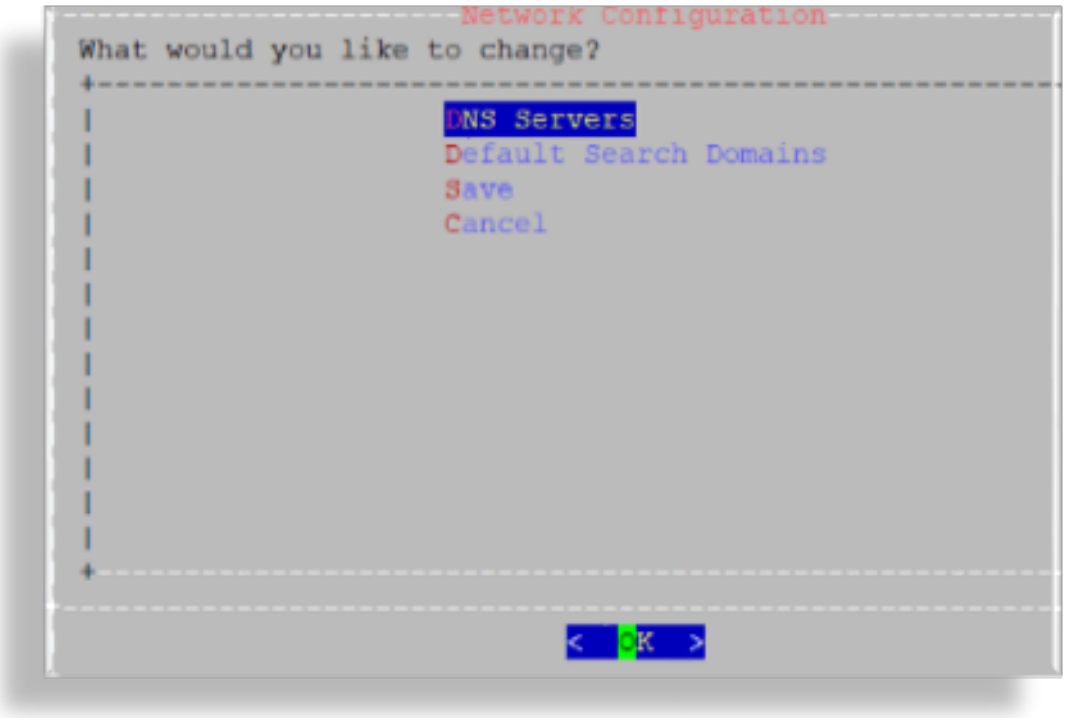
v. Save your changes.

3. Configure DNS settings:

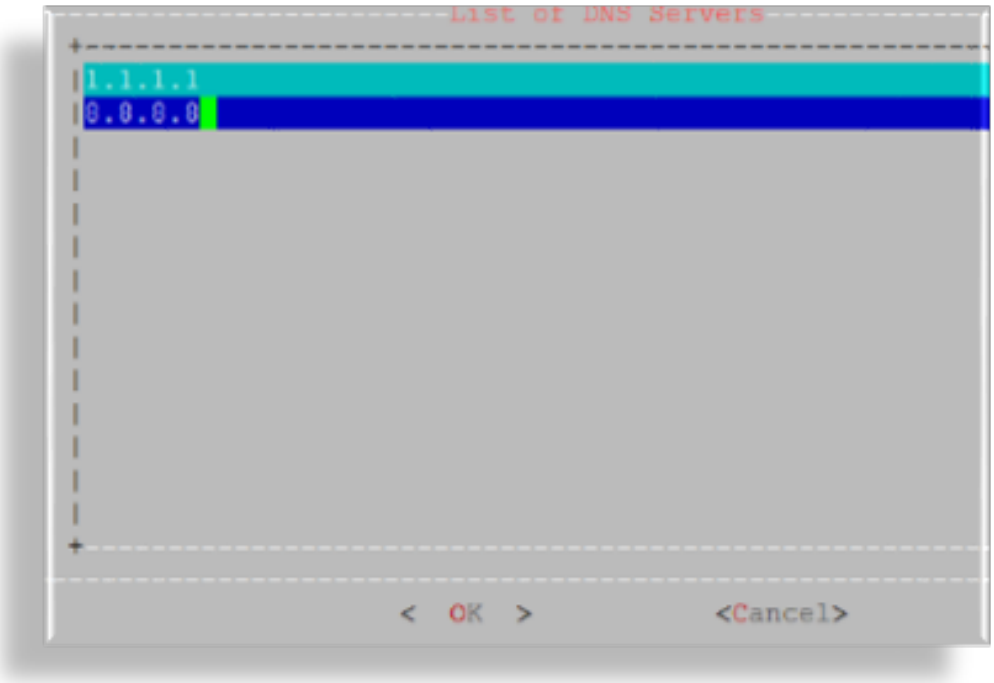
i. Select **DNS Settings**



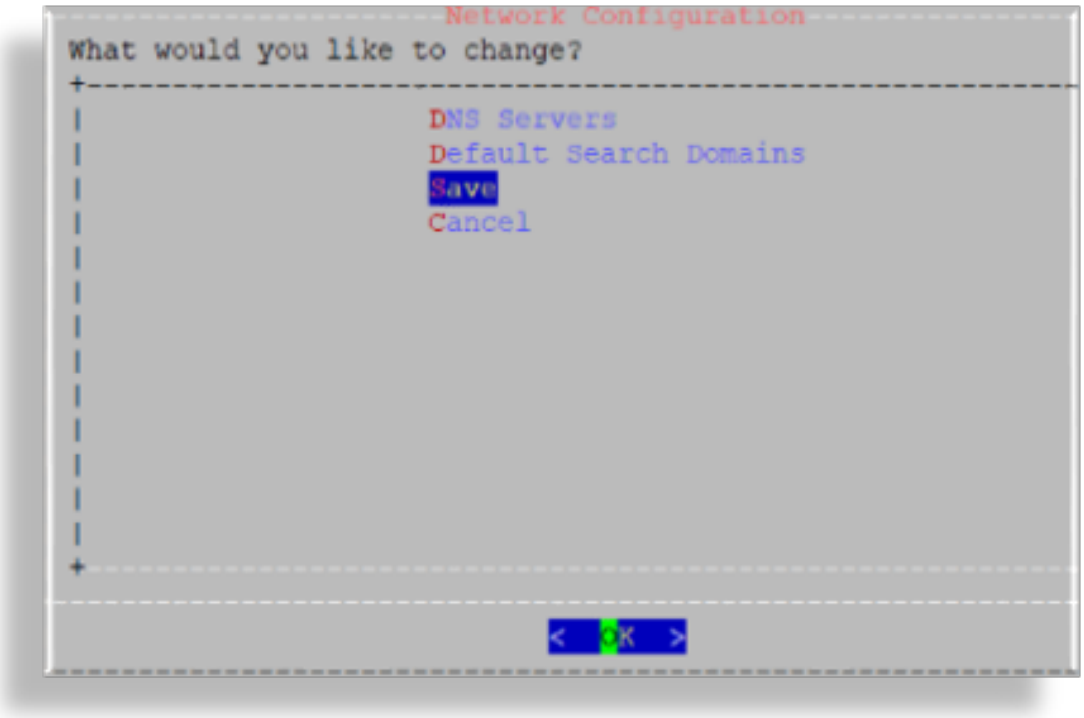
ii. Select **DNS Servers**.



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

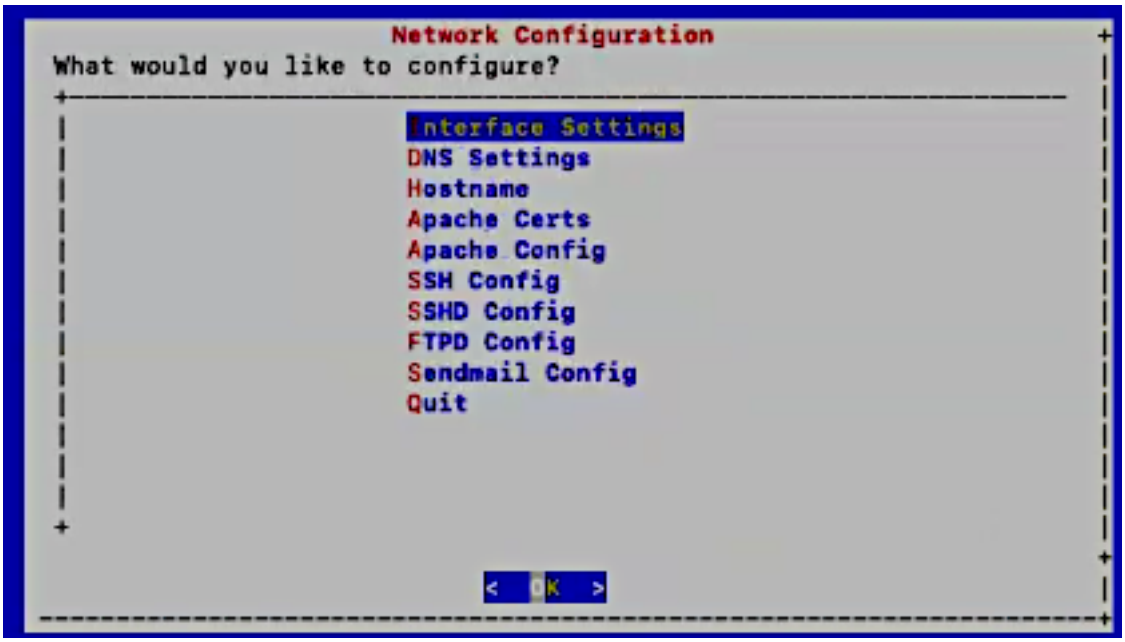


iv. Click **Save**.



4. Configure the hostname:
    i. Select **Hostname**.
    ii. Save to trigger the update.

    The console displays a message, *Updating hosts*. This setup may take a few minutes.

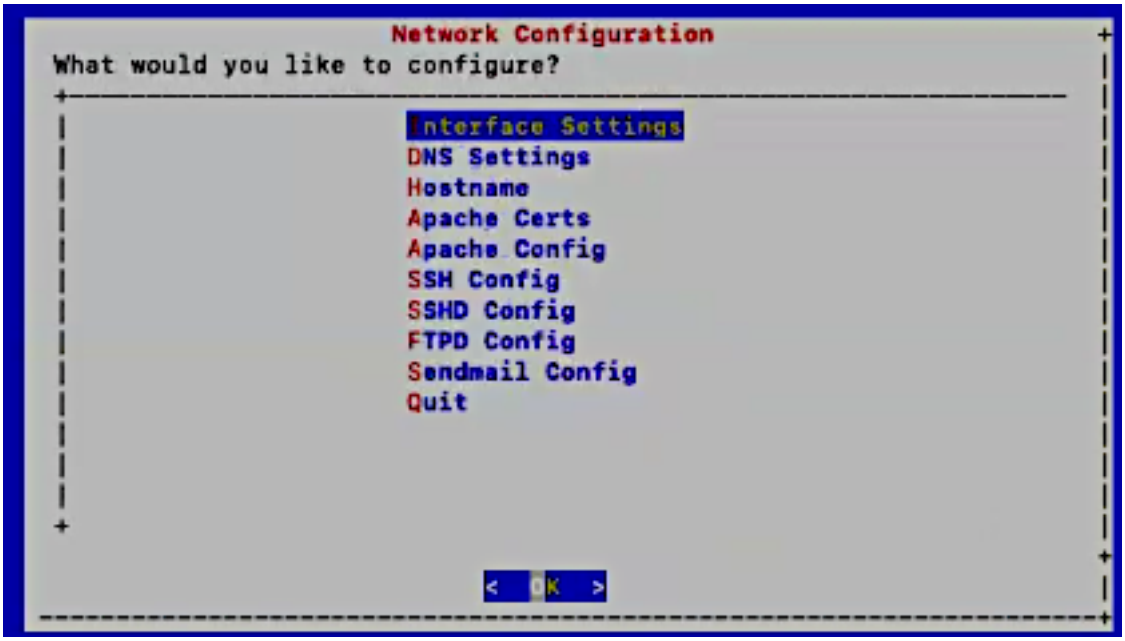


5. Update SSL ciphers.
    i. Select **Apache Config**.

```
SSLCipherSuite HIGH: !MEDIUM: !ADH: !LOW
```

Note:

- `SSLCipherSuite` defaults to `HIGH` encryption.
- For `SSLProtocol`, only TLSv1.2 is supported.
- OpenLDAP defaults to `HIGH` encryption.
- OpenSSH does not support weak ciphers.
- On system upgrade, if the contents of this configuration are no longer valid, then the contents will be will be reset to an empty state.



6. Configure SSH settings:

   i. Select **SSH Config**.

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

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

Note: On system upgrade, if the contents of this configuration are no longer valid, the contents will be reset to an empty state.

7. Configure SSHD:

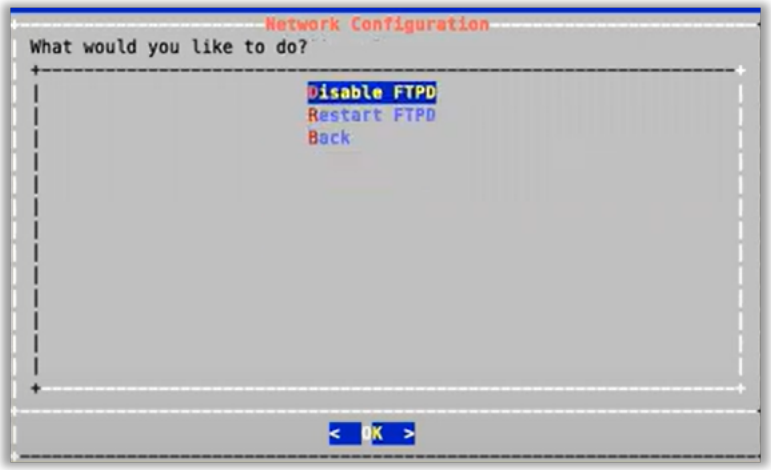
   i. Select **SSHD Config**.

Note:

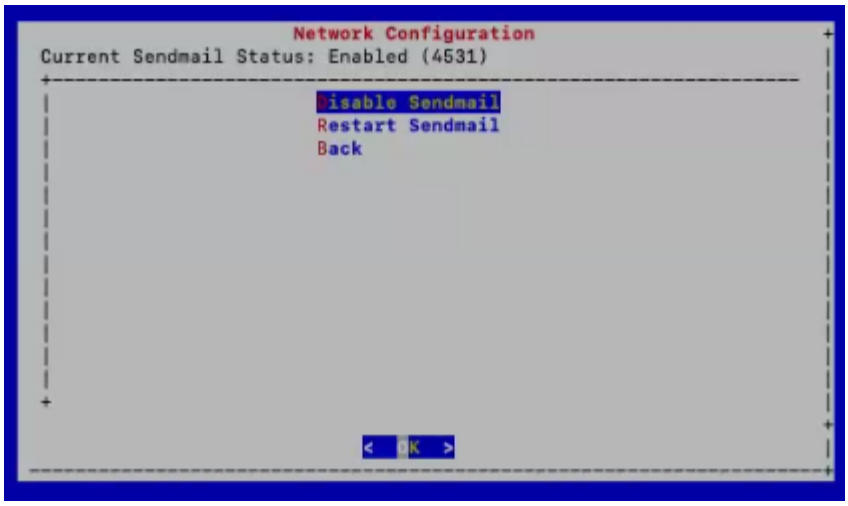
- Multi-line entries can be added, if required. For example, for CUCM v11.5 support, see: *Configure multi-line CUCM cipher support*.
- This step is relevant *only* to an Insights Assurance solution and its integration with Cisco UC systems. This step is *not* relevant to the DS9 and Insights NetFlow solution.
- On system upgrade, if the contents of this configuration are no longer valid, then the contents will be will be reset to an empty state.

8. Enable/disable FTPD or restart the FTPD daemon:
    1. 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. The drop account username is “drop”. You can set the password via the **Administration** menu.



9. Enable/disable Sendmail or restart Sendmail on port 25:



i. Select **Sendmail Config**. The current status of the service displays on the menu.

ii. Choose to enable, disable, or restart the service as required.

10. Base system installation is now complete. Select **Quit** to exit the **Administration** menu on the console.

Next steps

- *Step 7: Create GUI admin password for Arbitrator and Dashboard*

Step 7: Create GUI admin password for Arbitrator and Dashboard

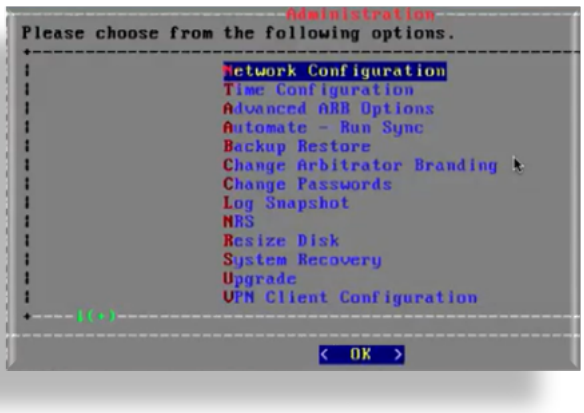
This procedure creates the GUI admin password, which is the password you will need to log in to Arbitrator or Dashboard via the browser.

The default credentials (admin:admin) will not allow browser access, so the GUI admin password must be set up for the Arbitrator and Dashboard systems. The procedure is the same for both Arbitrator and Dashboard.

Important: It is strongly recommended that you make a written or digital copy of any system passwords and share the copies with trusted team members or store them in a secure location from where they may be retrieved if needed.

The steps to create the GUI admin password for Arbitrator and Dashboard are the same.

1. On the **Administration** menu, select **Change Passwords**.



2. Select **Reset GUI admin user (local LDAP only)**.

3. Fill out a new GUI admin password.

   The GUI admin password cannot start with a number and must not contain the dollar ($) symbol.

4. Log in to the Arbitrator / Dashboard via the browser, using the GUI admin user password created in this procedure.

Next steps

- *Product registration and system configuration*

6.1.2. Product registration and system configuration

Once you've installed and configured initial settings via the Administration console, you can continue with product registration, and with the configuration of your system through the GUI:

- 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.

6.1.3. Configure 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
```

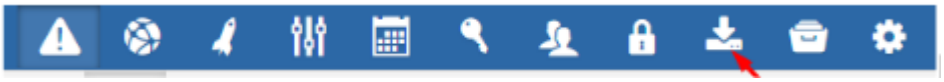
7. Database and System Setup

7.1. Install the Arbitrator System

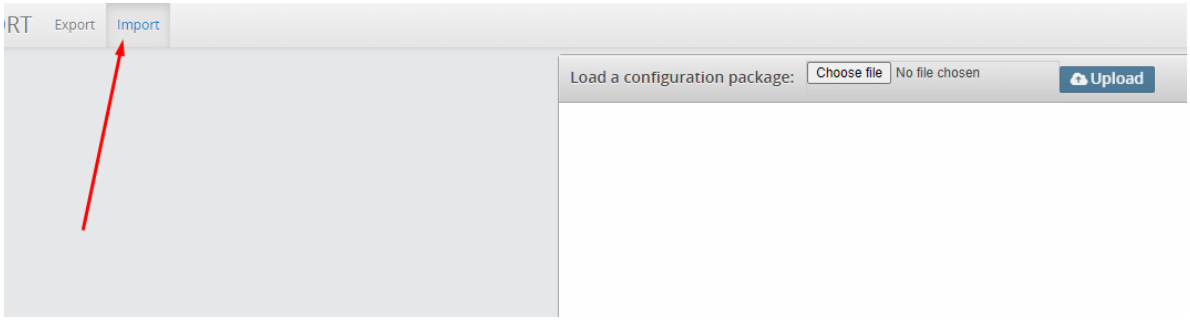
7.1.1. Arbitrator install steps

1. Log in to the Arbitrator as `admin`, with the password set up when installing the base system. See *Deploy and VM installation*.
2. Click the Wrench icon.

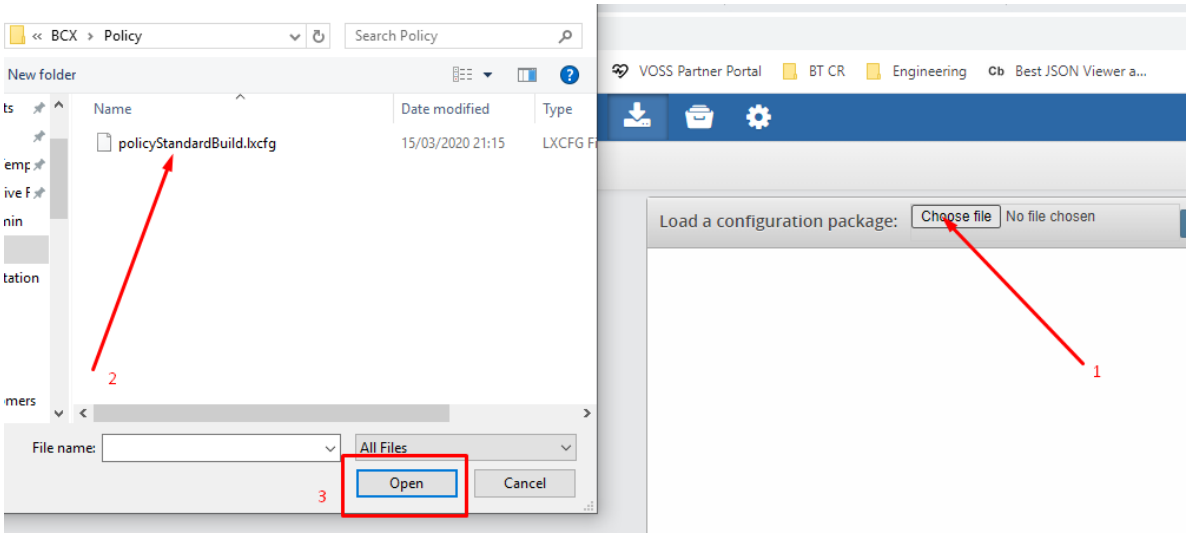
3. Click on the icon shown below



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: *Arbitrator install steps*

7.1.2. Policy configuration files

Policy configuration files are installed at the end of the installation process.

Polices 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 also contains several correlation rules that are designed to create alerts based on the best practices of that particular system manufacturer.

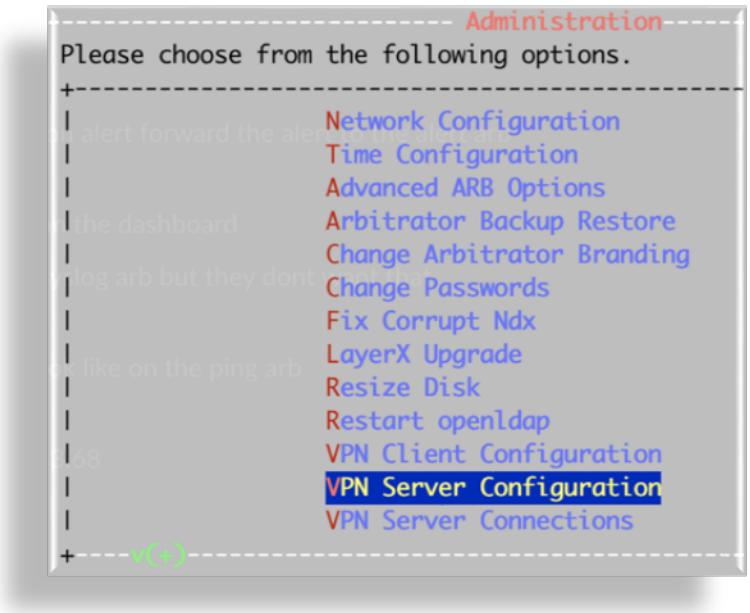
The table describes the configuration file components:

Component	Purpose	Filename
Controls	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. • Turn an alarm a different color • 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: • 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	`STDCONTROLS.lxcfg`
Probes	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 • AXL • API • CLI	`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`

7.2. Set up Arbitrator to Arbitrator communication

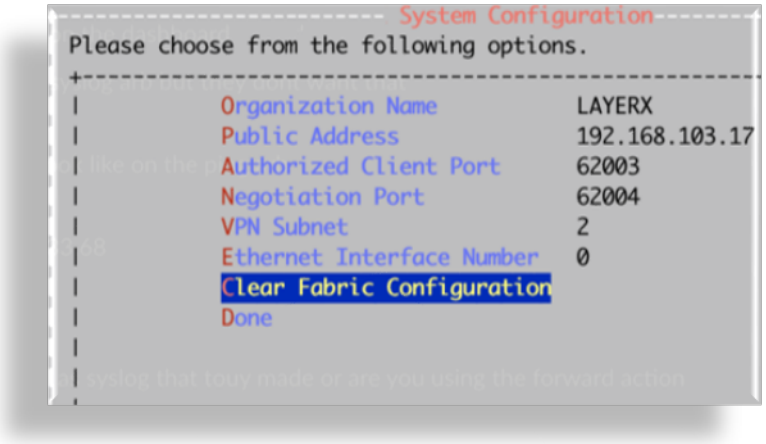
Log in as admin on the central/lead arbitrator and go to VPN Server Configuration



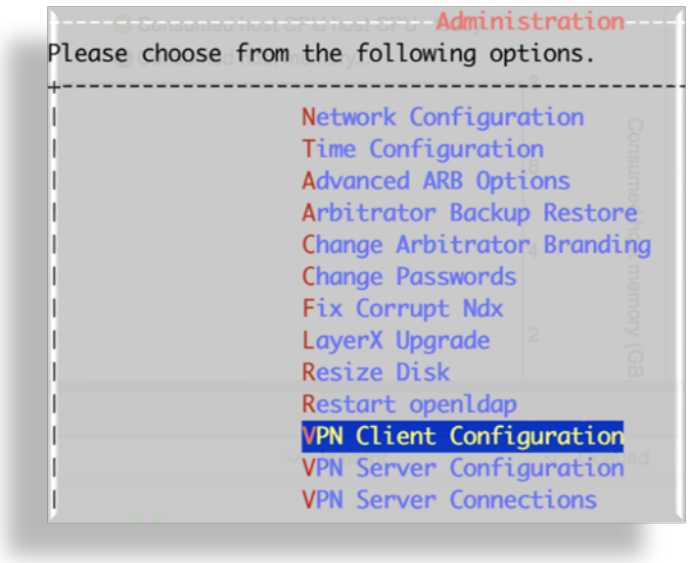
Then Clear Fabric Configuration, then reset this up:

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:



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:

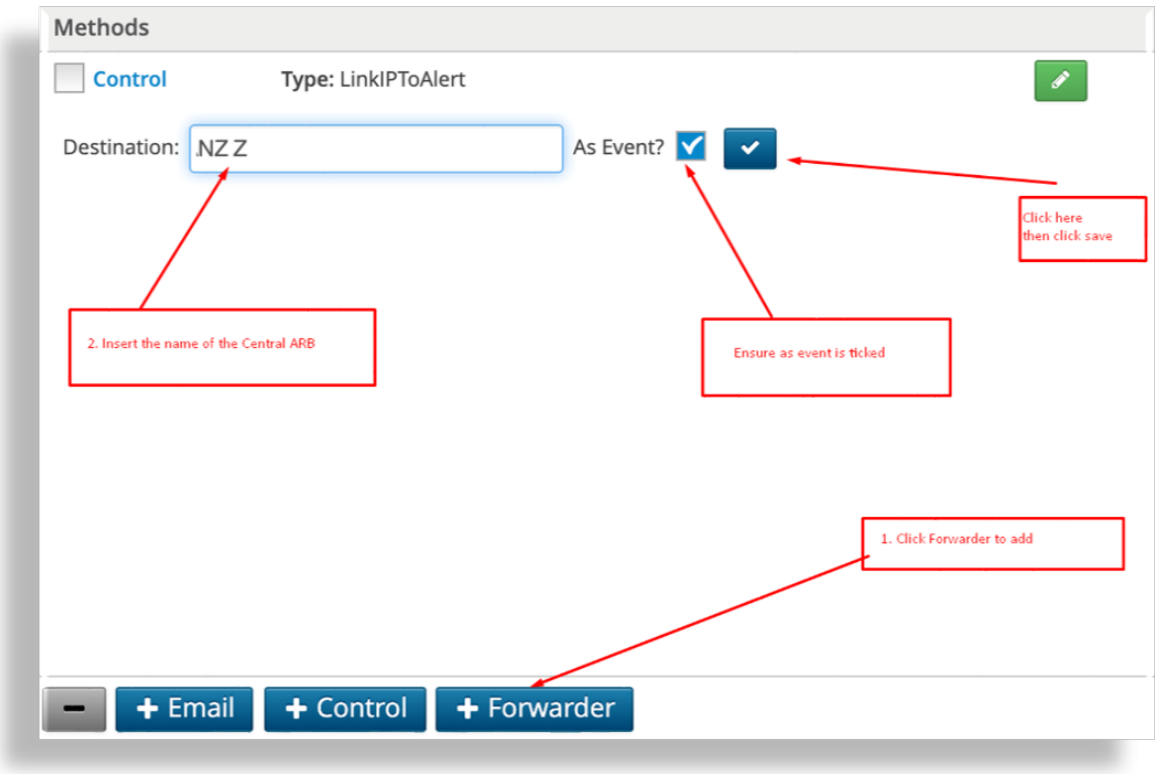
```
root@dharb1:~# netstat -ne | grep 3050
tcp        0      0 169.254.5.1:30501       169.254.5.6:18880       TIME_WAIT   0          0
tcp        0      0 169.254.5.1:30501       169.254.5.6:18920       ESTABLISHED 0          13090739
tcp        0      0 169.254.5.1:30501       169.254.5.6:18866       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@dharb1:~#
```

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

```
root@dharb1:~# 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@dharb1:~#
```

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

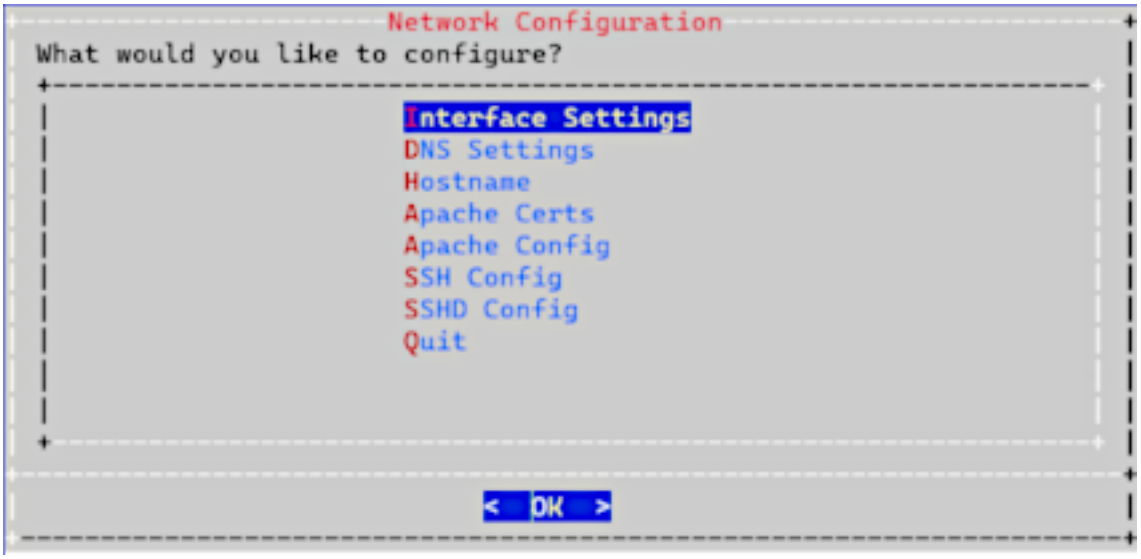
- On the Subordinate Arbitrator go to Response Procedures in the config area of the GUI:



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 headers and footers:

```
EXAMPLE:
-----BEGIN CERTIFICATE-----
MAIN SERVER CERTIFICATE
```

(continues on next page)

(continued from previous page)

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
INTERMEDIATE CERTIFICATE
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
ROOT CERTIFICATE
-----END CERTIFICATE-----
```

Error checking and solutions:

- `Error 20 at 0 depth lookup:  unable to get local issuer certificate`

  The server certificate needs an intermediate certificate to validate. Add the intermediate certificate after the server certificate.

- `Error 2 at 1 depth lookup:  unable to get issuer certificate`

  The server certificate needs the root certificate to validate. Add the root certificate after the intermediate and or server certificate.

- ```
  Error loading file /etc/apache2/server.crt.tmp
  error:05800088:x509 certificate routines unknown function):
  no certificate or crl found:crypto/x509
  ```

  No certificate; invalid format; or blank.

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**, then exit the menu.
10. Refresh the browser. The system should be using the new certificate.

8.1.2. Generate a CSR from an existing certificate

If you want to generate a CSR for the current certificate:

1. SSH to the system using admin account.
2. Select **Network Configuration**.
3. Select **Apache Certs**.
4. Select **Generate Cert**.
5. Press **Enter**. The CSR displays on the screen.
6. Copy and save it.
7. Select **Back**, then exit the menu.
8. Refresh the browser. The system should be using the updated unsigned certificate.

8.1.3. Create new 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.
    - For `the number of days the certificate should be valid. (default 365):`, the value should be a positive number from 1 to 3650.

Publicly Trusted Certificates: For certificates that need to be trusted by web browsers like Chrome, Firefox, or Safari, the maximum validity period is currently 398 days. This is a policy set by the CA/Browser Forum to enhance security by encouraging more frequent certificate renewals and updates.

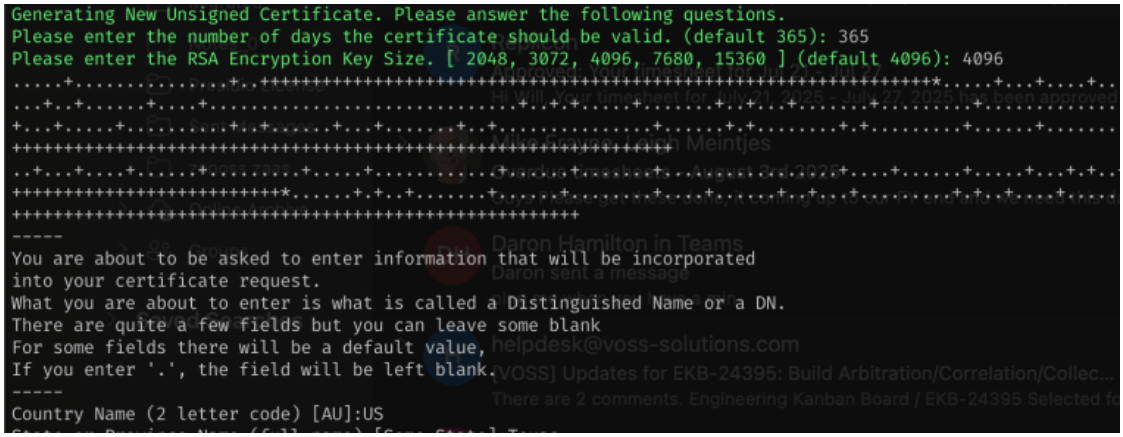
Self-Signed Certificates: When you are using OpenSSL to create a certificate for a private network or for testing purposes, you can set a much longer validity period. The tool itself does not prevent you from setting a very high number of days, but you may run into issues with the system's date and time representations (e.g., the Year 2038 problem on 32-bit systems).

- The default RSA Encryption Key Size is 4096.

  If the check: `Info: Checking modulus of the Certificate and Private Key.` returns with an error: `Error: Cerificate and Private Key DO NOT MATCH`, the possible reasons could be:

  - Either wrong certificate uploaded.
  - Private key not uploaded.

    Then generate new unsigned certificate, which will generate a new key and certificate.




```
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]: Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

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

9. CUCM Asset Onboarding

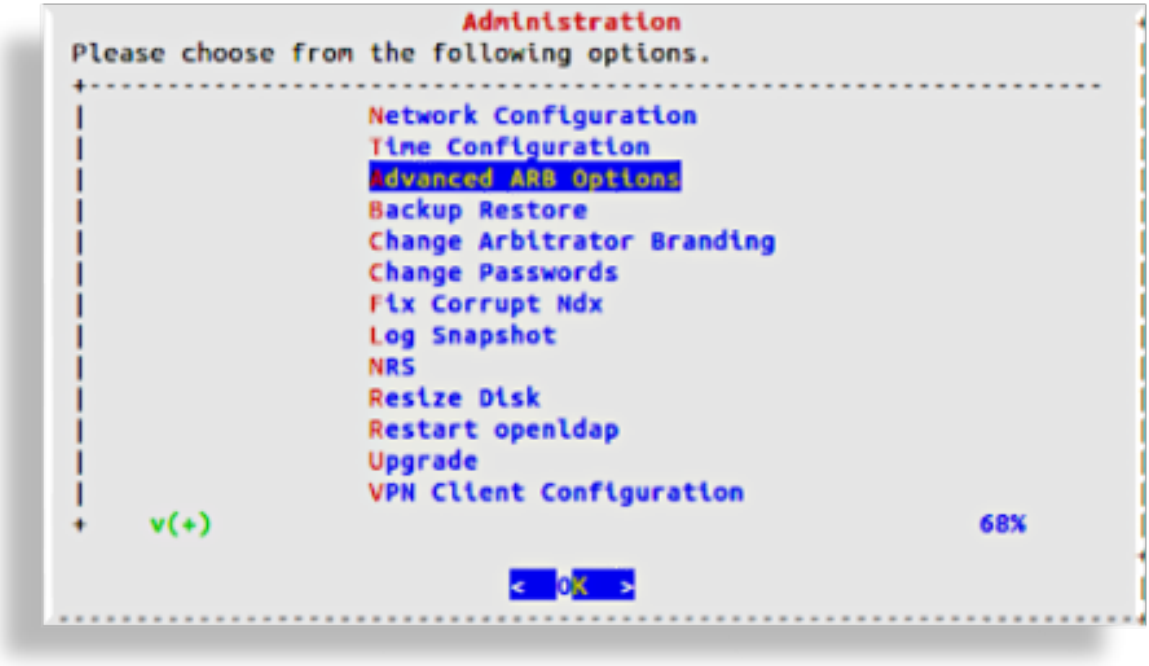
9.1. Customer Onboard

9.1.1. Add Customer CDR Folders

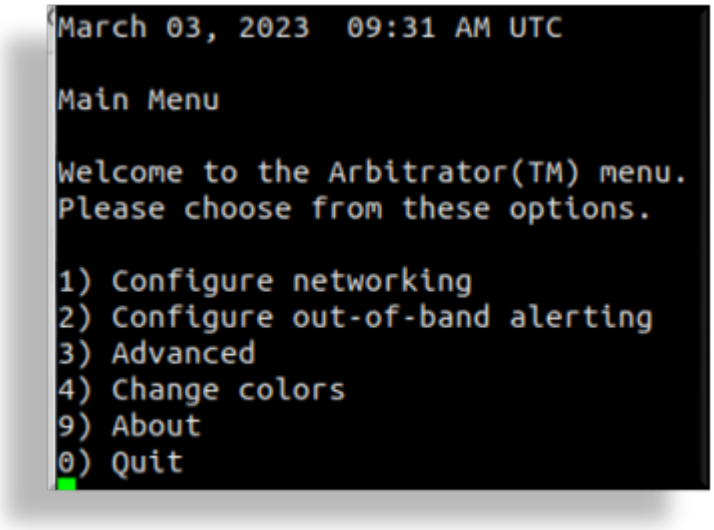
1. Log in via the CLI to the Arbitrator selected to receive CDR data from call managers:
   - Cisco UCM
   - Oracle Call Manager / Session Border Controller (SBC)

   Note: The call manager IP address name serves as a CDR folder name for incoming CDRs. The steps in this procedure show the menus for the selected call manager to be configured.

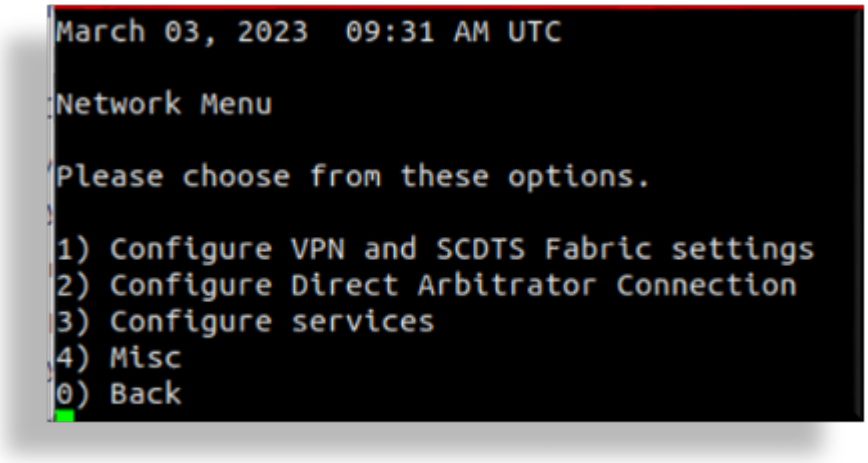
2. Use the admin credentials to log in, then select **Advanced Arb Options**.



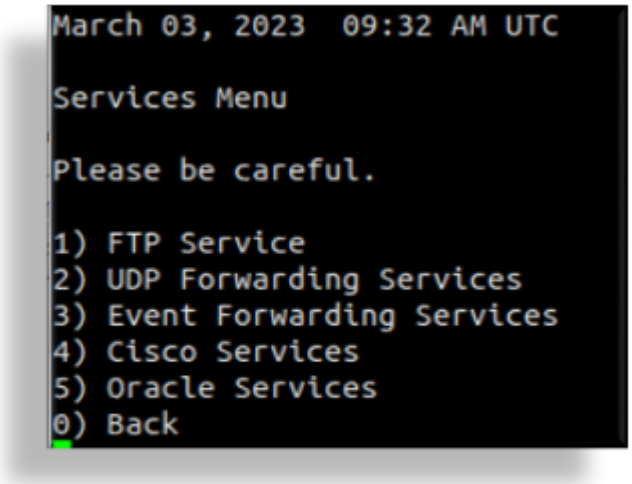
3. Select **Configure networking**



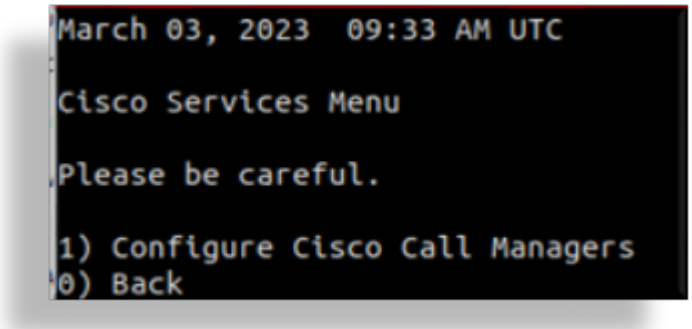
4. On the **Network Menu**, select **Configure services**.

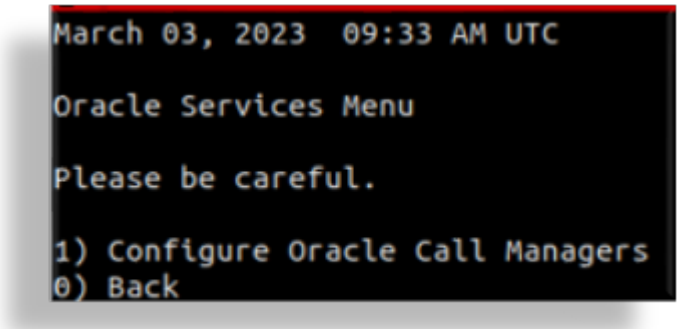


5. Choose the service to configure (Cisco Services or Oracle Services):

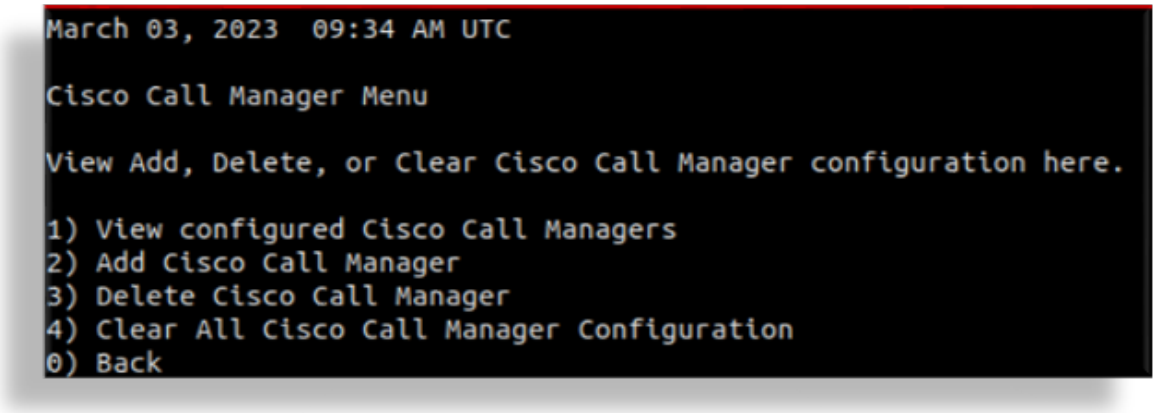


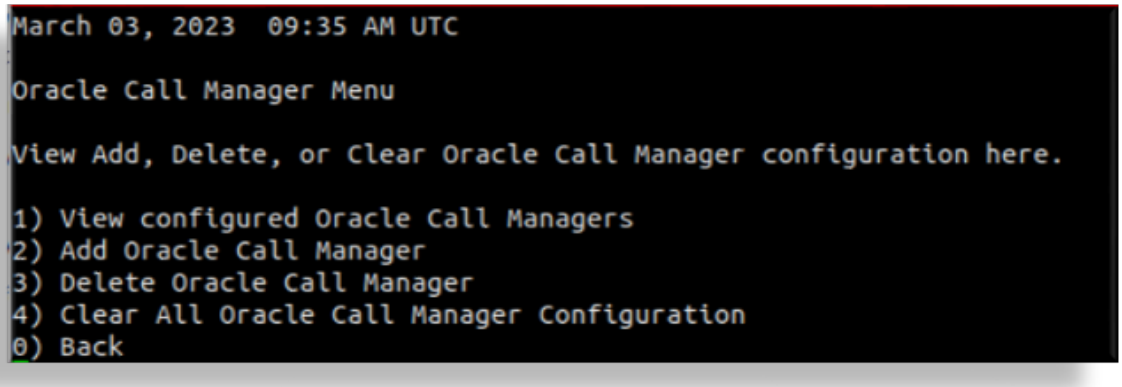
6. Select the required call manager.



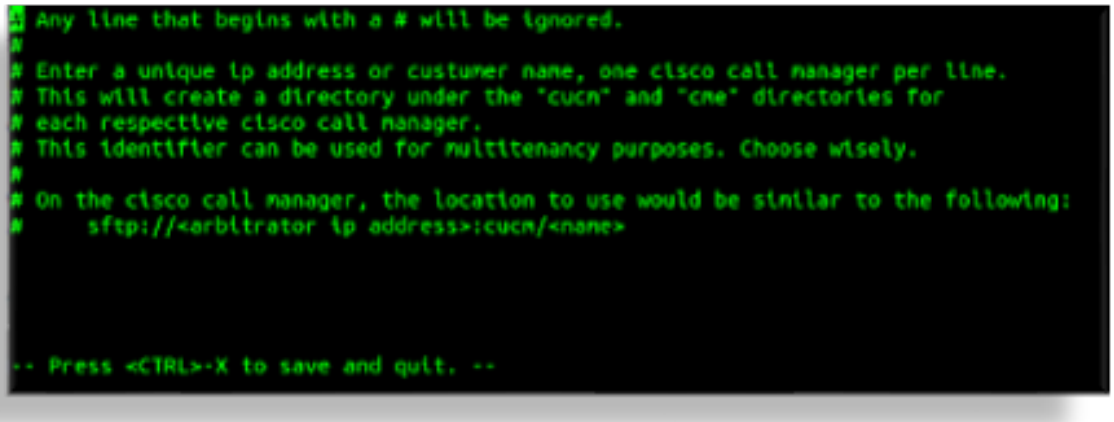


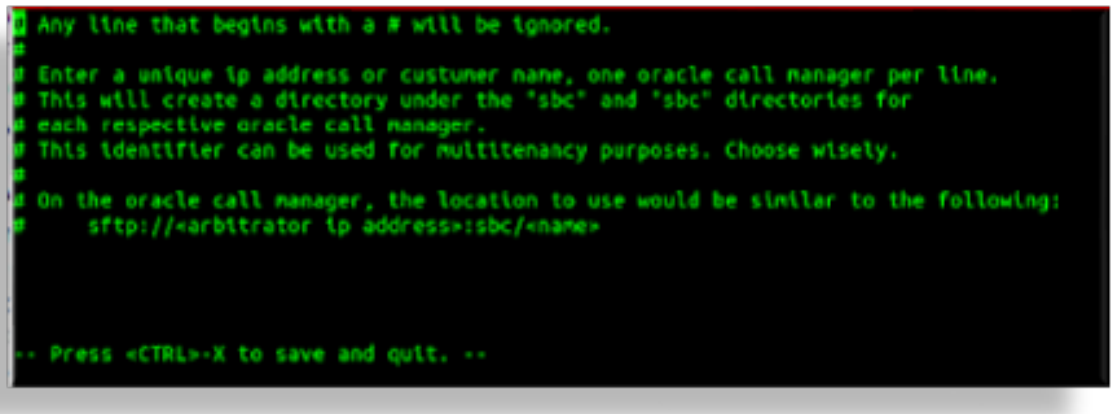
7. Select **Add (Cisco/Oracle) Call Manager**.





8. In the editor, add the IP address of the call manager, then press **Ctrl + X** to save and quit.



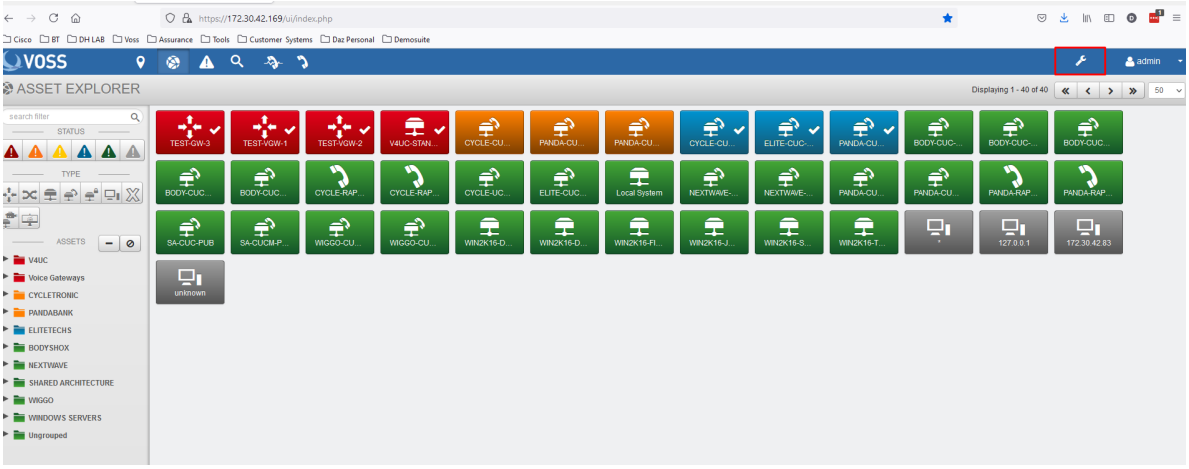


Related Topics

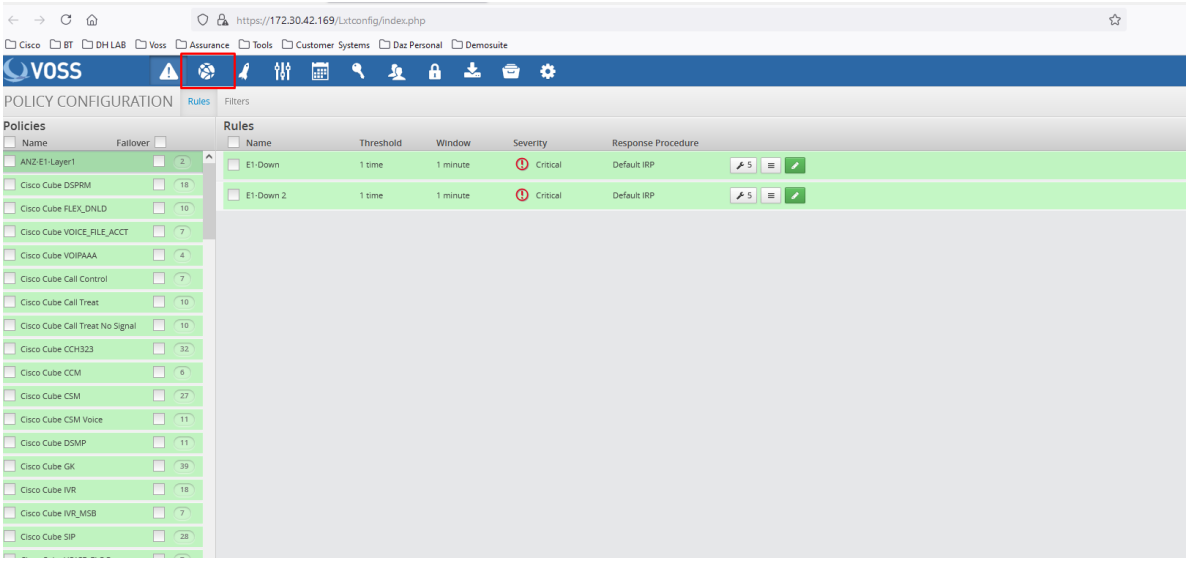
- For Collect setup in Arbitrator, see the "Configuration - Collect" topic in the Arbitrator Administration Guide.

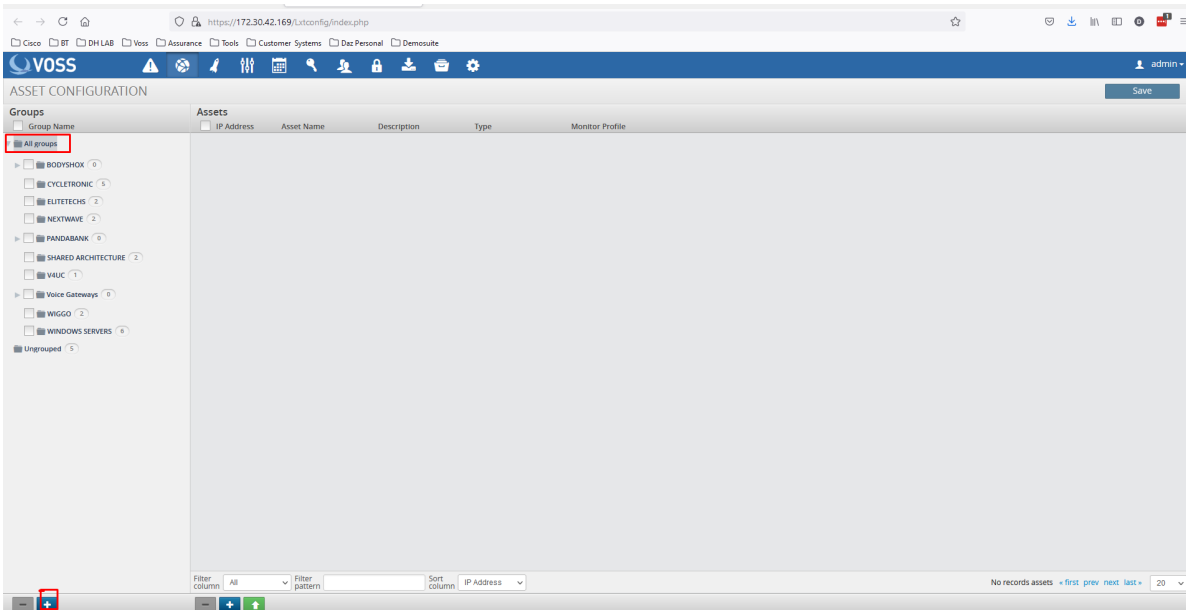
9.1.2. Add Customer Assets

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

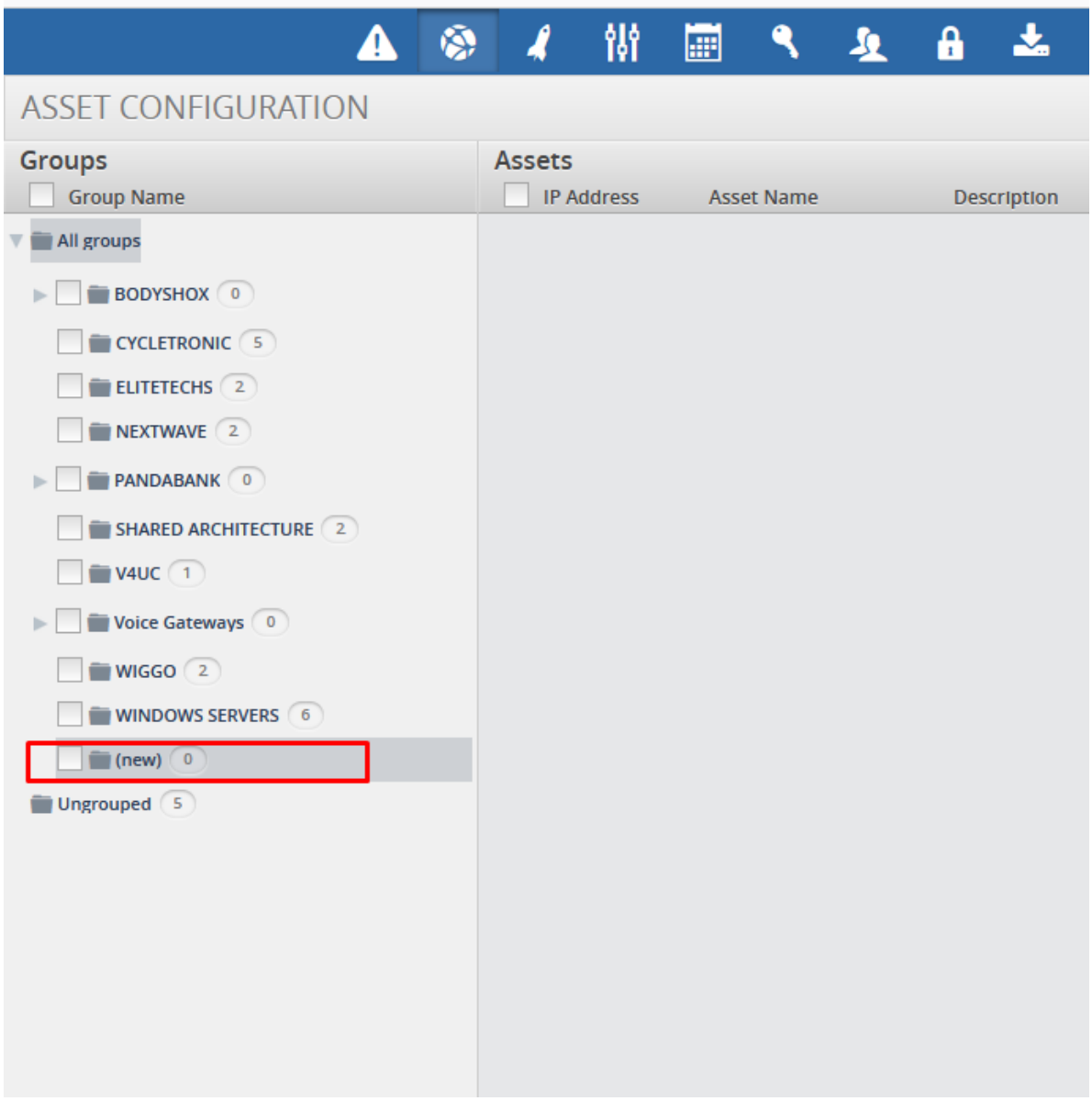


3. Click the Globe icon on the toolbar to open the **Asset Configuration** screen.

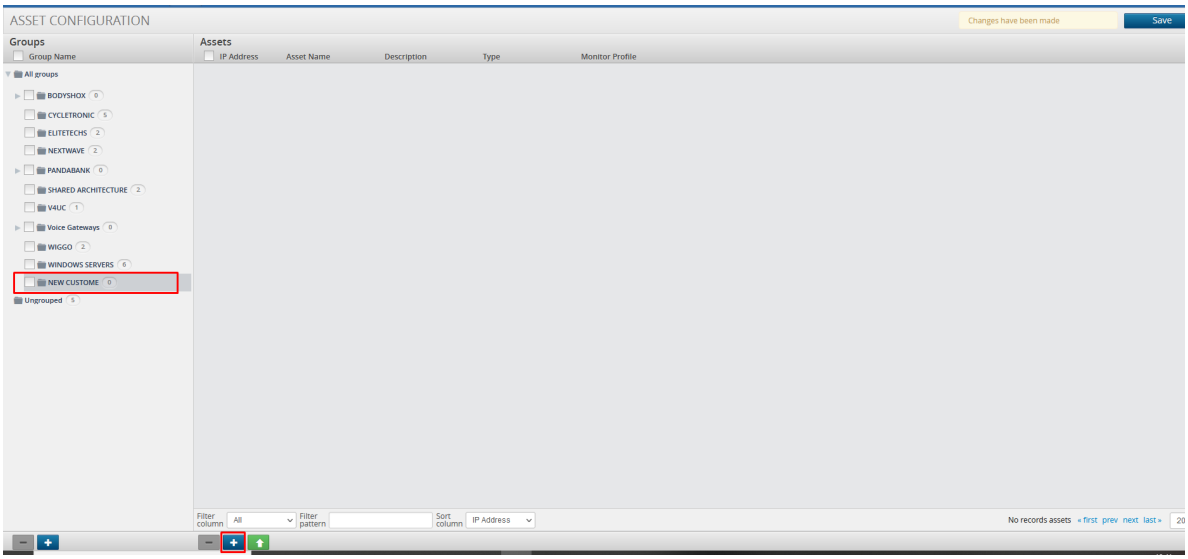




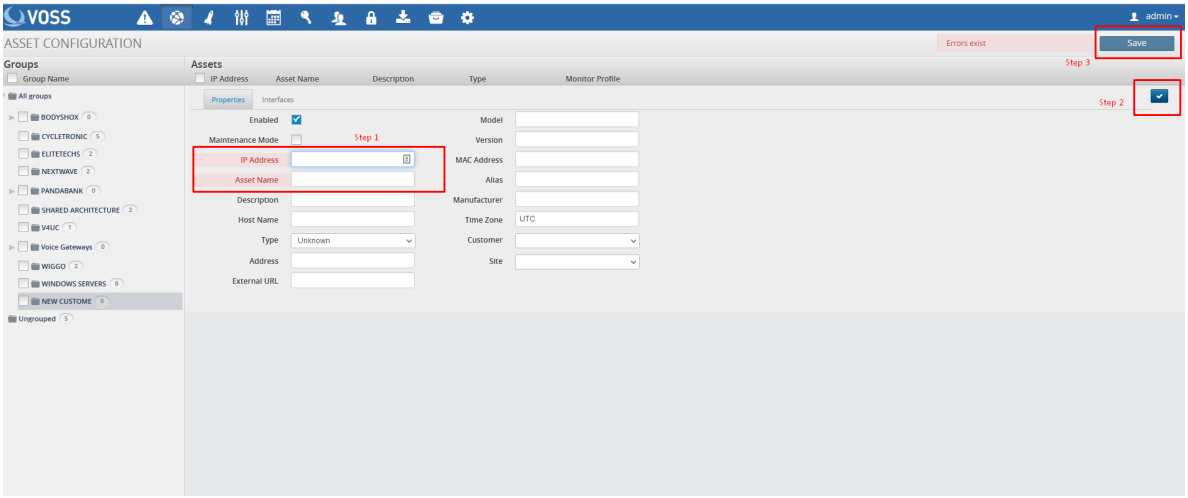
4. Select **All groups**, then select the Plus (+) icon to add a new folder.



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.



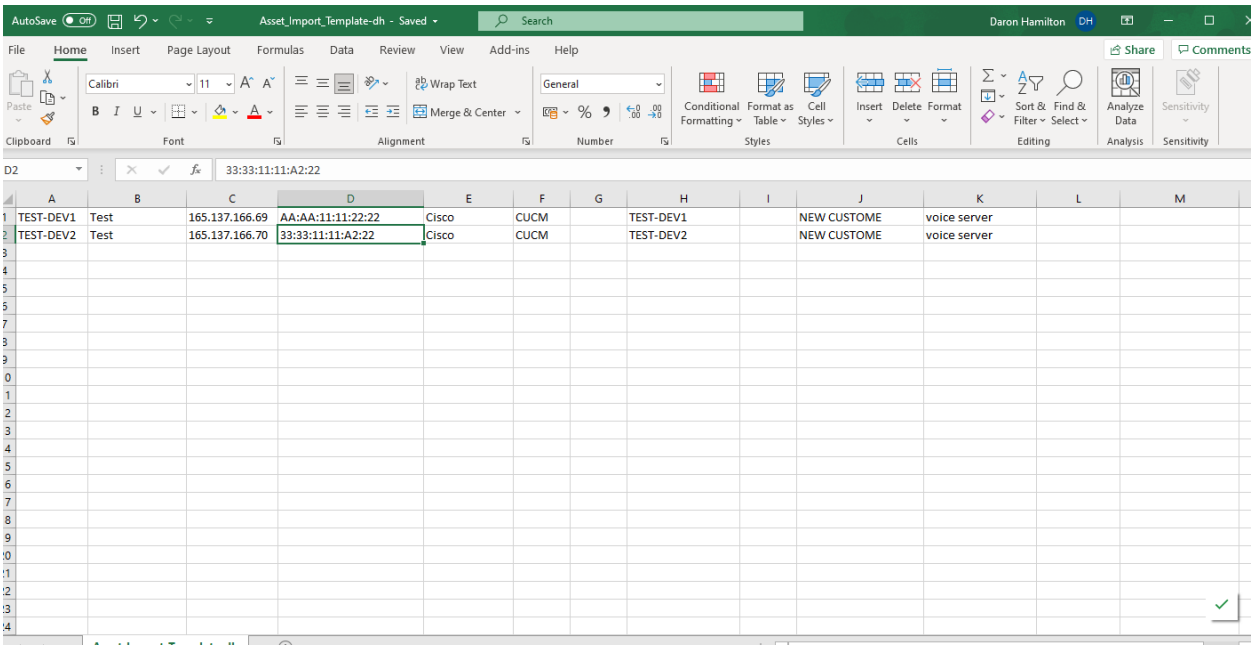
- Fill out the IP address (mandatory).
- Fill out the asset name (mandatory).
- Fill out any other information you have into the relevant fields.
- Click the Checkmark .
- Click **Save**.

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

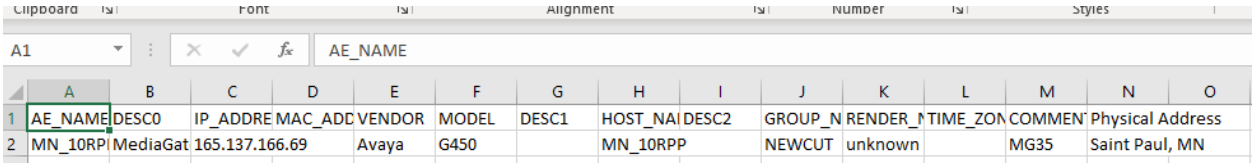
CSV Import of Assets

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

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



The CSV file is available in the Google Drive.



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
```

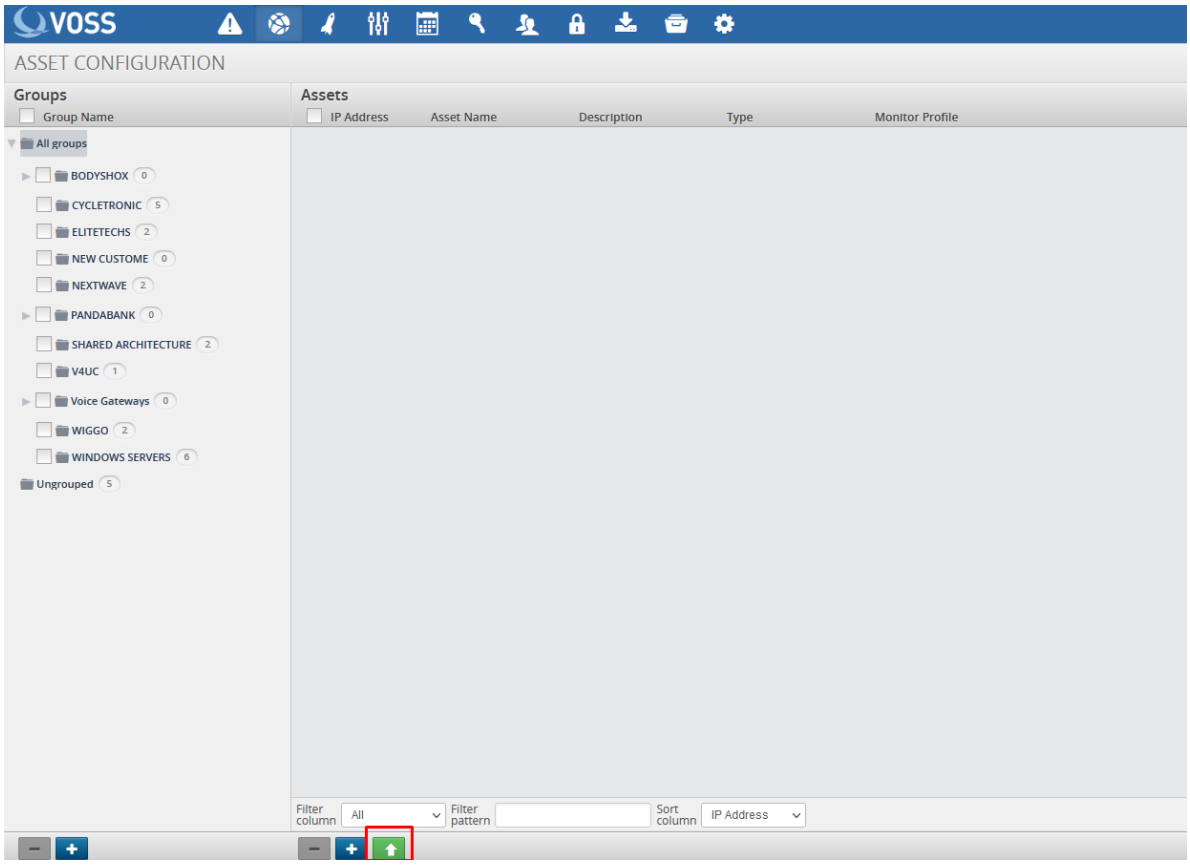
(continues on next page)

(continued from previous page)

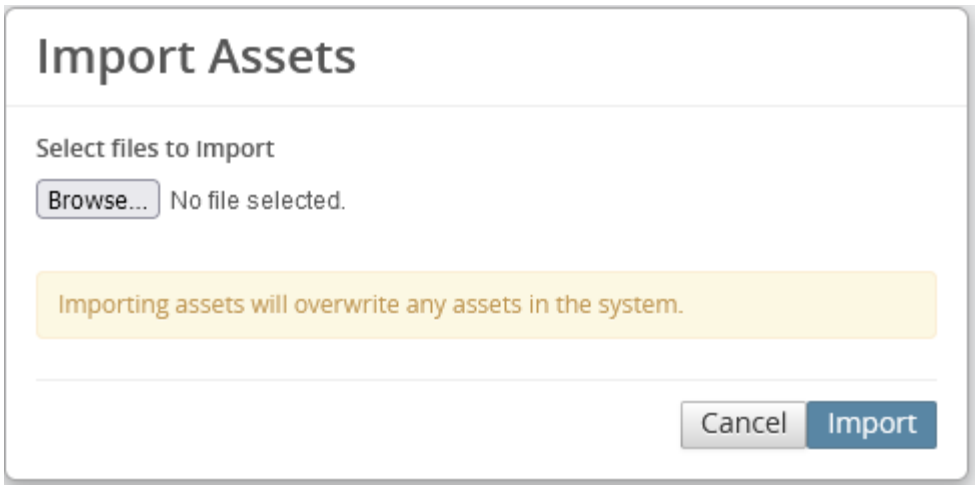
```
switch voice
server
voice server
server voice
workstation
phone
```

How to Import using CSV

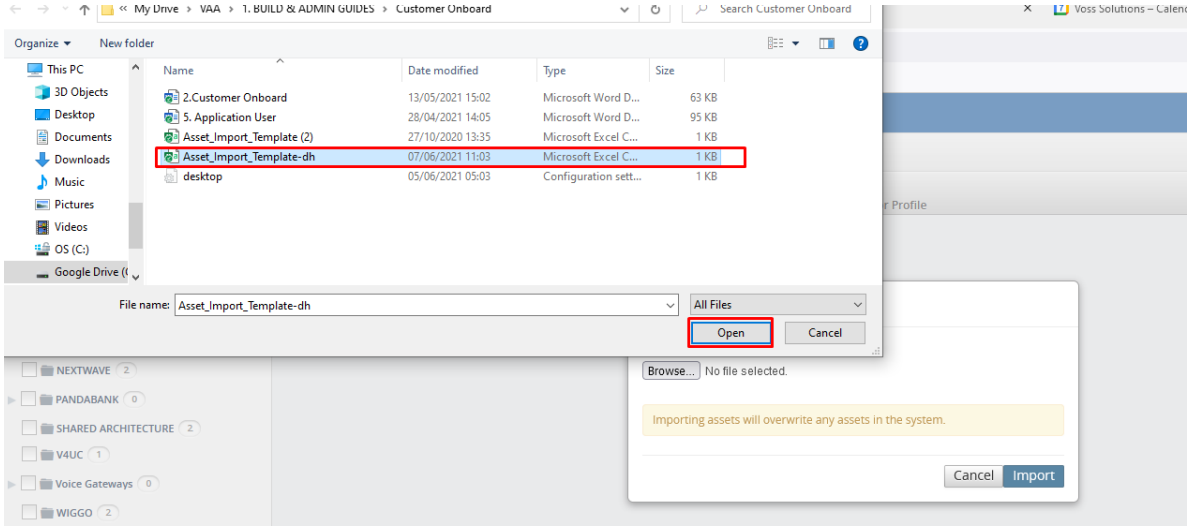
1. Log in to the Arbitrator with admin privileges.
2. Click the Wrench icon  to open the configuration screen.
3. Click the Globe icon  to open the Asset Configuration screen.



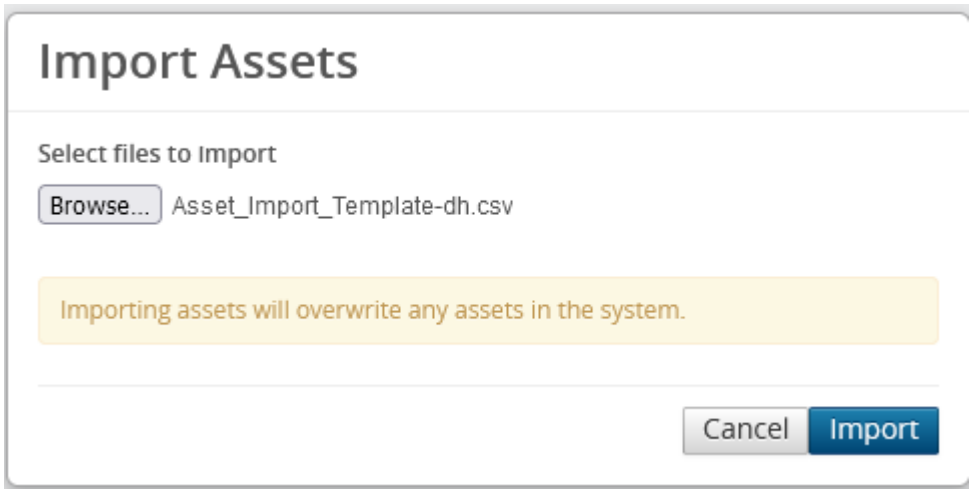
4. Click the Up-arrow  to open the **Import Assets** dialog.



5. Browse to your csv file.



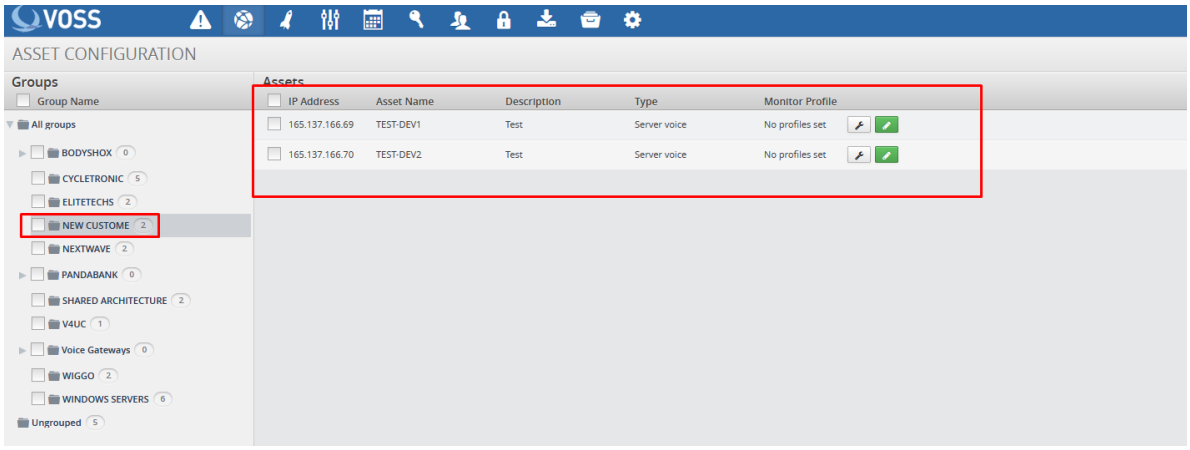
6. Click **Open**.



7. Click **Import**

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

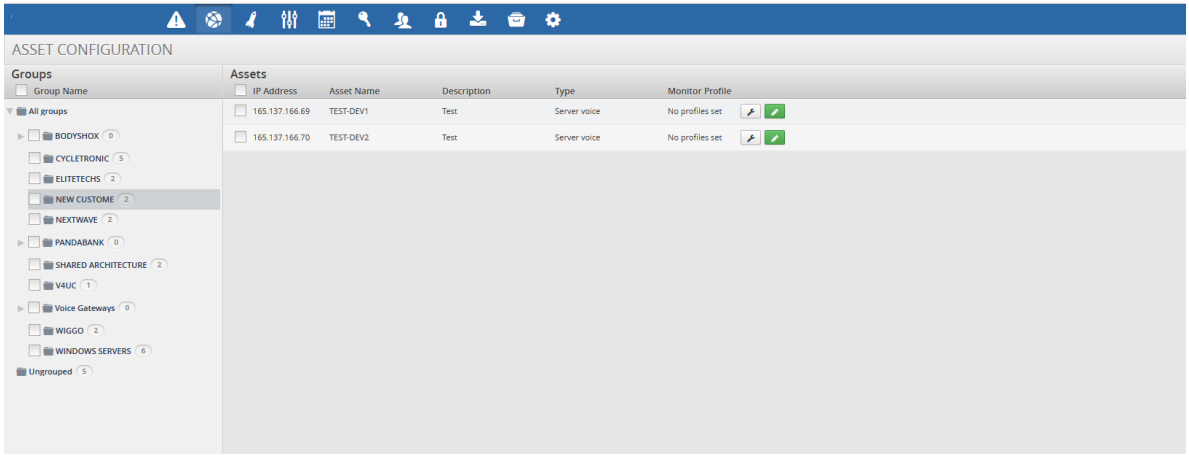
and in the correct location.



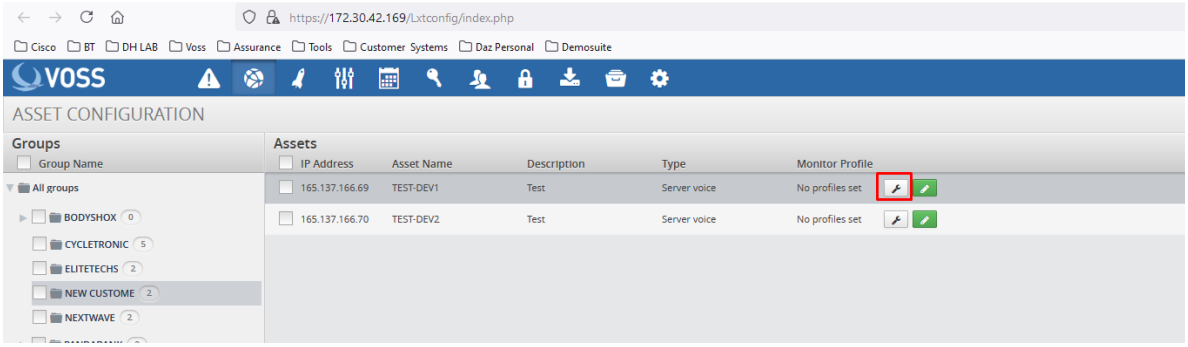
9.1.3. Assigning Probes to Assets

Assign Standard Probes

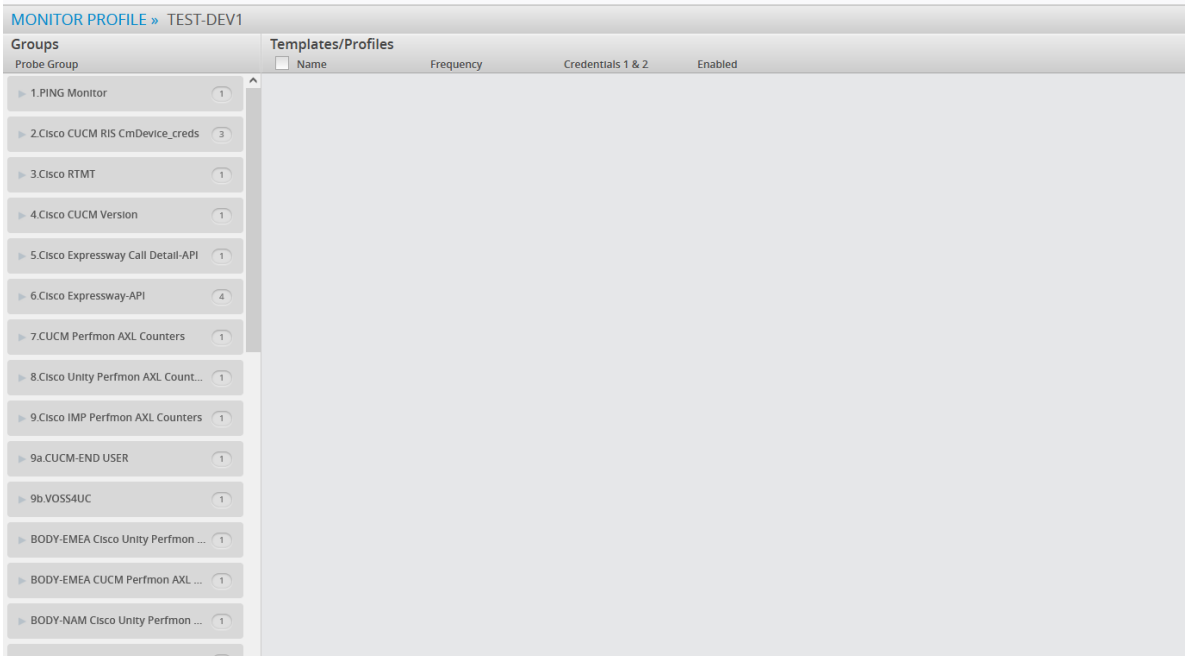
1. Log in to the Arbitrator with admin privileges.
2. Click on the  to open the configuration screen.
3. Click on the  to open the Asset Configuration screen.
4. Select the Asset Group that contains the assets you wish to configure



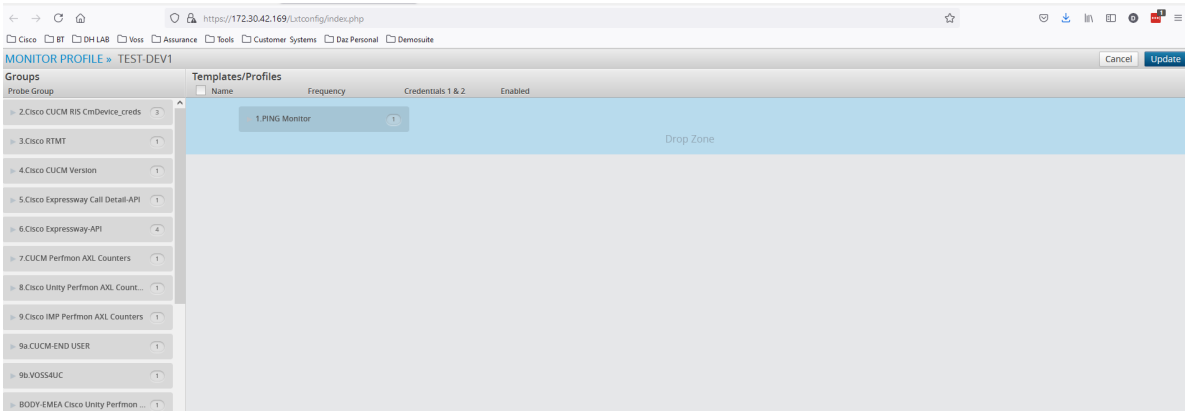
5. Click on the wrench icon as shown below.



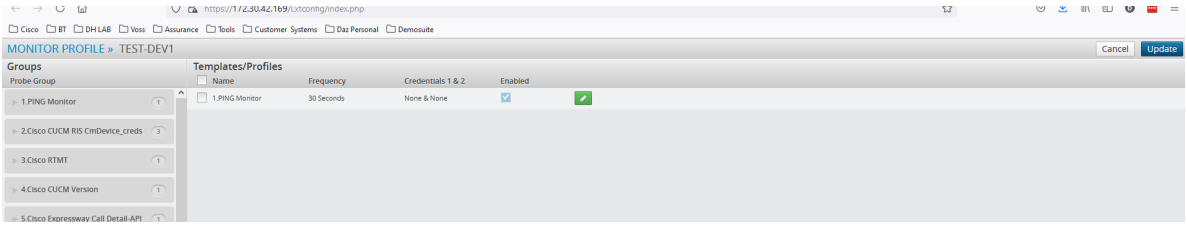
This will then open the Assignment screen.



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.



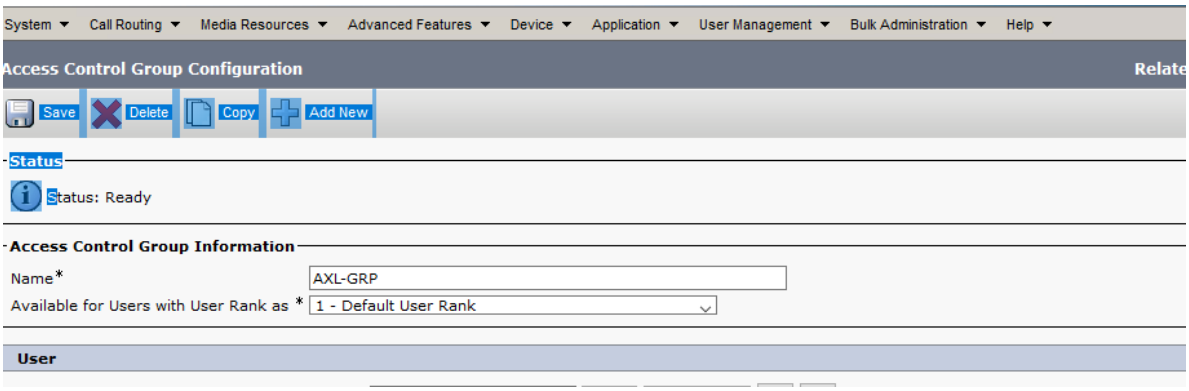
8. If you then click on  you can set any time schedules / credentials required for this probe
9. Once finished click **Update** and then click **Save**.

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

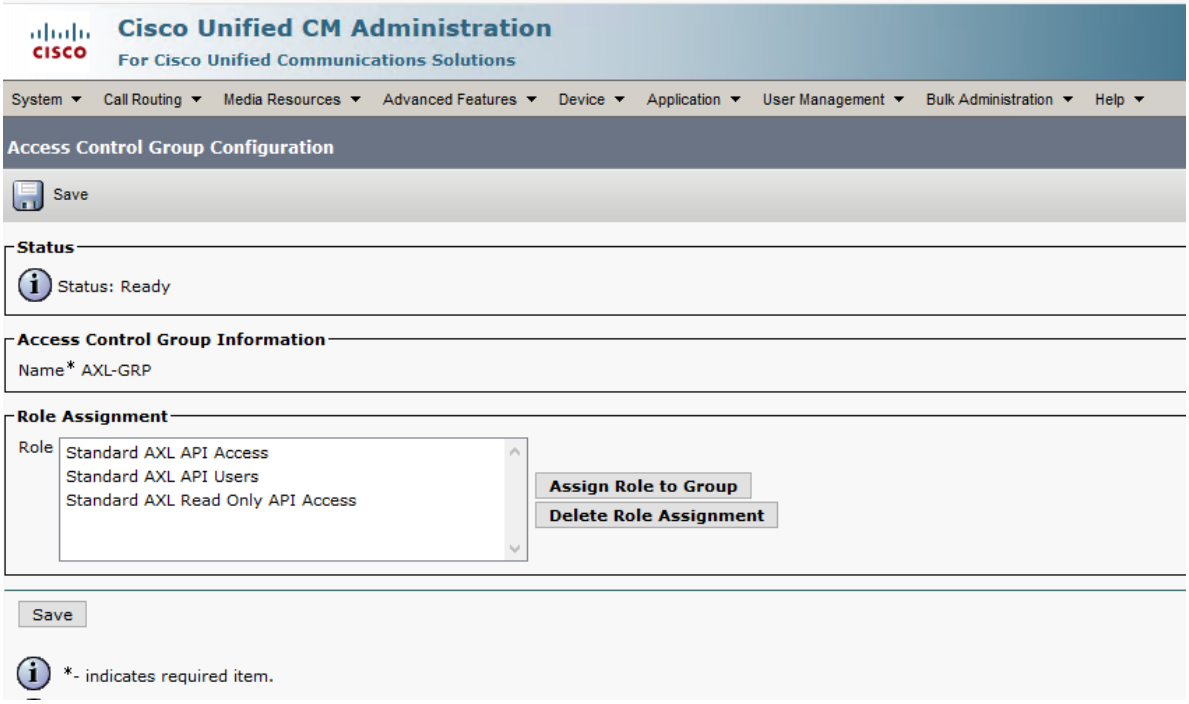
9.2. Call Manager Configuration

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.



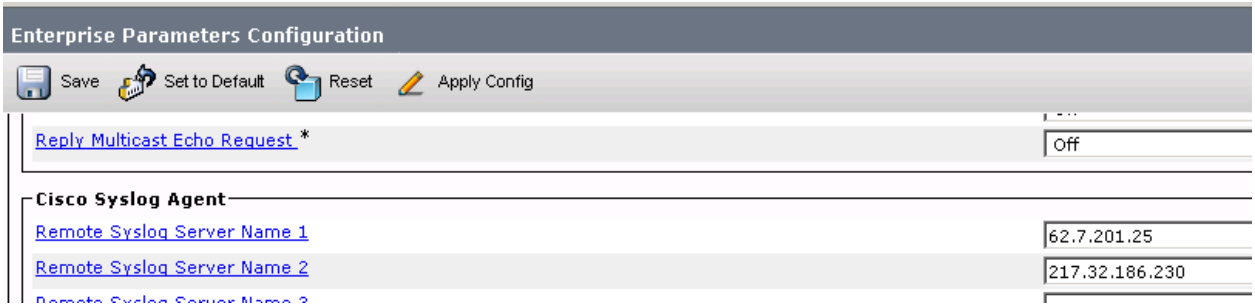
4. Add roles to this new group.



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

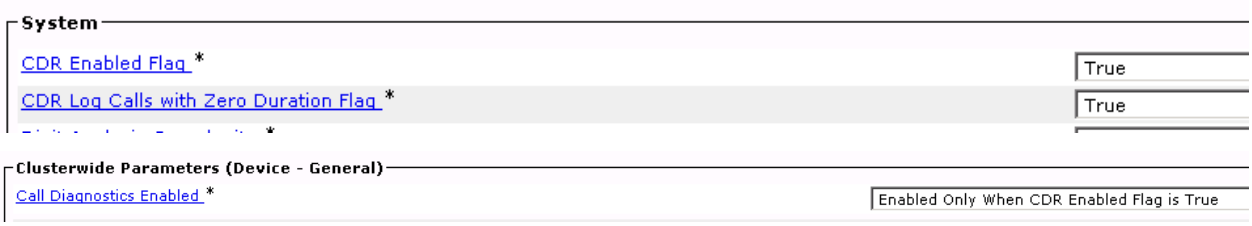
In Enterprise Parameters navigate the section Cisco Syslog Agent and configure the IP address of the Arbitrator in one of the Remote Syslog Server Name fields.



CUCM Service Parameters

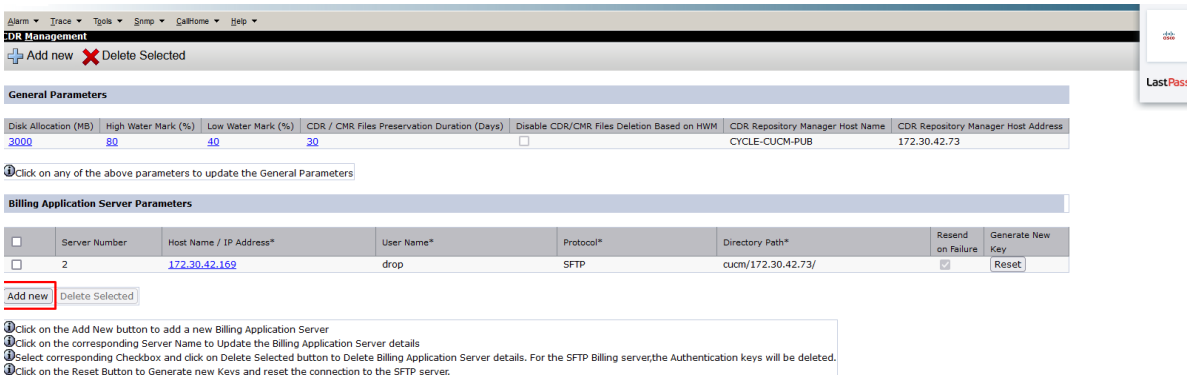
Ensure CDR Service Parameters are set:

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



CUCM Serviceability

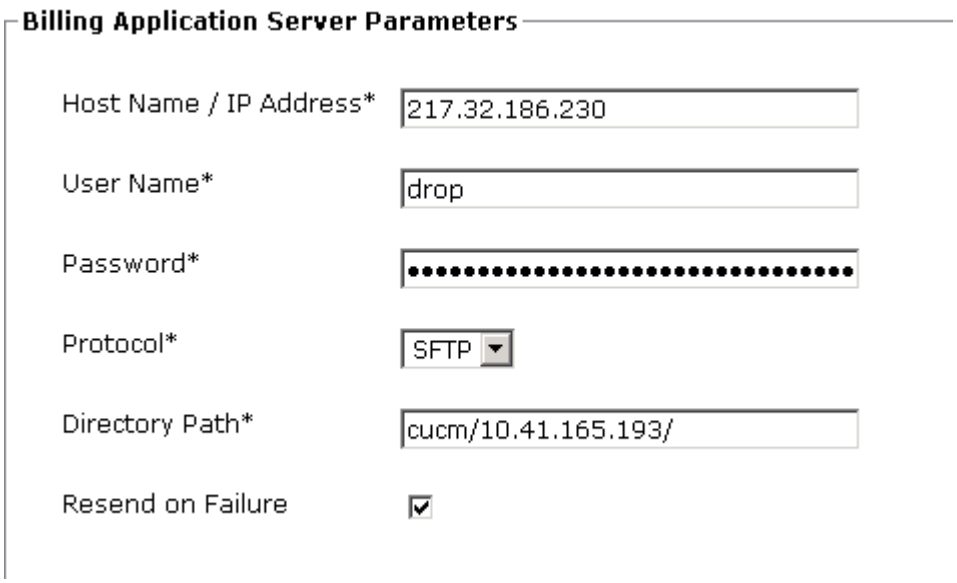
1. Navigate to Cisco Call Manager Serviceability.
2. Select **Tools > CDR Management**



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.

   Note: The drop account username is “drop”. You can set the password via the **Administration** menu.

   - **Protocol**: SFTP
   - **Directory Path***: cucm/ip address of call manager



10. Appendix

10.1. Digital Experience Monitoring (DEM) Agent Installation

10.1.1. Deployment Architecture

VOSS Insights provides for the installation and configuration of Digital Experience Monitoring (DEM) Agents.

The VOSS Insights Forwarder is an agent that collects statistics such as latency and response times on various cloud endpoints, along with system CPU statistics, which is sent by means of the API back to the Arbitrator.

The purpose of the agents are to monitor network experience, in particular for Microsoft Graph API, Teams, Web login and Exchange.

Measuring and widgets are available to:

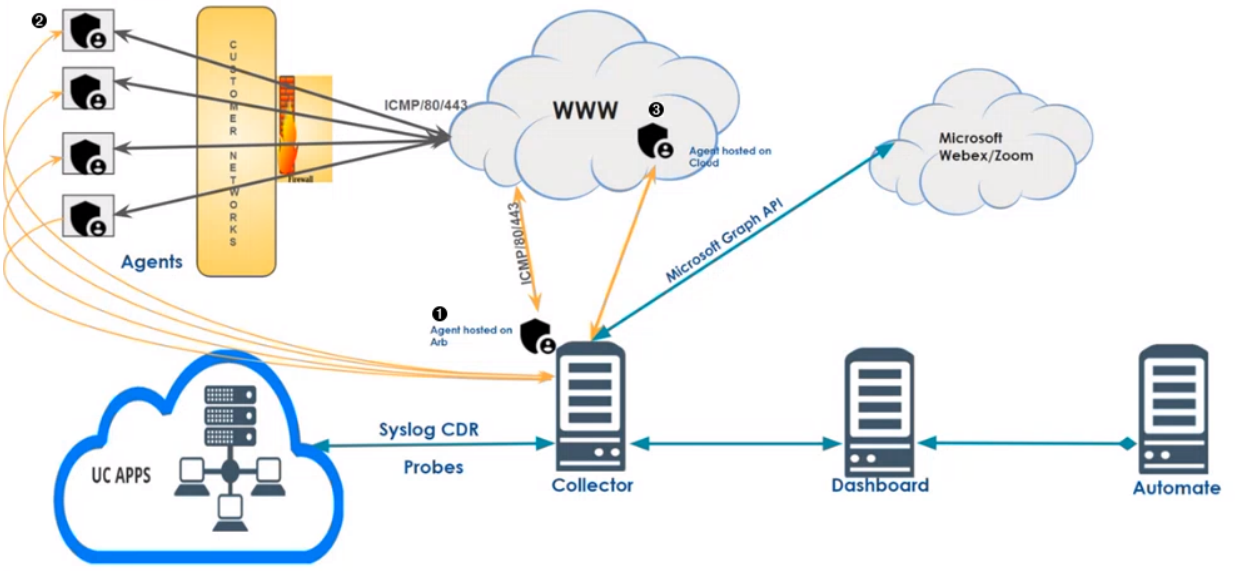
- Measure hops
- Measure latency
- Measure web performance
- Provide alarms on for example: too many hops, latency, bad response

A number of installation deployment options are available:

❶ One agent built into a single Collector

❷ Multiple agents within a customer network

❸ Agent hosted in the cloud



10.1.2. Hardware/OS requirements

The agent requires the deployment of a platform for it to run on - the agent itself is installed on that platform.

No specific hardware specification in terms of RAM, CPU, and so on is available: since this is a very lightweight agent, it can run on many hardware platforms.

However, some basic considerations are:

- Location - you want the device to be as close to the end user environment as possible - e.g “on the floor” with the users, not part of the data center (DC) infrastructure. For instance, part of the office wifi if that is the primary means of connectivity, or cabled into the local LAN if that is the primary.
- Connectivity - think of the different user connectivity options you want to test the experience over - LAN, wifi, guest wifi, etc.
- Small form factors typically work best, for example Intel NUC, Raspberry Pi, an old laptop, and so on.
- OS requirements are: Debian Linux OS. The agent installs via a Debian package install process.

The DEM agent does not currently support multiple network interfaces as part of the test suite - so if multiple interfaces are present, it will use the OS default routing. It is therefore currently best to just have a single network interface per device to ensure you know the interface being used.

10.1.3. Connectivity

This section outlines the connectivity required to and from the agent.

VOSS Insights platform connectivity

The agent needs to communicate with the Arbitrator - whether that is in the same environment or in the VOSS Cloud.

Destination	Protocol/Port/Type	Purpose
Arbitrator	HTTPS 443 TCP ICMP	Registration and sending test results

Testing Connectivity

DNS - for resolving hostnames as part of the testing.

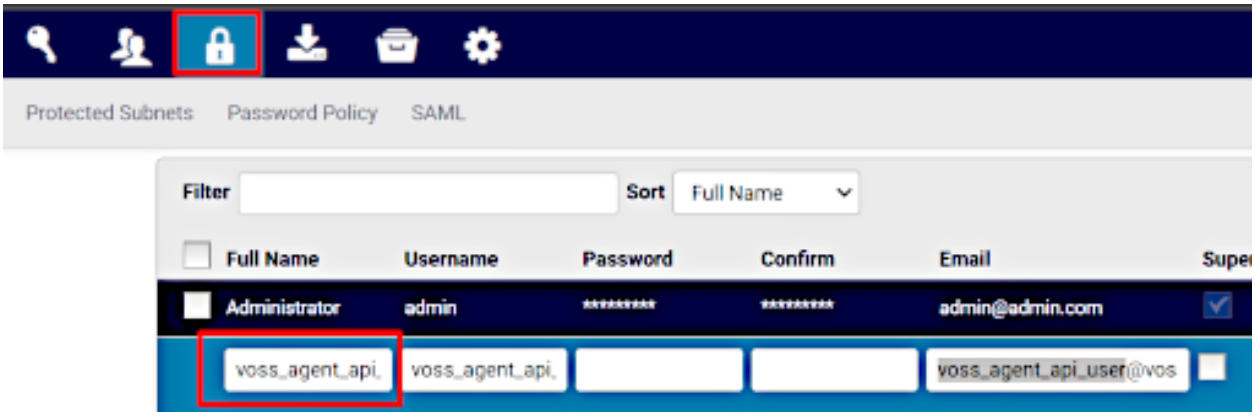
The recommended tests require the following connectivity if you intend to use them. Additional/alternate connectivity may be required if other tests are intended to be used.

The current schedule of test runs is every 5 minutes.

Destination	Protocol/Port/Type	Purpose
https://graph.microsoft.com	HTTPS 443 TCP	Graph API connectivity
https://graph.microsoft.com	ICMP	Reachability stats for graph
https://teams.microsoft.com	HTTPS 443 TCP	Access to Teams front-end
https://teams.microsoft.com	ICMP	Reachability stats for Teams
https://login.microsoftonline.com	HTTPS 443 TCP	Web Testing example - microsoft login front-end
https://outlook.office.com	HTTPS 443 TCP	Web Testing example - Microsoft exchange web
https://outlook.Office365.com	HTTPS 443 TCP	Web Testing example - Microsoft exchange web

Setup and Configuration

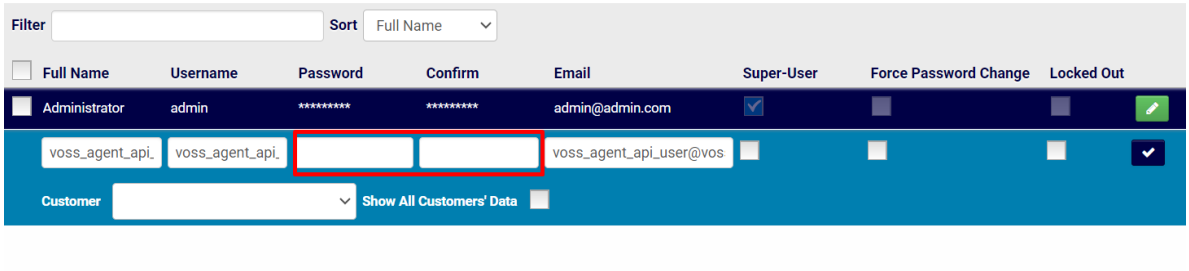
From release 24.1, the Arbitrator is automatically furnished with a new user account. This username is : `voss_agent_api_user`



Important: By default, no password is set for this user. Therefore, this account needs to have a password set.

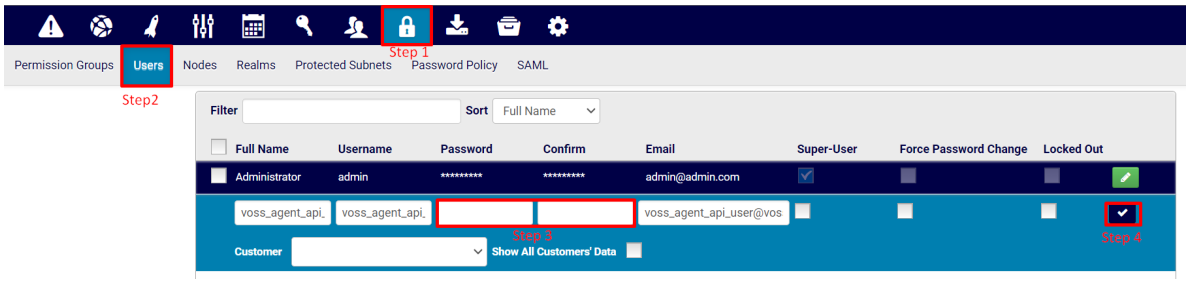
To set the user password, log in to the configuration area of the Arbitrator and follow the steps below:

1. Click on **Access Control**  .
2. Click on **Users**  .
3. Click on the green pencil  to modify.
4. Set the password.



Note when entering the password, you will see the text, but once the password is saved, it will be masked.

5. Once the password has been set, click the blue tick mark to confirm  .
6. Click **Save** at the bottom of the page.



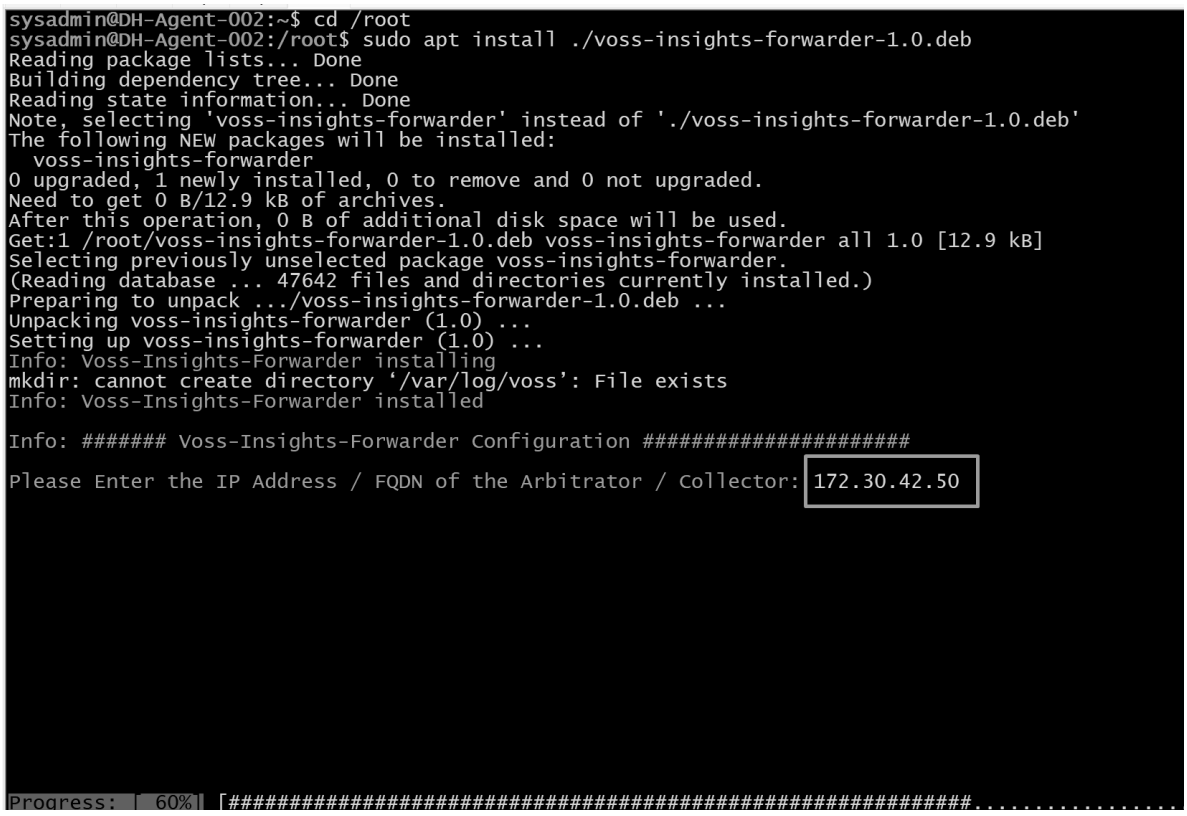
Agent Installation

When installing the Voss-Forwarder package to the agent host, a number of failsafe options built in to assist you with the correct installation. These are also highlighted below.

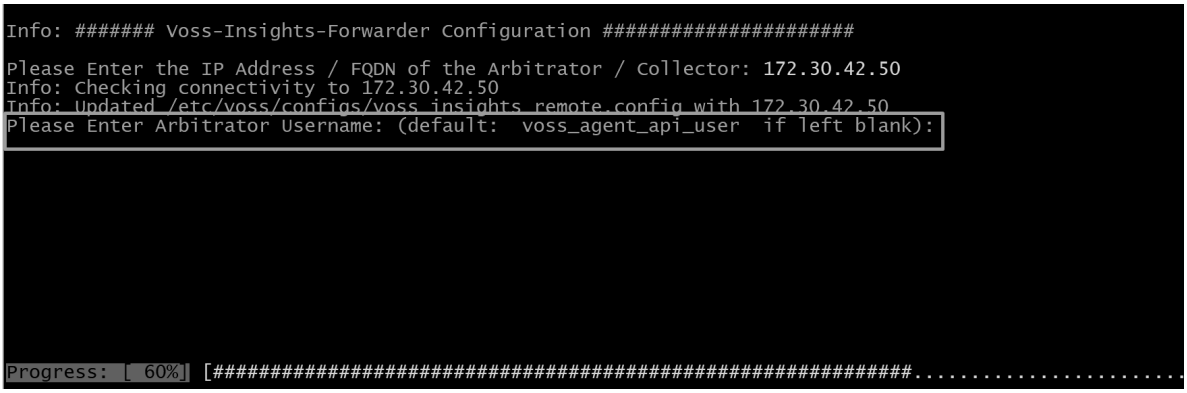
The first step is to move the installation file to the host. (Use SCP, Filezilla, etc.)

The current file is named: `voss-insights-forwarder-1.0.deb`

1. At the host prompt, run: `sudo apt install ./voss-insights-forwarder-1.0.deb`

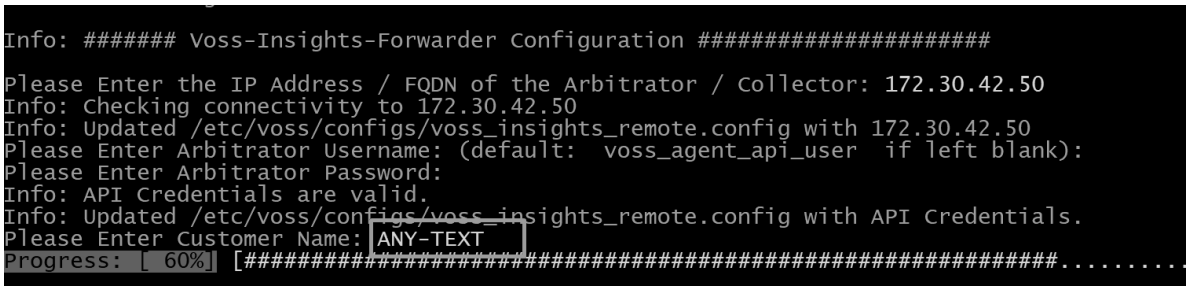


2. Enter the IP Address or FQDN of the Arbitrator that the agent is to report to then press Enter. The agent will now do a connectivity check via ICMP (Ping) to the Arbitrator.
   - If connectivity is good, move on to the next step.
   - If there is no connectivity after 4 attempts, the package will exit.

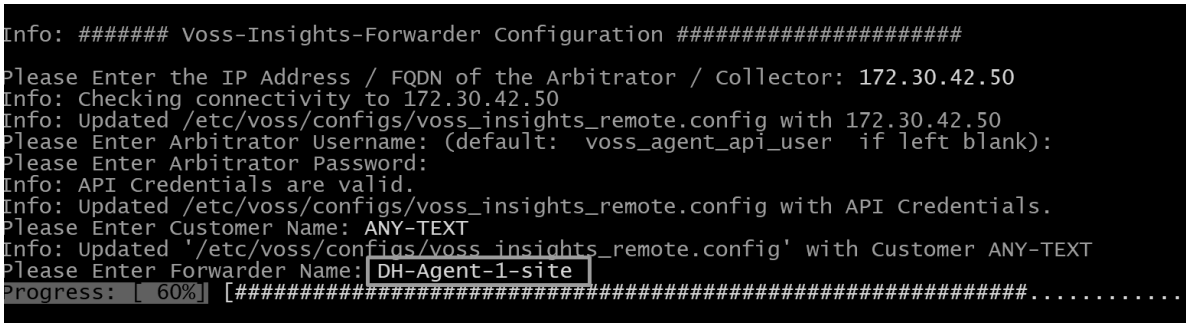


3. Enter the username (if you created a new API user) or keep the default user and press Enter.

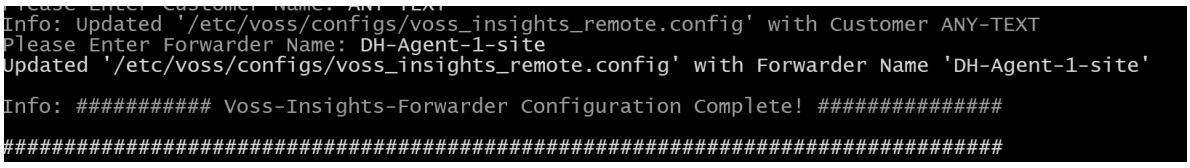
4. Enter the password (set on the Arbitrator). This will then check the credentials are valid.
   - If credentials are valid, you move on to the next step.
   - If credentials are invalid after 4 attempts, the package will exit.



5. Enter a customer name (data is required to continue) and press Enter.



6. Enter the Forwarder name (this should for example be a descriptive location). Press Enter.



This completes the configuration.

The **DEM Agent Stats** dashboard under **Diagnostics > Synthetic Transactions Dashboards** then shows each agent configuration on the widgets: **Forwarder System Stats** and **Forwarder Linux Distributions**.

See also:

the Diagnostics section under *Insights Reference Dashboards* in the Dashboard Administration Guide.

Changes to Agent Configuration

In the event of redeploying the agent to another site or a different Arbitrator, the commands below allow you to make these changes.

To update or change configuration, run any of the following commands:

- To change the IP Address or FQDN for the Arbitrator:

  ```
  sudo ./etc/voss/bin/update-forwarder-arbitrator.sh
  ```

- To update / change the API credentials:

  ```
  sudo ./etc/voss/bin/update-forwarder-credentials.sh
  ```

- To update / change the Customer:

  ```
  sudo ./etc/voss/bin/update-forwarder-customer.sh
  ```

- To update / change the Forwarder Name:

  ```
  sudo ./etc/voss/bin/update-forwarder-name.sh
  ```

Index

F