VOSS Insights
Arbitrator Install Guide

Release 24.2

November 22, 2024

Legal Information

DOCUMENT ID: 20241122145305

Contents

1. What's New

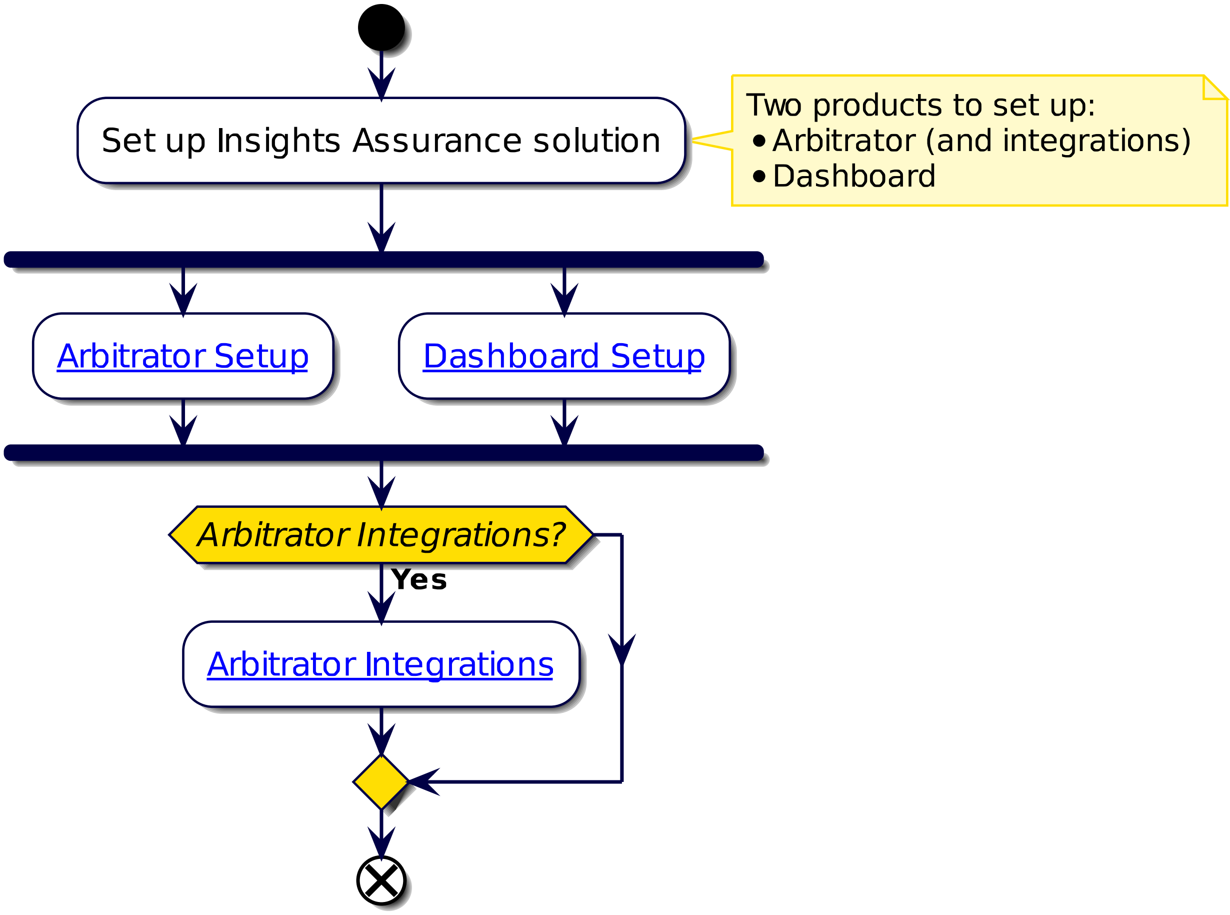
1.1. Arbitrator Install Guide: Release 24.2

- EKB-21311: Add admin option on dashboard to disable sendmail for improved security. See: *Deploy and VM Installation*

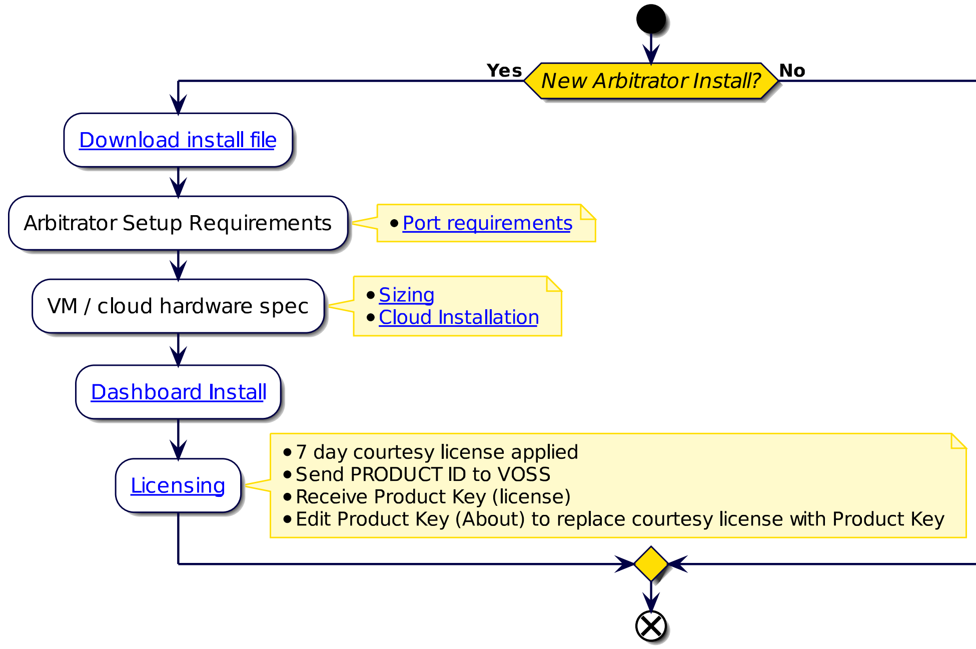
  Added details on the admin menu option on the Dashboard to disable Sendmail.

2. Insights Assurance Quickstart

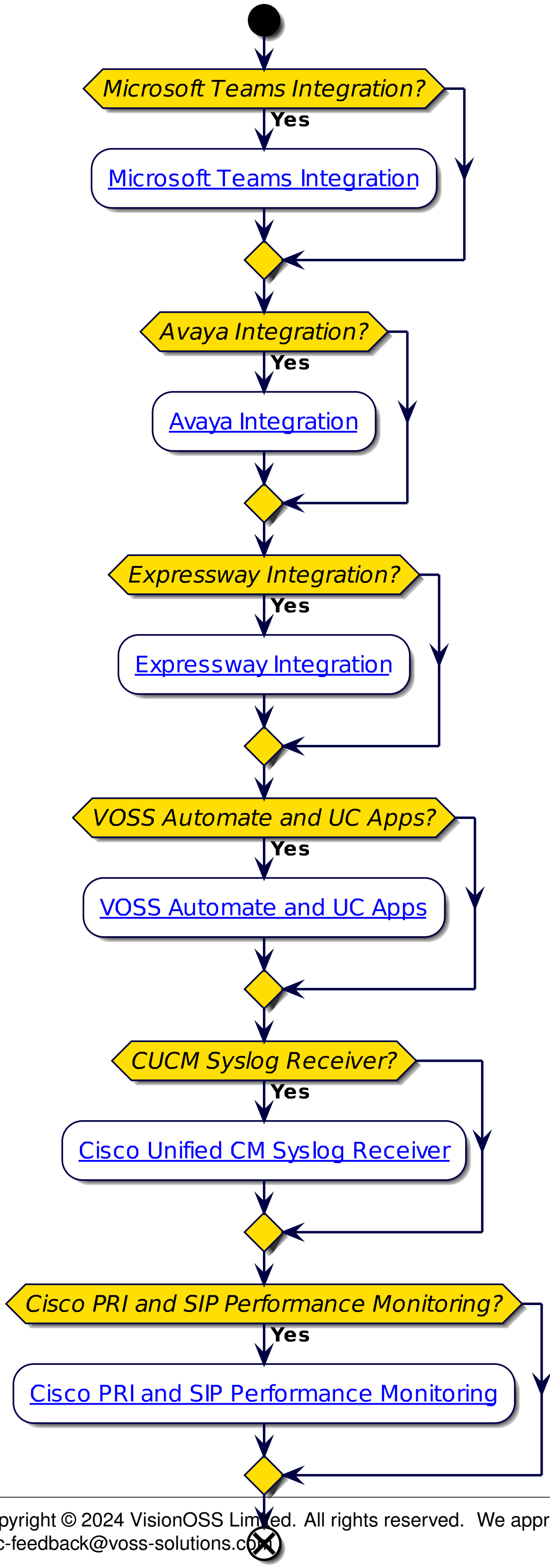
2.1. Insights Assurance Setup Overview



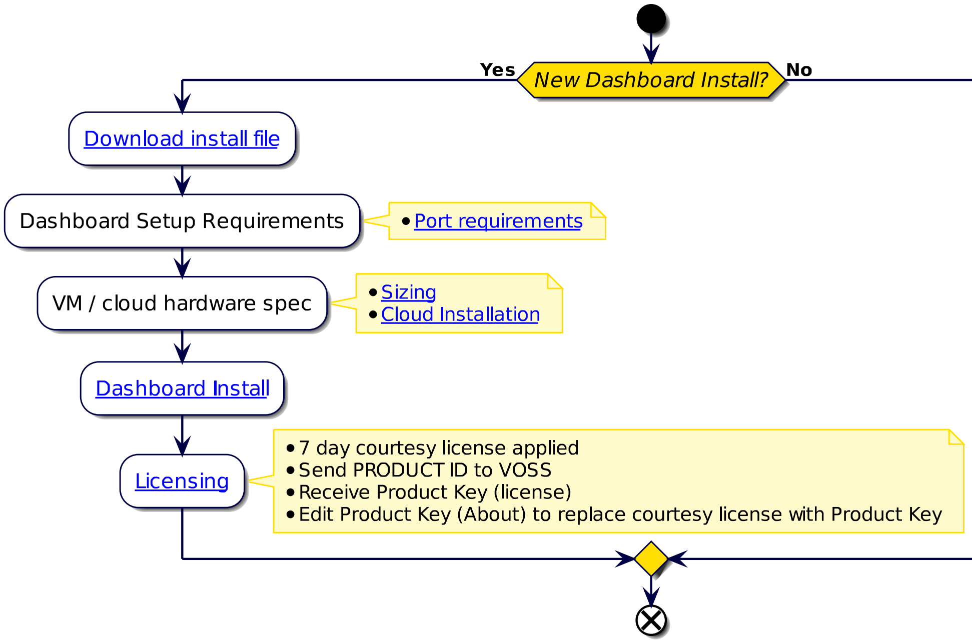
2.2. Arbitrator Setup


New Arbitrator Install?
Yes
No
Download install file
Arbitrator Setup Requirements
• Port requirements
VM / cloud hardware spec
• Sizing
• Cloud Installation
Dashboard Install
Licensing
• 7 day courtesy license applied
• Send PRODUCT ID to VOSS
• Receive Product Key (license)
• Edit Product Key (About) to replace courtesy license with Product Key
Download upgrade file
Upgrade Arbitrator

2.3. Arbitrator Integrations


Microsoft Teams Integration?
Yes
Microsoft Teams Integration
Avaya Integration?
Yes
Avaya Integration
Expressway Integration?
Yes
Expressway Integration
VOSS Automate and UC Apps?
Yes
VOSS Automate and UC Apps
CUCM Syslog Receiver?
Yes
Cisco Unified CM Syslog Receiver
Cisco PRI and SIP Performance Monitoring?
Yes
Cisco PRI and SIP Performance Monitoring

2.4. Dashboard Setup


New Dashboard Install?
Yes
No
Download install file
Dashboard Setup Requirements
• Port requirements
VM / cloud hardware spec
• Sizing
• Cloud Installation
Dashboard Install
Licensing
• 7 day courtesy license applied
• Send PRODUCT ID to VOSS
• Receive Product Key (license)
• Edit Product Key (About) to replace courtesy license with Product Key
Download upgrade file
Upgrade Dashboard

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)	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 recommended 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, 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	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
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
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	VOSS Webhooks Server	443 TCP	The VOSS Webhooks server receives call record notifications from Microsoft. The Webhooks server only receives call record IDs with minimal details. The Arbitrator periodically pulls these call record IDs from the Webhooks server. In order to do this, the Arbitrator requires access to the internet, specifically, to cloud.voss-solutions.com on port 443.
Arbitrator	Microsoft (https://graph.microsoft.com/v1.0)	443 TCP	The Arbitrator will then pull 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 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	**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

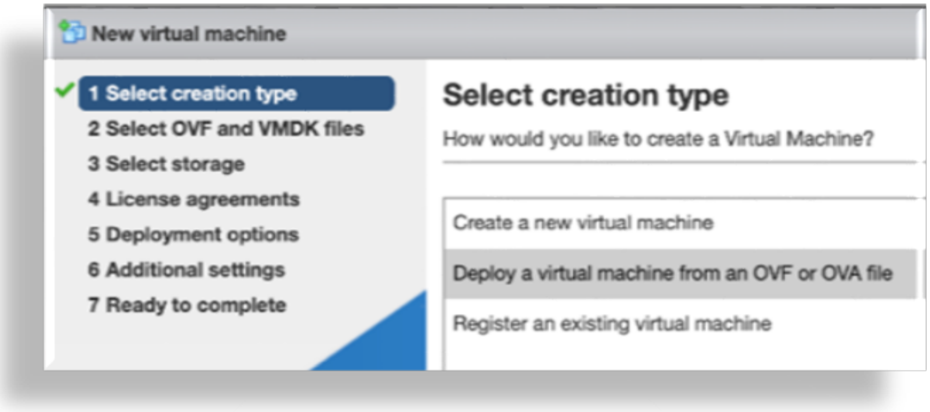
6.1. Deploy and VM Installation

6.1.1. Base Install and Configuration

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

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



Select creation type

How would you like to create a Virtual Machine?

Deploy a virtual machine from an OVF or OVA file

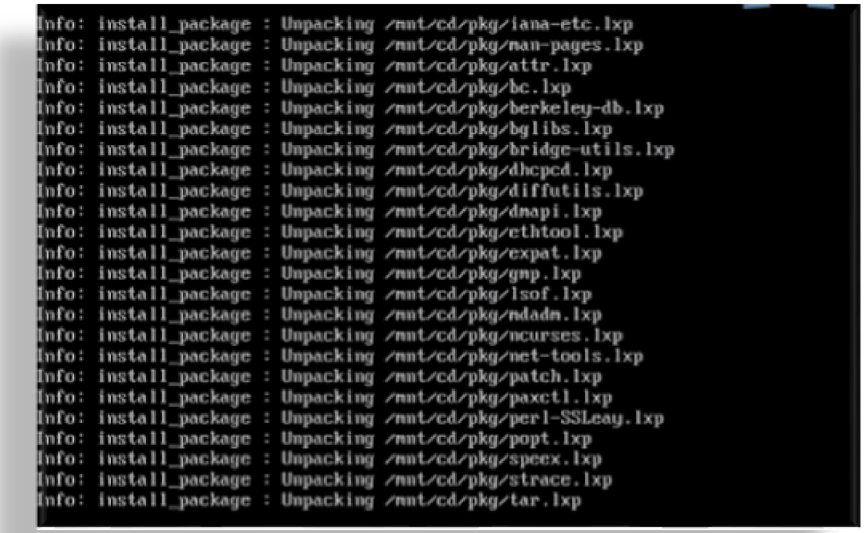
    2. Configure storage settings via the **Select storage** menu, based on the recommended hardware specifications for the required configuration.

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

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

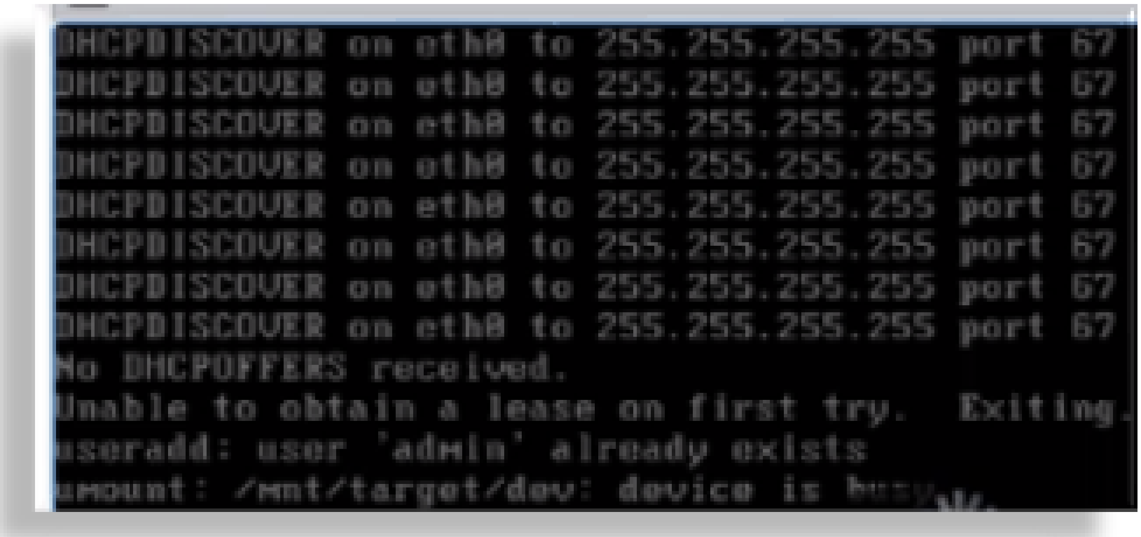
See the *VMWare Specification and Requirements* for your system.

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



```
Info: install_package : Unpacking /mnt/cd/pkg/iana-etc.lxp
Info: install_package : Unpacking /mnt/cd/pkg/man-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/dhcpcd.lxp
Info: install_package : Unpacking /mnt/cd/pkg/diffutils.lxp
Info: install_package : Unpacking /mnt/cd/pkg/dmapi.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-SSLeay.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 eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 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>
        Flavor:
```

(continues on next page)

(continued from previous page)

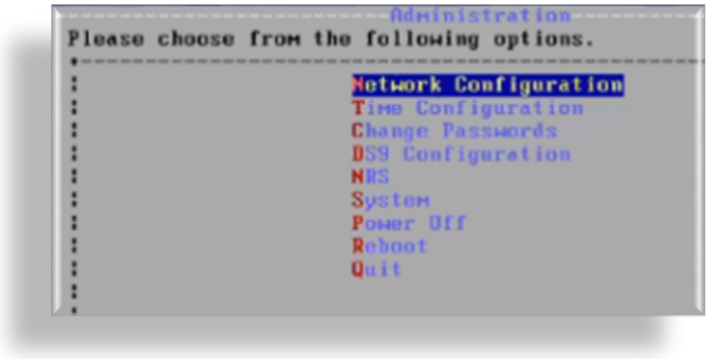
```
      License:  NNNNN-NNNNN-NNNNN-NNNNN-NNNNN
 Days Licensed:  nnnnn
Days Remaining:  nnnnn
   Product Key:
       Website:  <website>
        Kernel:  Linux n.nn.nn-lxt-3 x86_64 GNU/Linux

<hostname> login:
```

4. Log in:

   - On the **About** console, at **<hostname> login:**, log in as `admin`. For the password, use 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 logged in, the **Administration** menu displays (the image displays an example for DS9):



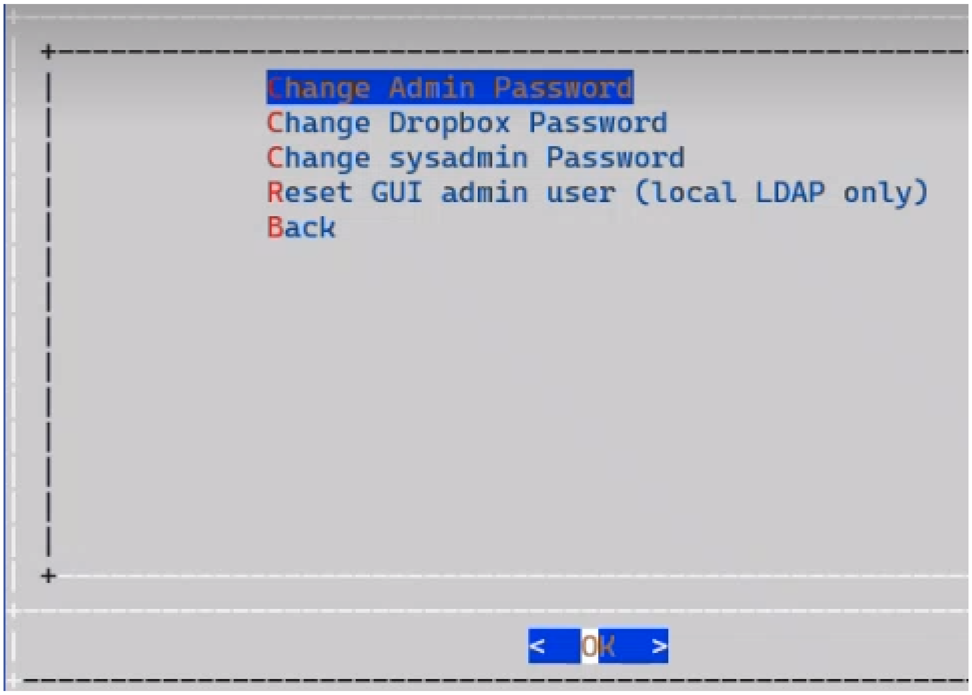
```
Administration
Please choose from the following options.

                    Network Configuration
                    Time Configuration
                    Change Passwords
                    DS9 Configuration
                    NRS
                    System
                    Power Off
                    Reboot
                    Quit
```

5. Change your password:

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

   Note:

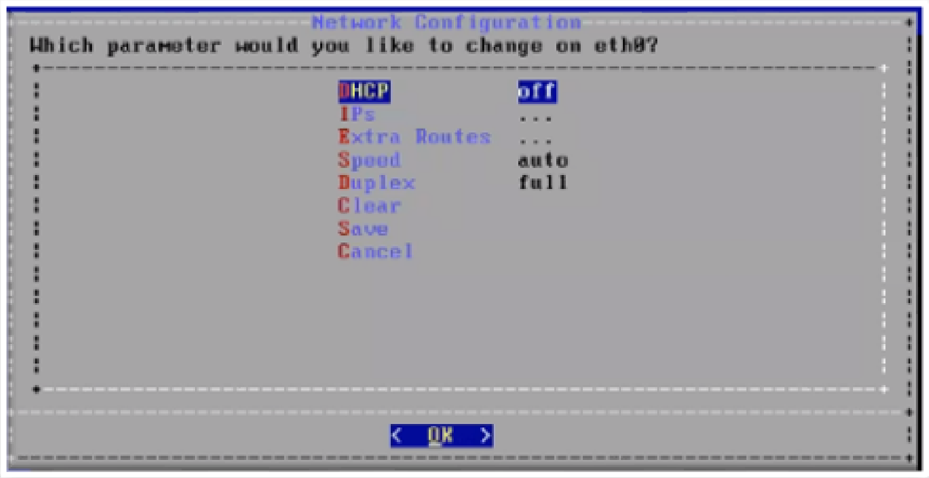
   - It is strongly recommended that you change your password immediately.
   - The **Reset GUI admin user** option on the allows for this admin user's password reset.



6. Configure network settings:

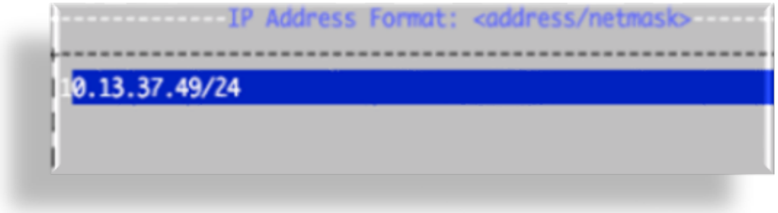
   1. On the **Administration** menu, select **Network Configuration**.
   2. Configure interface settings via the **Interface Settings** menu:

      1. Select the relevant interface.



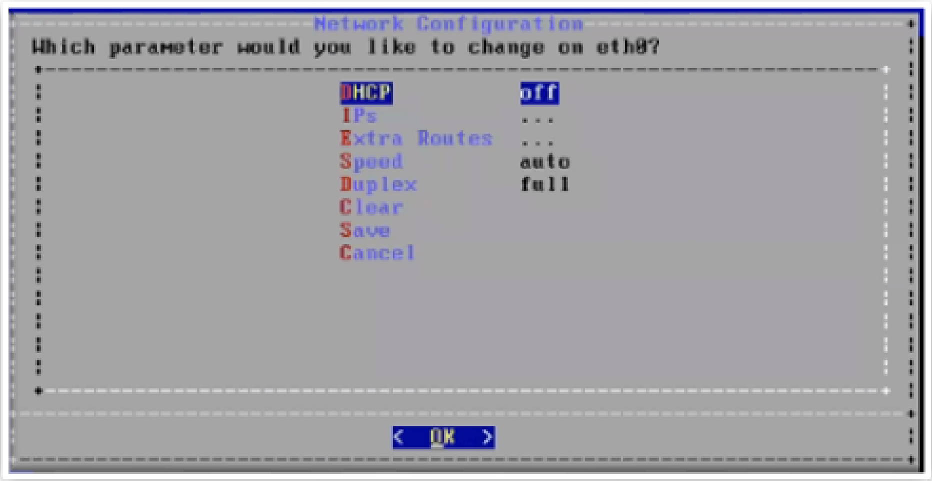
```
Network Configuration
Which parameter would you like to change on eth0?

DHCP            off
IPs             ...
Extra Routes    ...
Speed           auto
Duplex          full
Clear
Save
Cancel
```

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



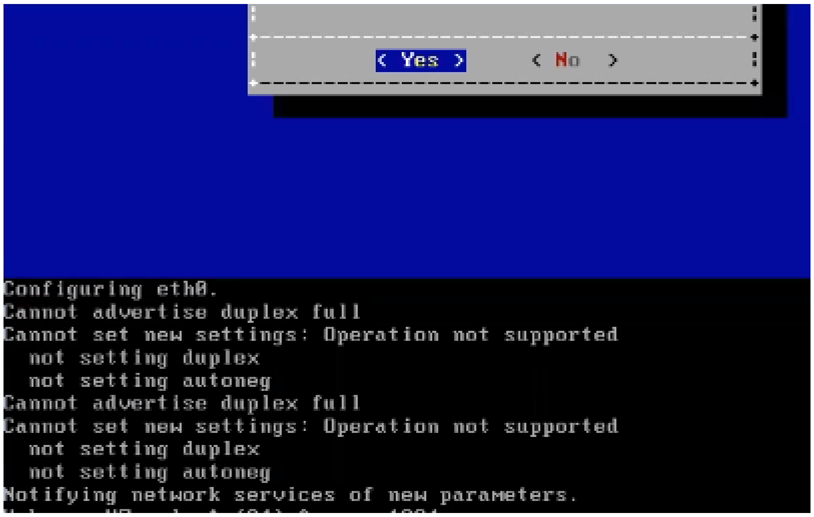
```
IP Address Format: <address/netmask>
10.13.37.49/24
```

3. Configure the default gateway via the **Extra Routes** menu.



```
Network Configuration
Which parameter would you like to change on eth0?

          DHCP            off
          IPs             ...
          Extra Routes    ...
          Speed           auto
          Duplex          full
          Clear
          Save
          Cancel

                  < OK >
```

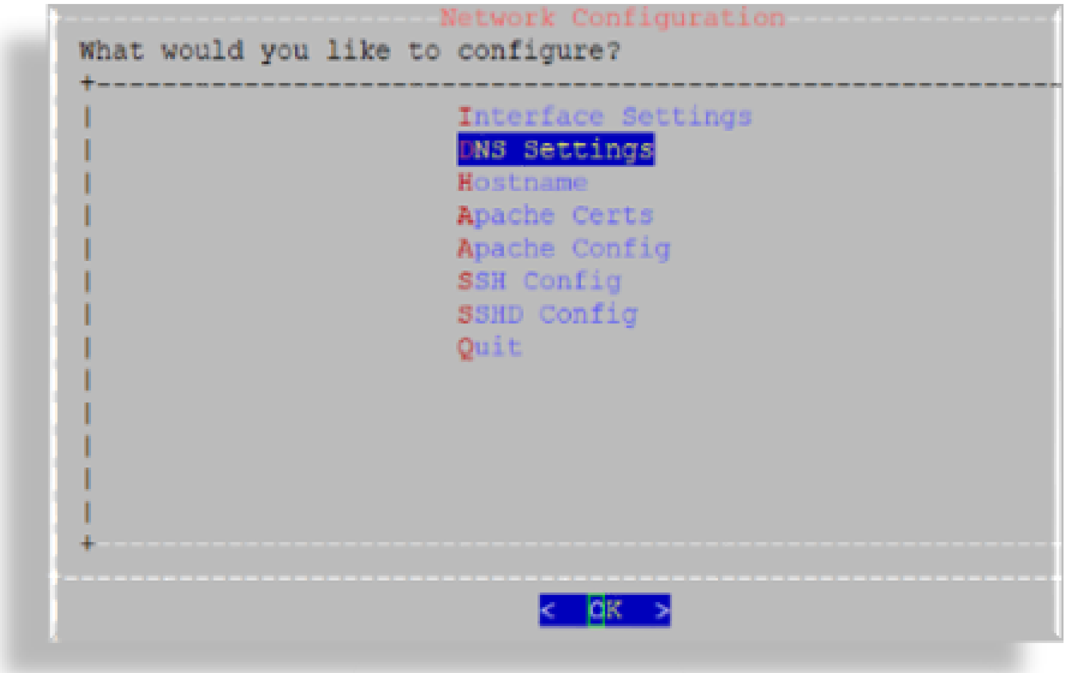
- Use the following format for the entry: *default <gateway IP address>*
- The word *default* is required. For additional route entries use the *<subnet>* < *gateway>* format. Similar to what would be done on a Linux system at the CLI.



```
< Yes >    < No  >
```

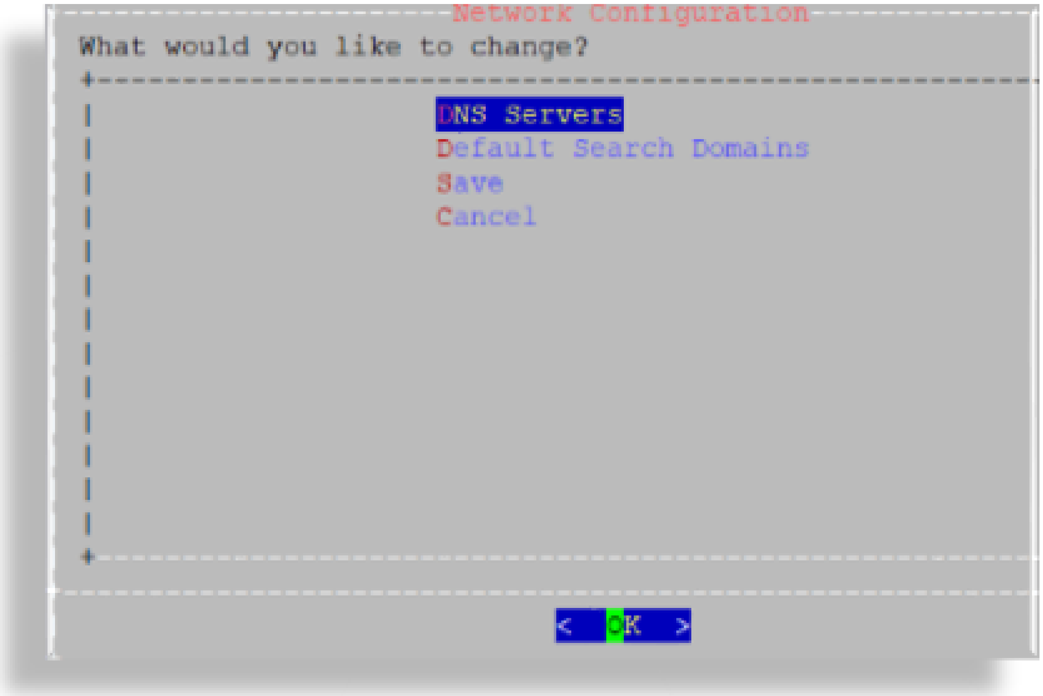
```
Configuring eth0.
Cannot advertise duplex full
Cannot set new settings: Operation not supported
  not setting duplex
  not setting autoneg
Cannot advertise duplex full
Cannot set new settings: Operation not supported
  not setting duplex
  not setting autoneg
Notifying network services of new parameters.
```

4. Configure DNS settings via the **DNS Settings** menu:



What would you like to configure?

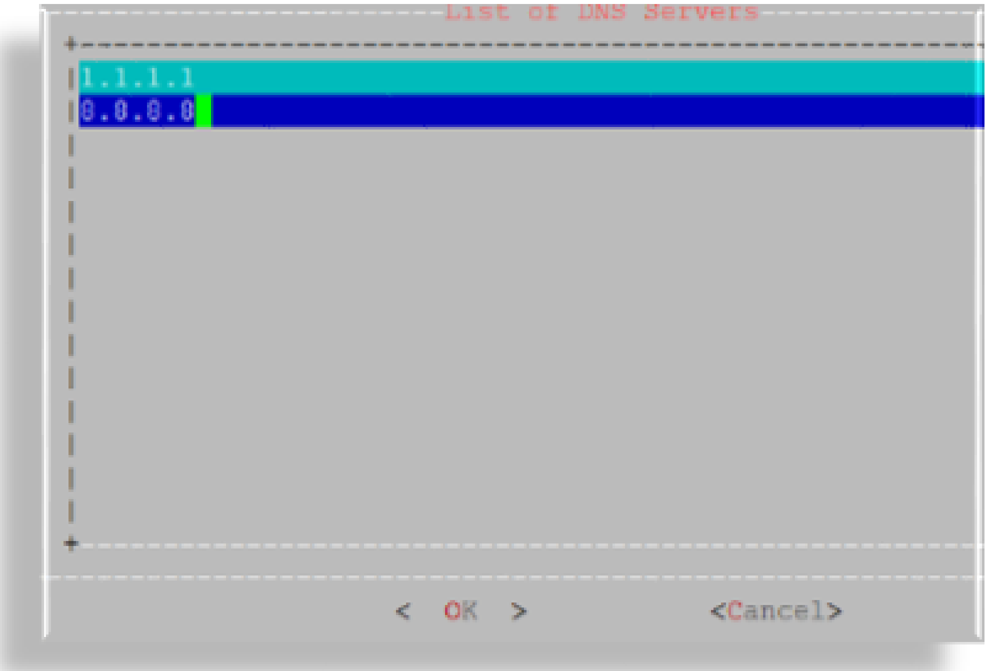
1. Select **DNS Servers**.



What would you like to change?

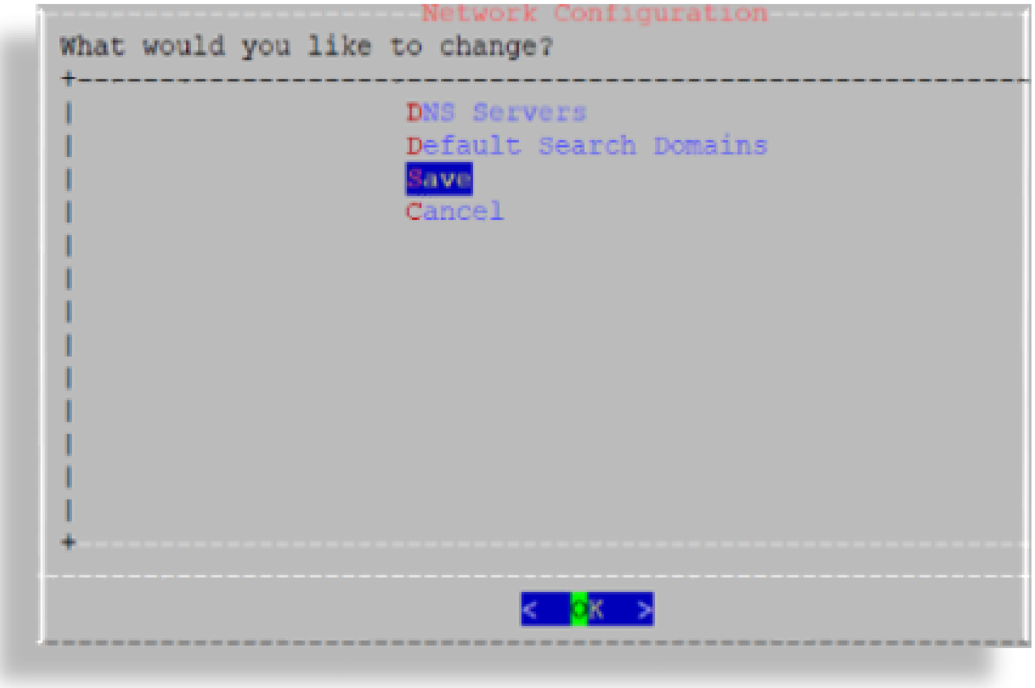
2. Add the IP address for each DNS server, one per line, then click **OK**.

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



```
1.1.1.1
8.8.8.8
```

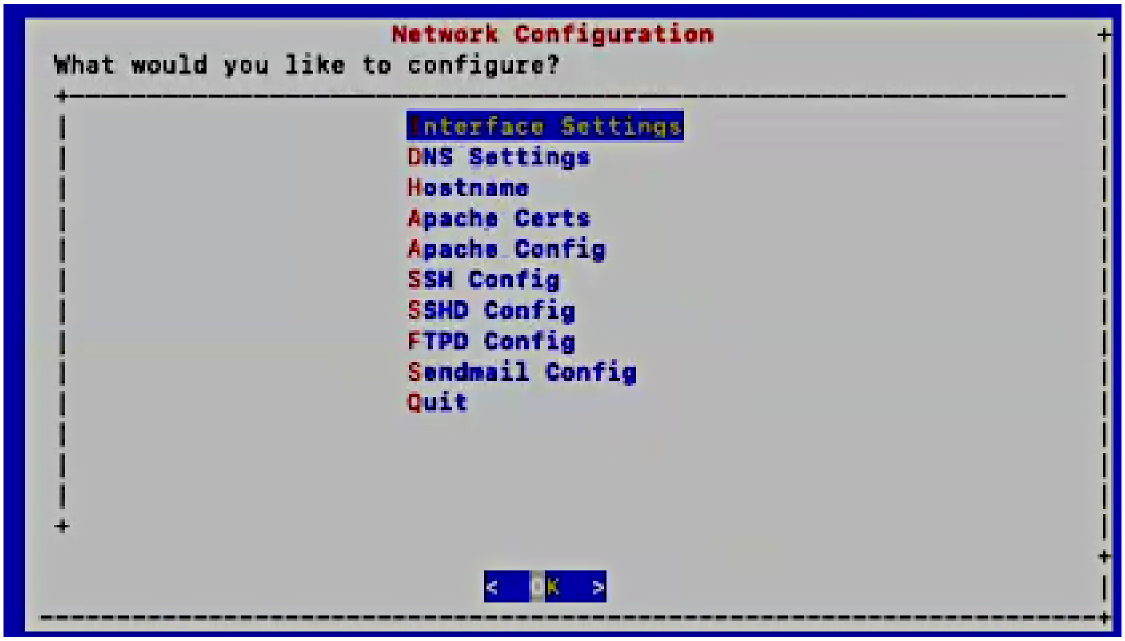
3. Click **Save**.



```
What would you like to change?
```

5. Configure the hostname via the **Hostname** menu, then save to trigger the update.

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



Network Configuration

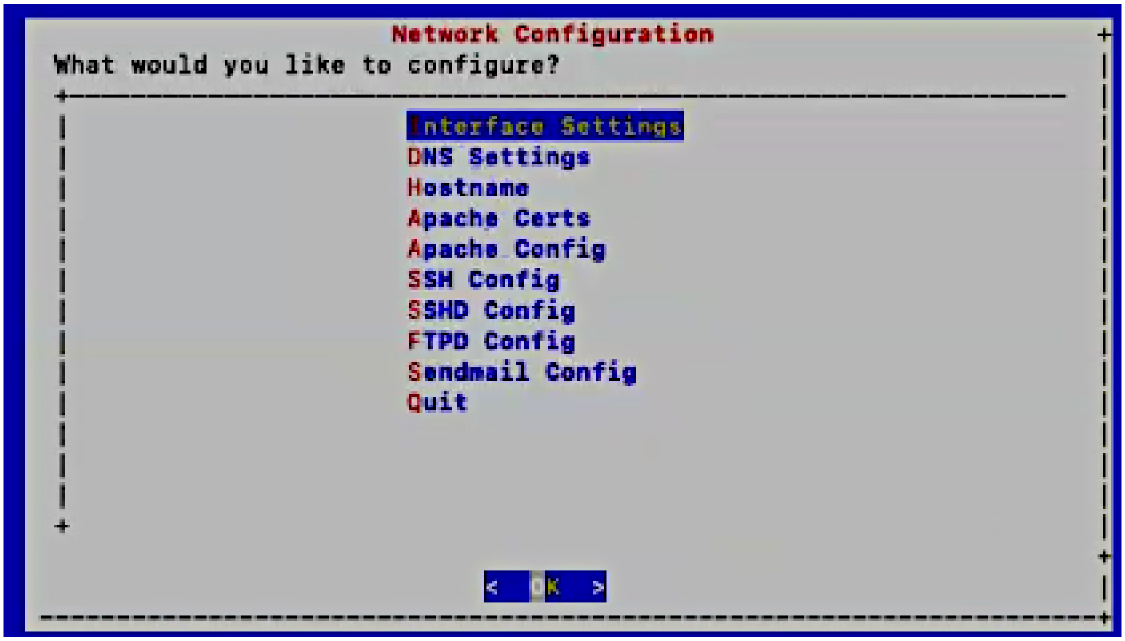
What would you like to configure?

6. Update SSL ciphers via the **Apache Config** menu.

```
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.



Network Configuration

What would you like to configure?

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

7. Configure SSH settings via the **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
   ```

8. Configure SSHD via the **SSHD Config** menu.

   Note:

   - Multi-line entries can be added, if required. For example, for CUCM v11.5 support, see: *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.

9. Enable/disable FTPD or restart the FTPD daemon:

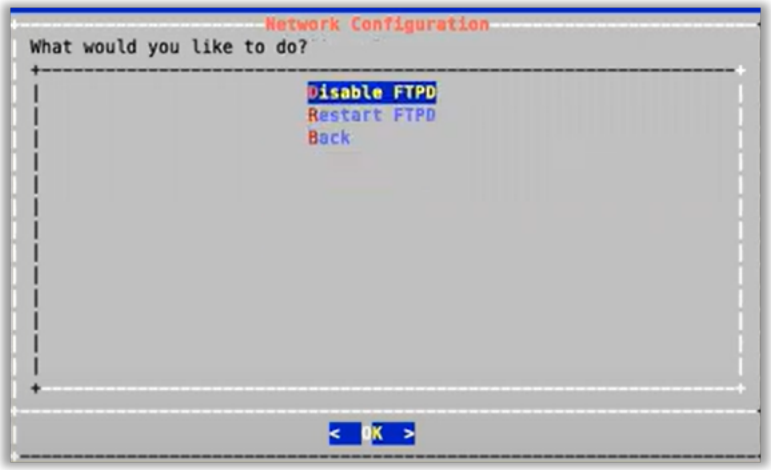
   1. On the **Administration** menu, select **Network Configuration**.
   2. Select **FTPD Config**.

      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.

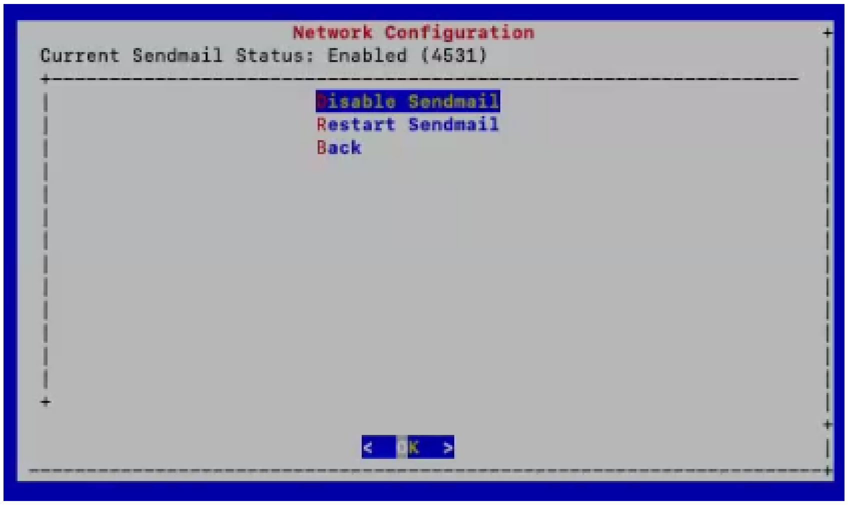
      The drop account username is “drop”. You can set the password via the **Administration** menu.



Network Configuration

What would you like to do?

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



```
Current Sendmail Status: Enabled (4531)
```

1. On the **Administration** menu, select **Network Configuration**.
2. Select **Sendmail Config**. The current status of the service is displayed on the menu.

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

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

   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

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 will also contain several correlation rules that are designed to create Alerts based on the best practices of that particular system manufacturer.

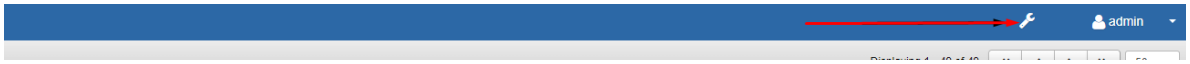
The configuration files in this table are installed at the end of the installation process. The table describes the purpose of the components:

Component	Purpose	Filename
Controls	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.	

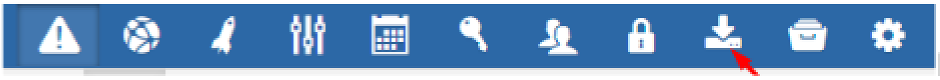
Policies	A set of rules for the data that is turned into an alert. It enables an alert to be generated and defines the alarm ID and the content of the alarm that gets presented to a user.	`SiteStats_08122020.lxcfg`
		`POLICIESUCCE221020.lxcfg`
		`POLICIESCUCM221020.lxcfg`
		`POLICIESCUCIMP221020.lxcfg`
		`PINGMON.lxcfg`

7.1.2. Installation Steps

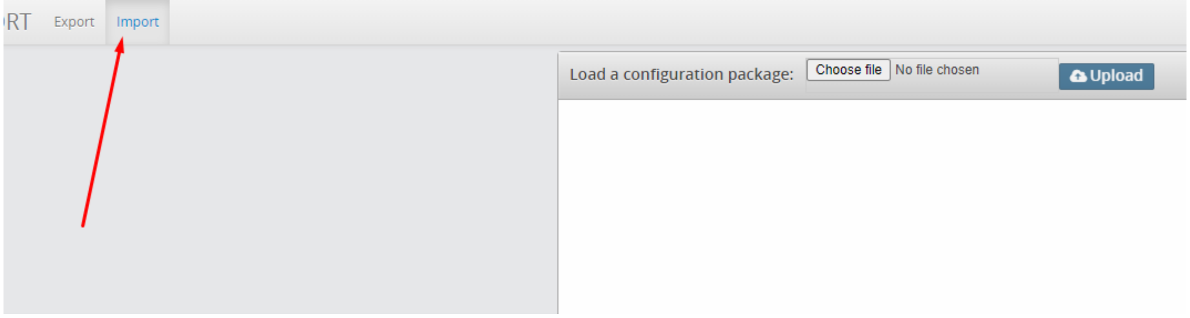
1. Log in to the Arbitrator: `admin/admin`
2. Click the Wrench icon.



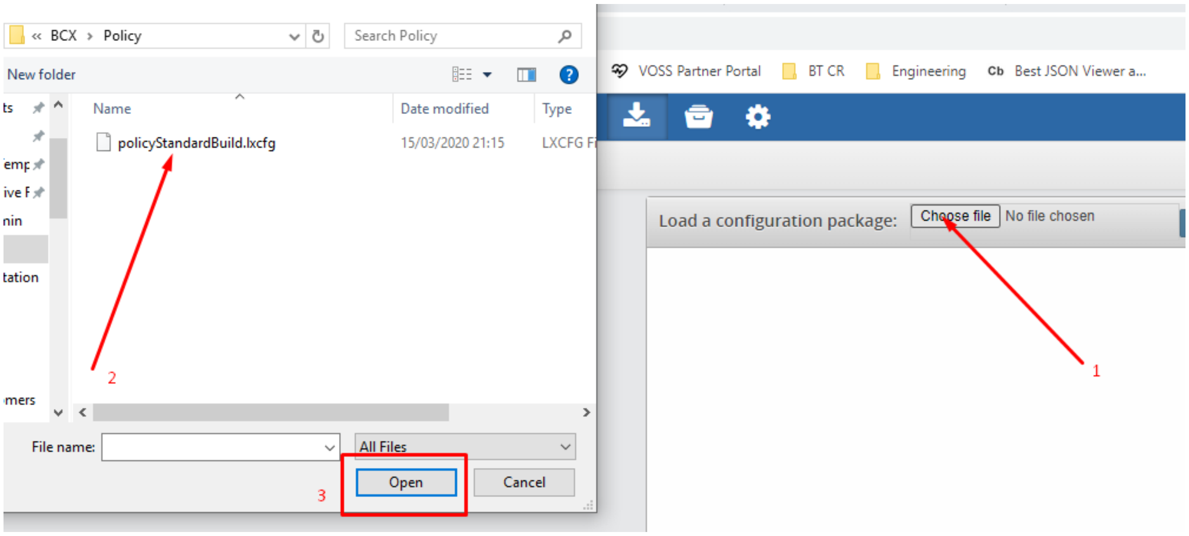
3. Click on the icon shown below



4. Click **Import**,



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

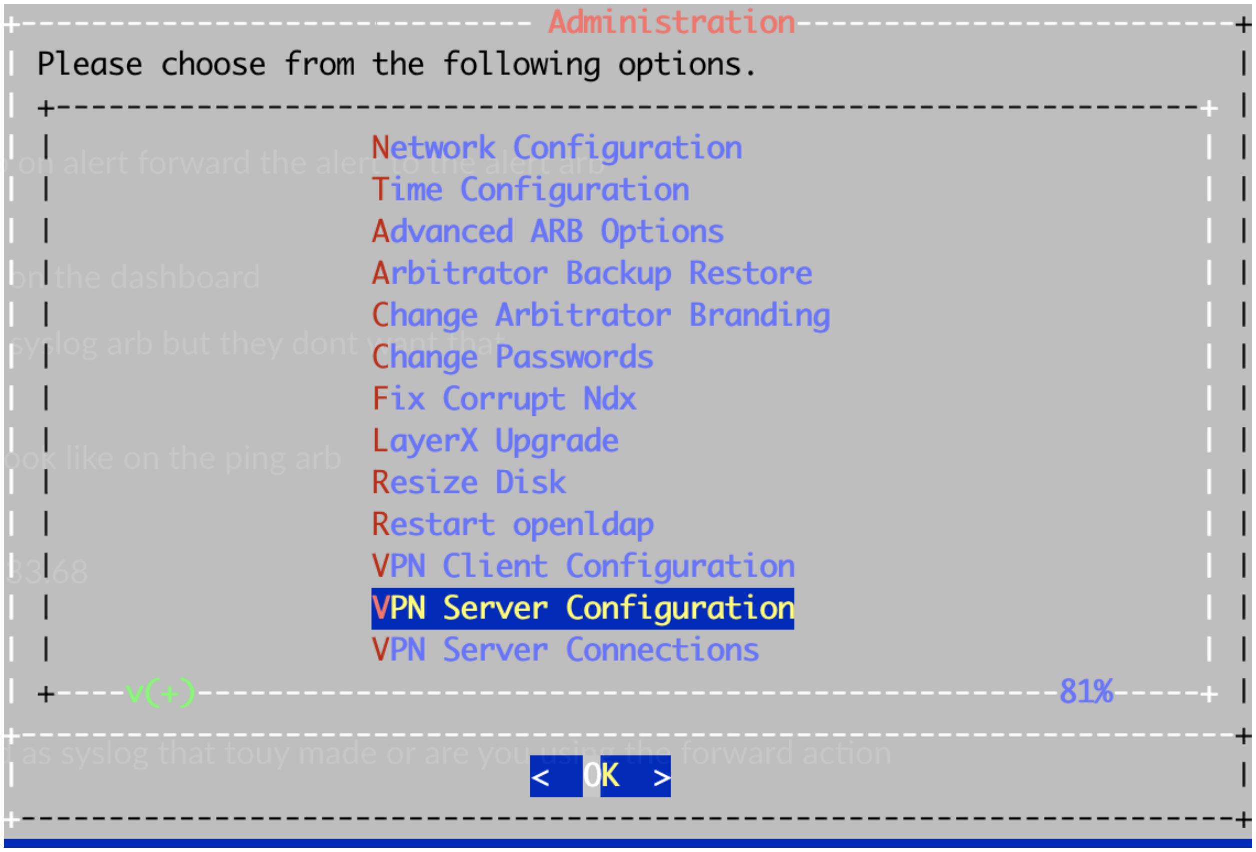


6. Ensure the name of the file you selected displays adjacent to **Choose file**, then click **Upload**.
7. Once the file has uploaded click **Import**.
8. Repeat this procedure for the following:
   - **Controls**
   - **Probes**
   - **Response Procedures**
   - **Policies**

   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



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

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)

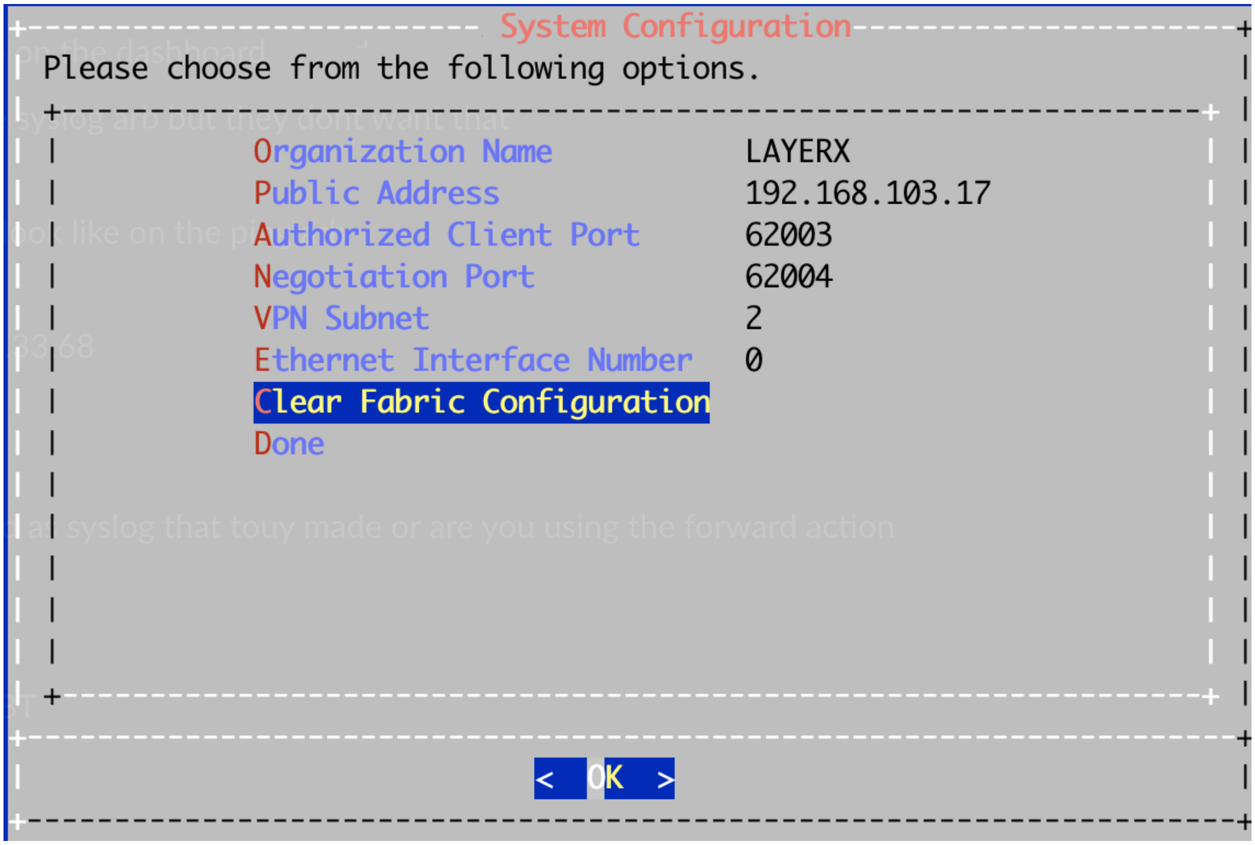
c. Set Authorized Client Port to 62003

d. Set the Negotiation Port to 62004

e. Set the VPN Subnet (to a number between 1 and 150)

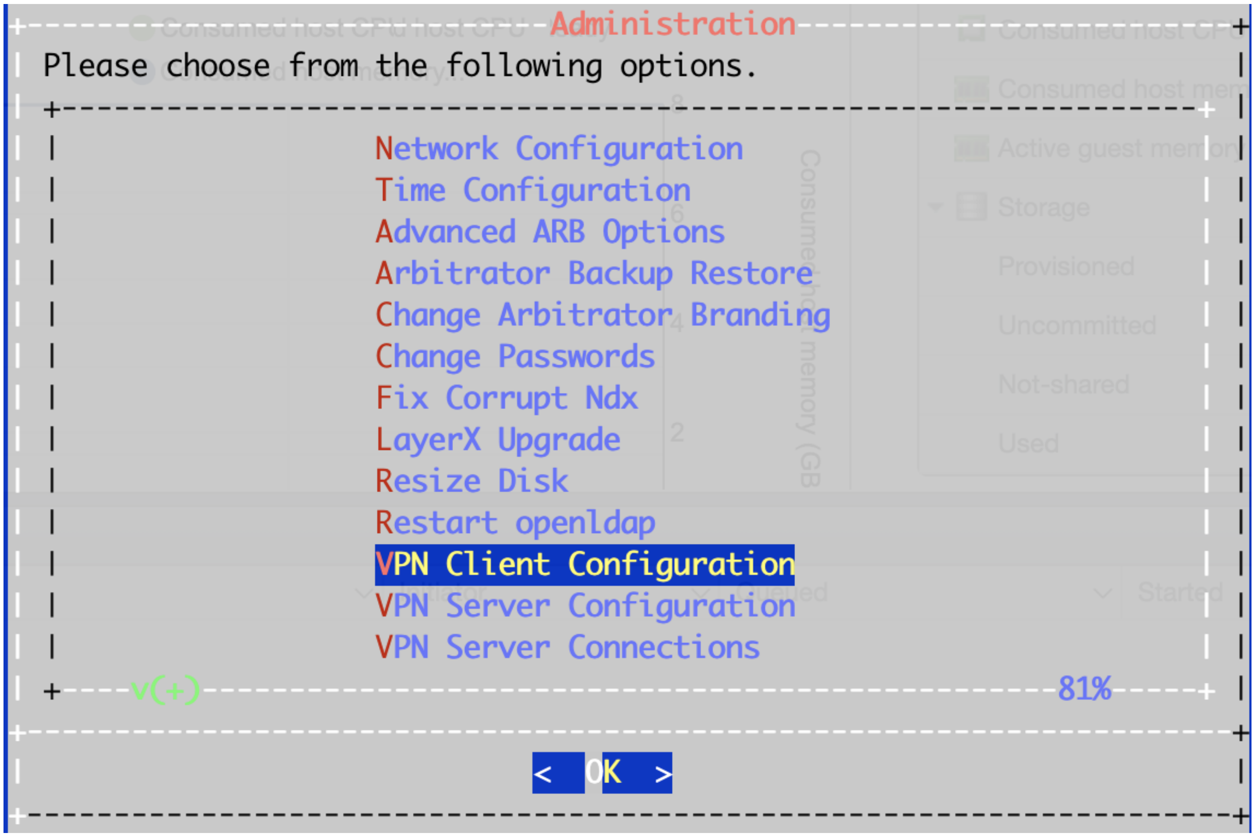
f. Set the Ethernet Interface Number (Usually 0)

As shown in the example below:



```
+------------------------- 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  >                                 |
+-----------------------------------------------------------------------+
```

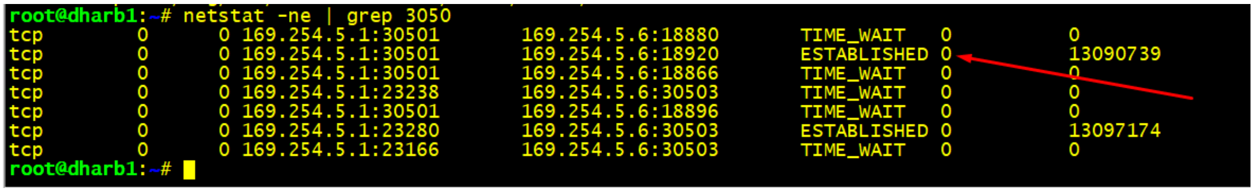
On the subordinate Arbitrator log in as admin and navigate to VPN Client Configuration



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**.

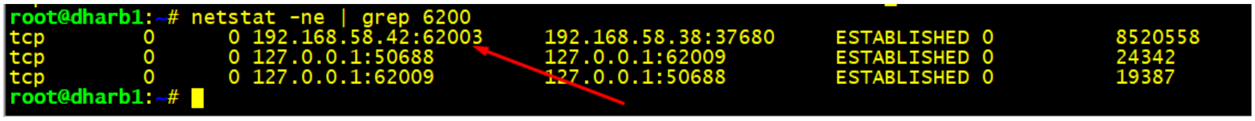
A Tunnel will now be set up between the Arbitrators.

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



```
root@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:~#
```

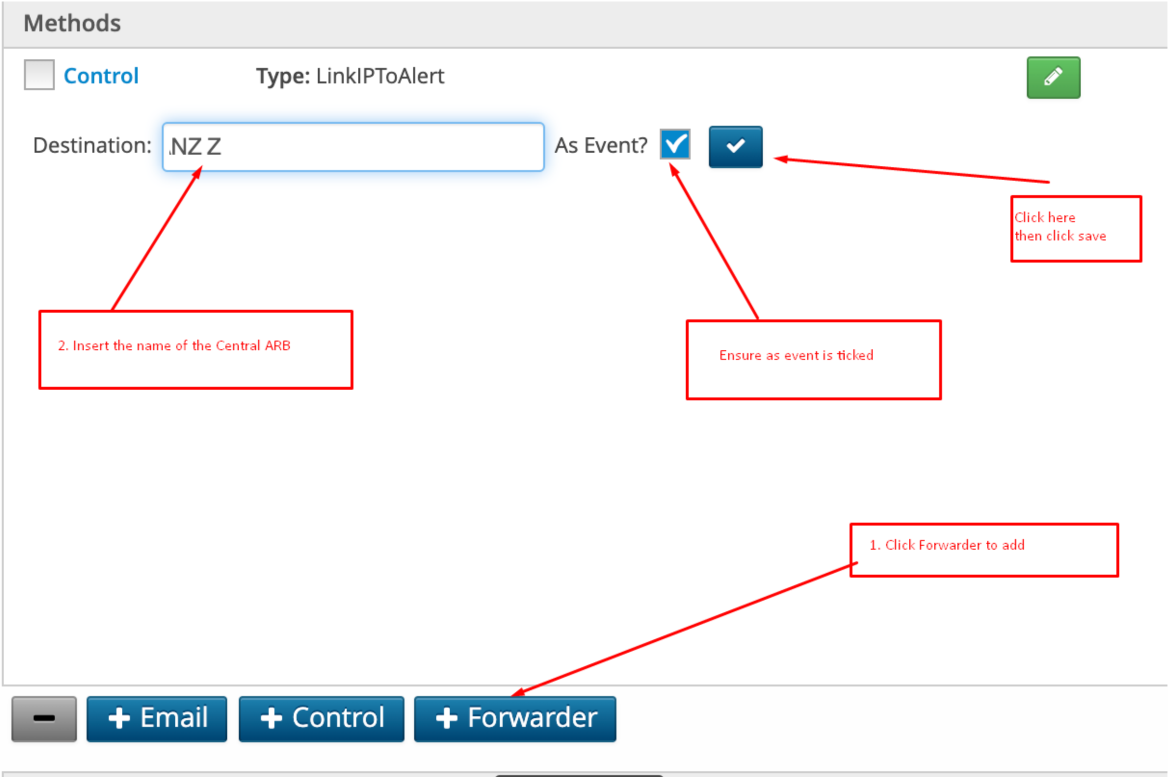
The tunnel is setup using `169.253.x.x` addresses:



```
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:



2. Insert the name of the Central ARB

Ensure as event is ticked

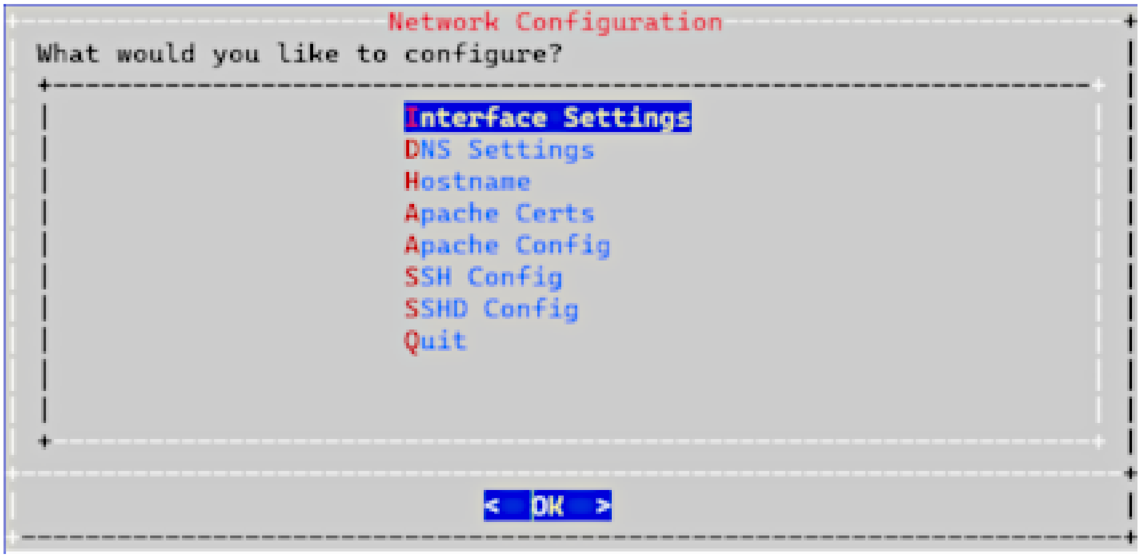
Click here then click save

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.



```
Network Configuration
What would you like to configure?

Interface Settings
DNS Settings
Hostname
Apache Certs
Apache Config
SSH Config
SSHD Config
Quit

< OK >
```

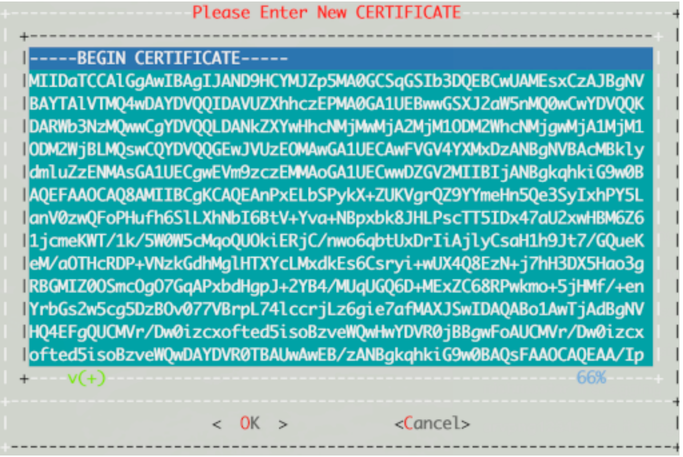
8.1.1. Add Certificates

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--
```



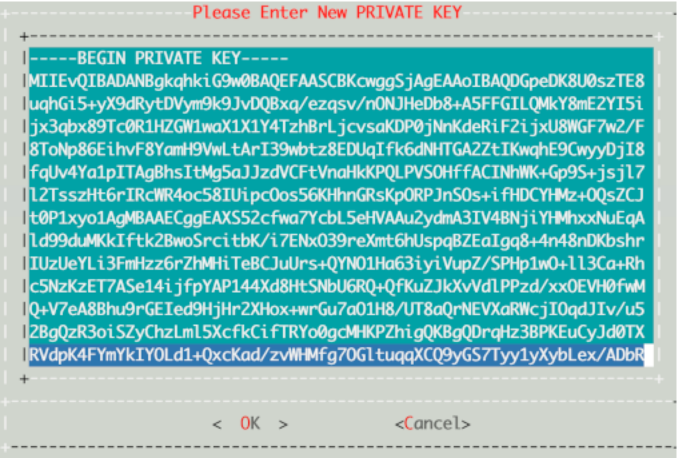
Please Enter New CERTIFICATE

```
-----BEGIN CERTIFICATE-----
MIIDaTCCAlGgAwIBAgIJAND9HCYMJZp5MA0GCSqGSIb3DQEBCwUAMEsxCzAJBgNV
BAYTAlVTMQ4wDAYDVQQIDAVUZXhhczEPMA0GA1UEBwwGSXJ2aW5nMQ0wCwYDVQQK
DARWb3NzMQwwCgYDVQQLDANkZXYwHhcNMjMwMjA2MjM1ODM2WhcNMjgwMjA1MjM1
ODM2WjBLMQswCQYDVQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBkly
dmluZzENMAsGA1UECgwEVm9zczEMMAoGA1UECwwDZGV2MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAnPxELbSPykX+ZUKVgrQZ9YYmeHn5Qe3SyIxhPY5L
anV0zwQFoPHufh6SlLXhNbI6BtV+Yva+NBpxbk8JHLPscTT5IDx47aU2xwHBM6Z6
1jcmeKWT/1k/5W0W5cMqoQUOkiERjC/nwo6qbtUxDrIiAjlyCsaH1h9Jt7/GQueK
eM/aOTHcRDP+VNzkGdhMglHTXYcLMxdkEs6Csryi+wUX4Q8EzN+j7hH3DX5Hao3g
RBGMIZ0OSmcOgO7GqAPxbdHgpJ+2YB4/MUqUGQ6D+MExZC68RPwkmo+5jHMf/+en
YrbGs2w5cg5DzBOv077VBrpL74lccrjLz6gie7afMAXJSwIDAQABo1AwTjAdBgNV
HQ4EFgQUCMVr/Dw0izcxofted5isoBzveWQwHwYDVR0jBBgwFoAUCMVr/Dw0izcx
ofted5isoBzveWQwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAA/Ip
```

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--
```



Please Enter New PRIVATE KEY

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDGpeDK8U0szTE8
uqhGi5+yX9dRytDVym9k9JvDQBxq/ezqsv/nONJHeDb8+A5FFGILQMkY8mE2YI5i
jx3qbx89Tc0R1HZGW1waX1X1Y4TzhBrLjcvsaKDP0jNnKdeRiF2ijxU8WGF7w2/F
8ToNp86EihvF8YamH9VwLtArI39wbtz8EDUqIfk6dNHTGA2ZtIKwqhE9CwyyDjI8
fqUv4Ya1pITAgBhsItMg5aJJzdVCFtVnaHkKPQLPVSOHffACINhWK+Gp9S+jsjl7
l2TsszHt6rIRcWR4oc58IUipcOos56KHhnGRsKpORPJnSOs+ifHDCYHMz+OQsZCJ
t0P1xyo1AgMBAAECggEAXS52cfwa7YcbL5eHVAAu2ydmA3IV4BNjiYHMhxxNuEqA
ld99duMKkIftk2BwoSrcitbK/i7ENxO39reXmt6hUspqBZEaIgq8+4n48nDKbshr
IUzUeYLi3FmHzz6rZhMHiTeBCJuUrs+QYNO1Ha63iyiVupZ/SPHp1wO+ll3Ca+Rh
c5NzKzET7ASe14ijfpYAP144Xd8HtSNbU6RQ+QfKuZJkXvVdlPPzd/xxOEVH0fwM
Q+V7eA8Bhu9rGEIed9HjHr2XHox+wrGu7aO1H8/UT8aQrNEVXaRWcjIOqdJIv/u5
2BgQzR3oiSZyChzLml5XcfkCifTRYo0gcMHKPZhigQKBgQDrqHz3BPKEuCyJd0TX
RVdpK4FYmYkIYOLd1+QxcKad/zvWHMfg7OGltuqqXCQ9yGS7Tyy1yXybLex/ADbR
```

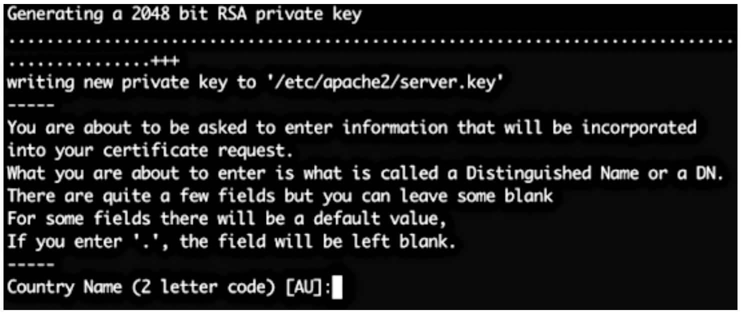
8. Select **Display Cert Details** to view certificate details.
9. Select **Back** and exit the menu.
10. Refresh the browser. The system should be using the new certificate.

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

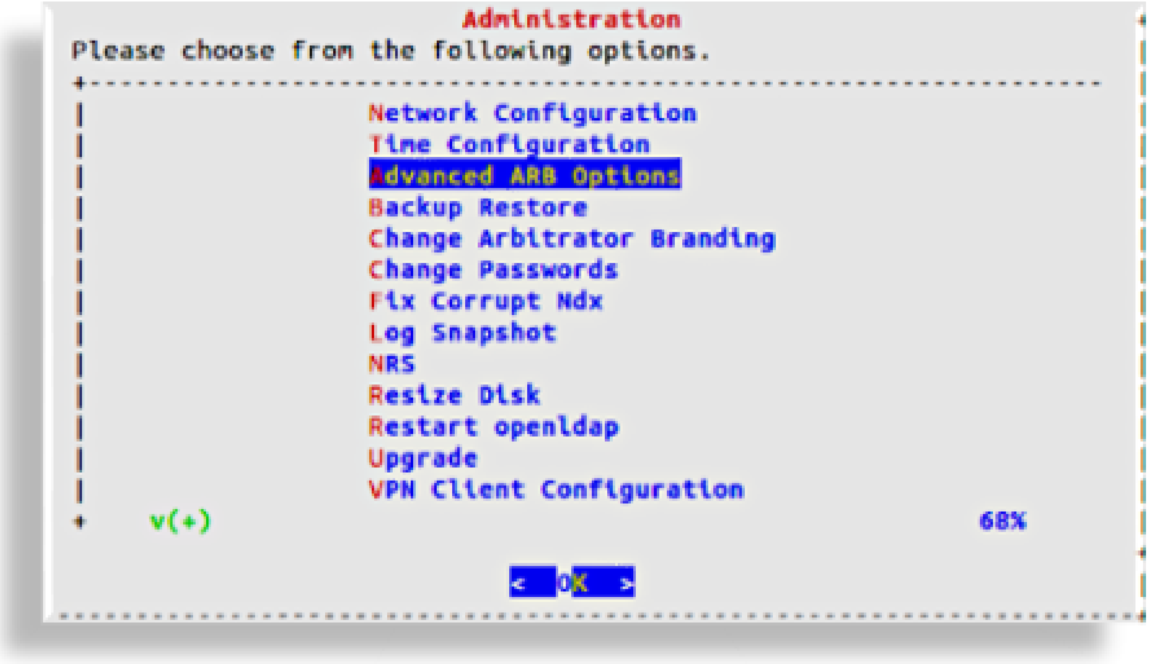
9.1. Customer Onboard

9.1.1. Add Customer CDR Folders

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

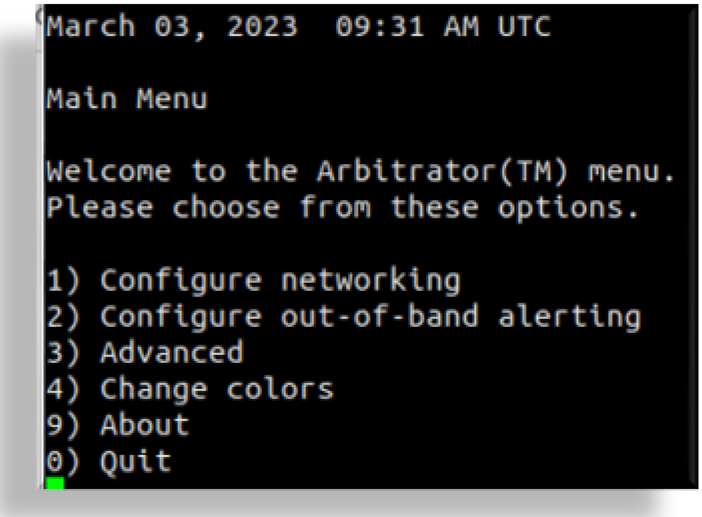
Note: The call manager IP address name serves as a CDR folder name for incoming CDRs. The steps in this procedure show the menus for the selected call manager to be configured.

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



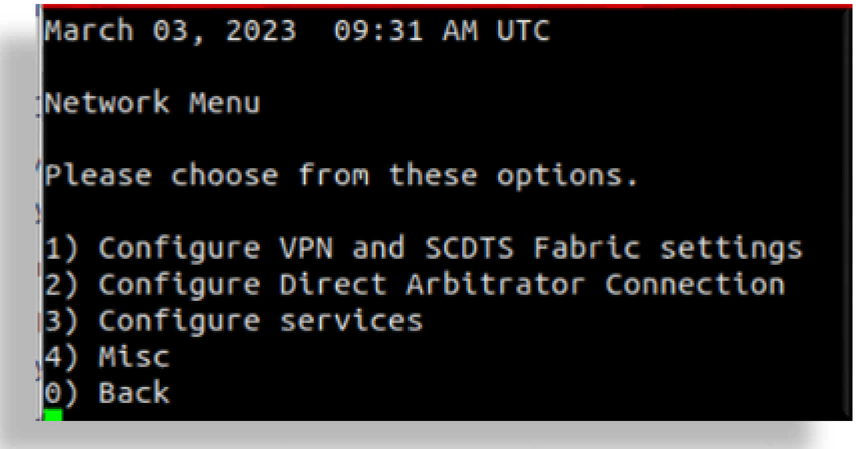
Please choose from the following options.

3. Select **Configure networking**



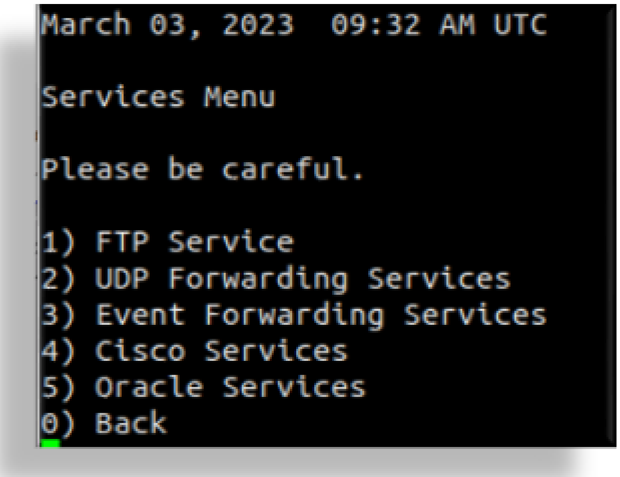
```
March 03, 2023  09:31 AM UTC

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
```

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



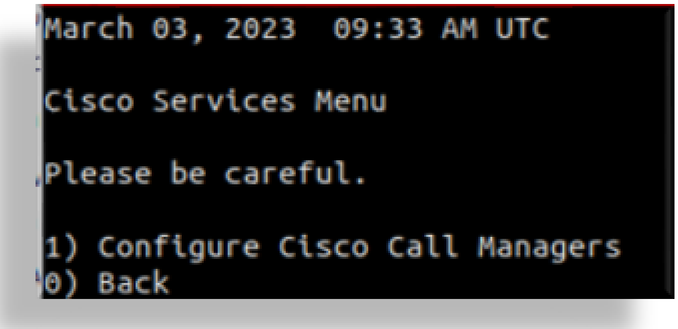
```
March 03, 2023  09:31 AM UTC

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
```

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

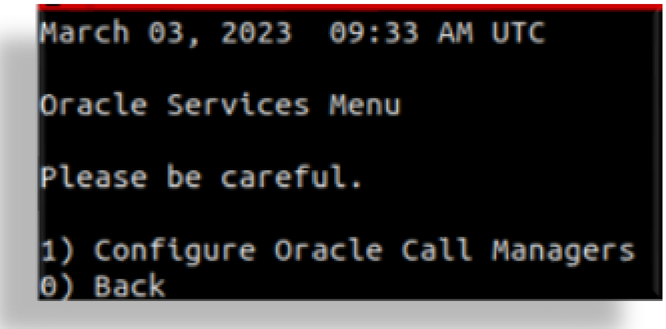


```
March 03, 2023  09:32 AM UTC

Services Menu

Please be careful.

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

6. Select the required call manager.

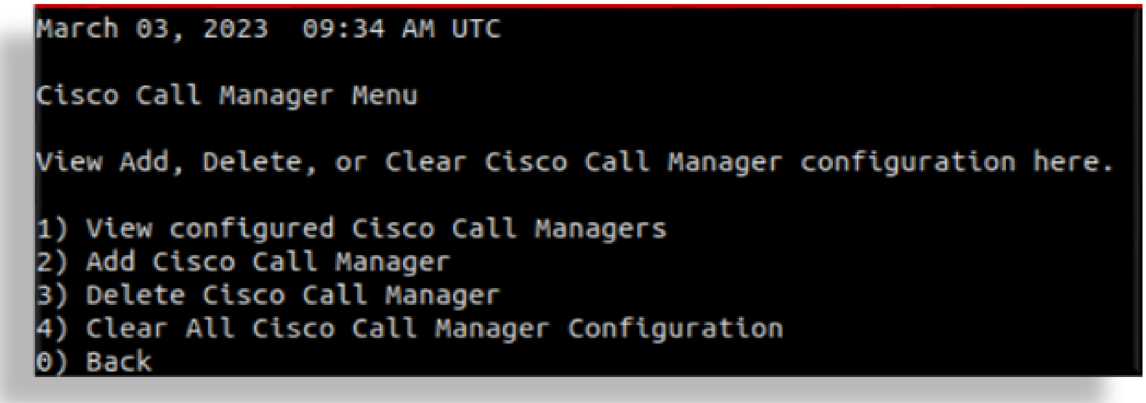


```
March 03, 2023  09:33 AM UTC

Cisco Services Menu

Please be careful.

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

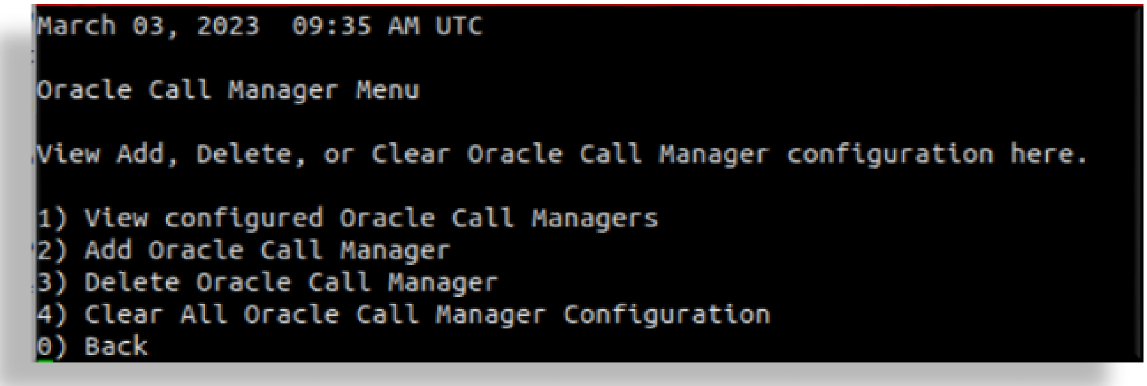


```
March 03, 2023  09:33 AM UTC

Oracle Services Menu

Please be careful.

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

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

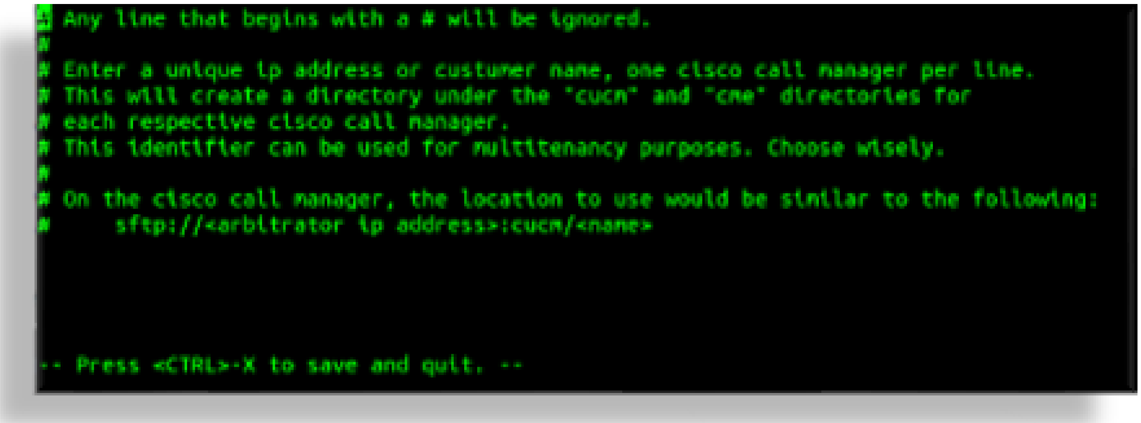


```
March 03, 2023  09:34 AM UTC

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
```

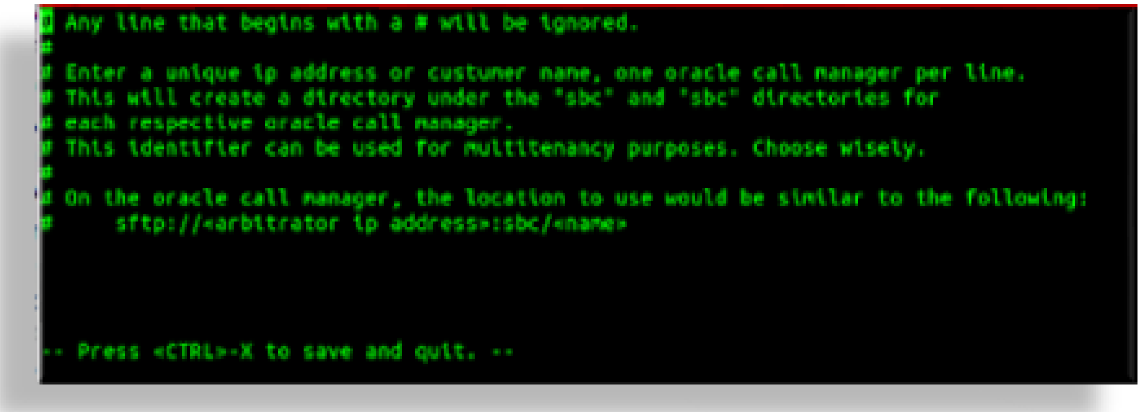


```
March 03, 2023  09:35 AM UTC

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 and quit.



```
# Any line that begins with a # will be ignored.
#
# Enter a unique ip address or custumer name, one cisco call manager per line.
# This will create a directory under the "cucm" 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>:cucm/<name>




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



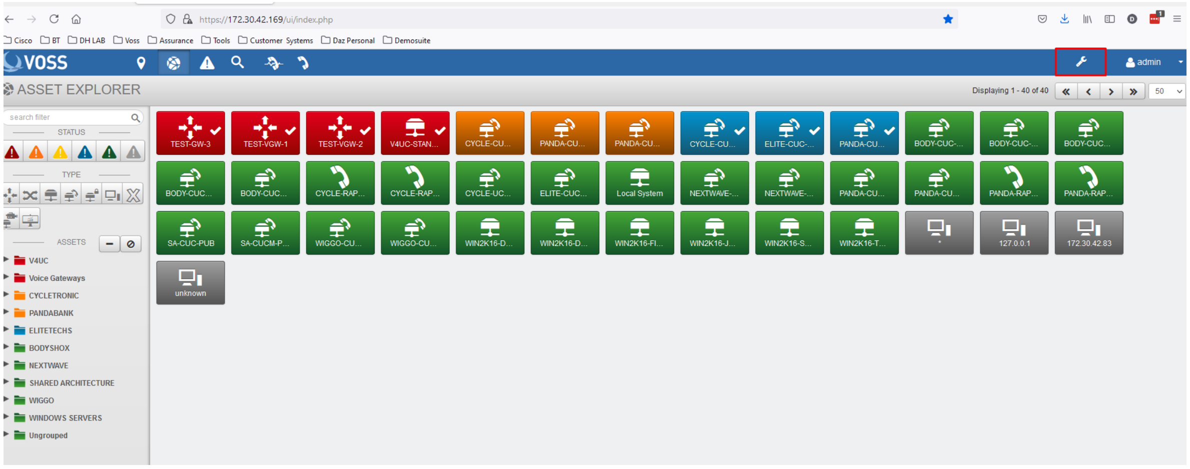
```
# Any line that begins with a # will be ignored.
#
# Enter a unique ip address or custumer name, one oracle call manager per line.
# This will create a directory under the "sbc" and "sbc" directories for
# each respective oracle call manager.
# This identifier can be used for multitenancy purposes. 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. --
```

Related Topics

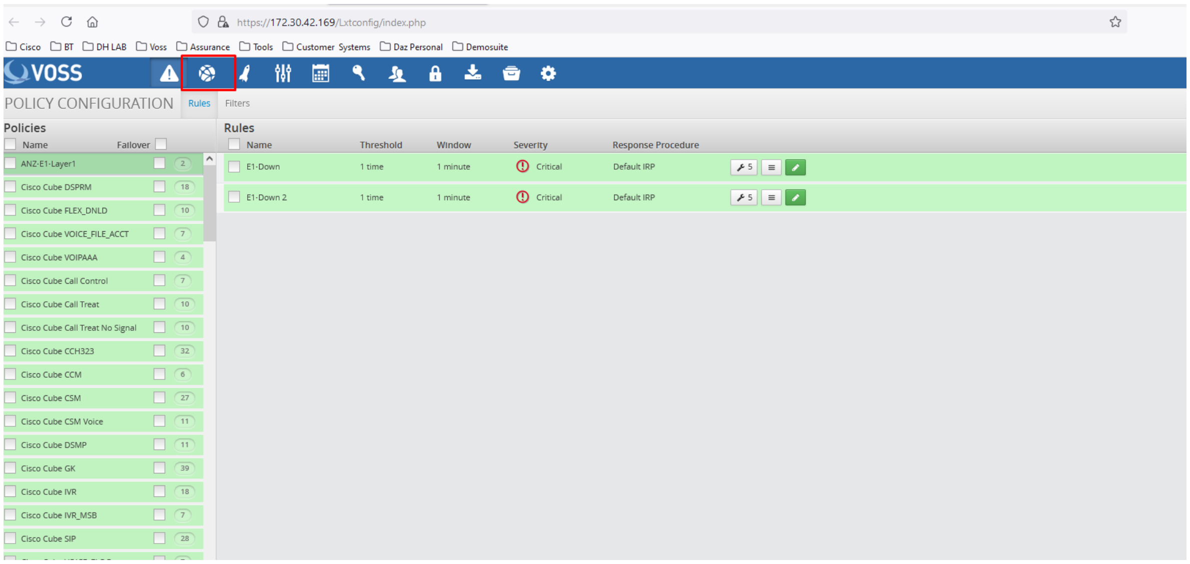
- For Collect setup in Arbitrator, see the "Configuration - Collect" topic in the Arbitrator Administration Guide.

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.



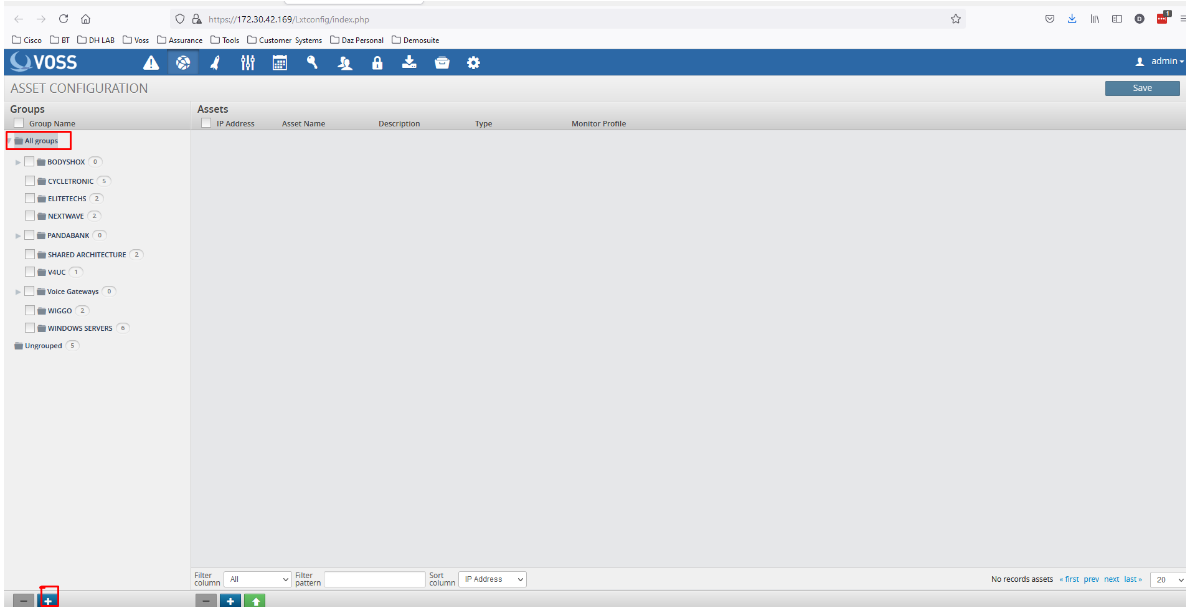
Policies

□ Name	Failover □	
□ ANZ-E1-Layer1	□	2
□ Cisco Cube DSPRM	□	18
□ Cisco Cube FLEX_DNLD	□	10
□ Cisco Cube VOICE_FILE_ACCT	□	7
□ Cisco Cube VOIPAAA	□	4
□ Cisco Cube Call Control	□	7
□ Cisco Cube Call Treat	□	10
□ Cisco Cube Call Treat No Signal	□	10
□ Cisco Cube CCH323	□	32
□ Cisco Cube CCM	□	6
□ Cisco Cube CSM	□	27
□ Cisco Cube CSM Voice	□	11
□ Cisco Cube DSMP	□	11
□ Cisco Cube GK	□	39
□ Cisco Cube IVR	□	18
□ Cisco Cube IVR_MSB	□	7
□ Cisco Cube SIP	□	28

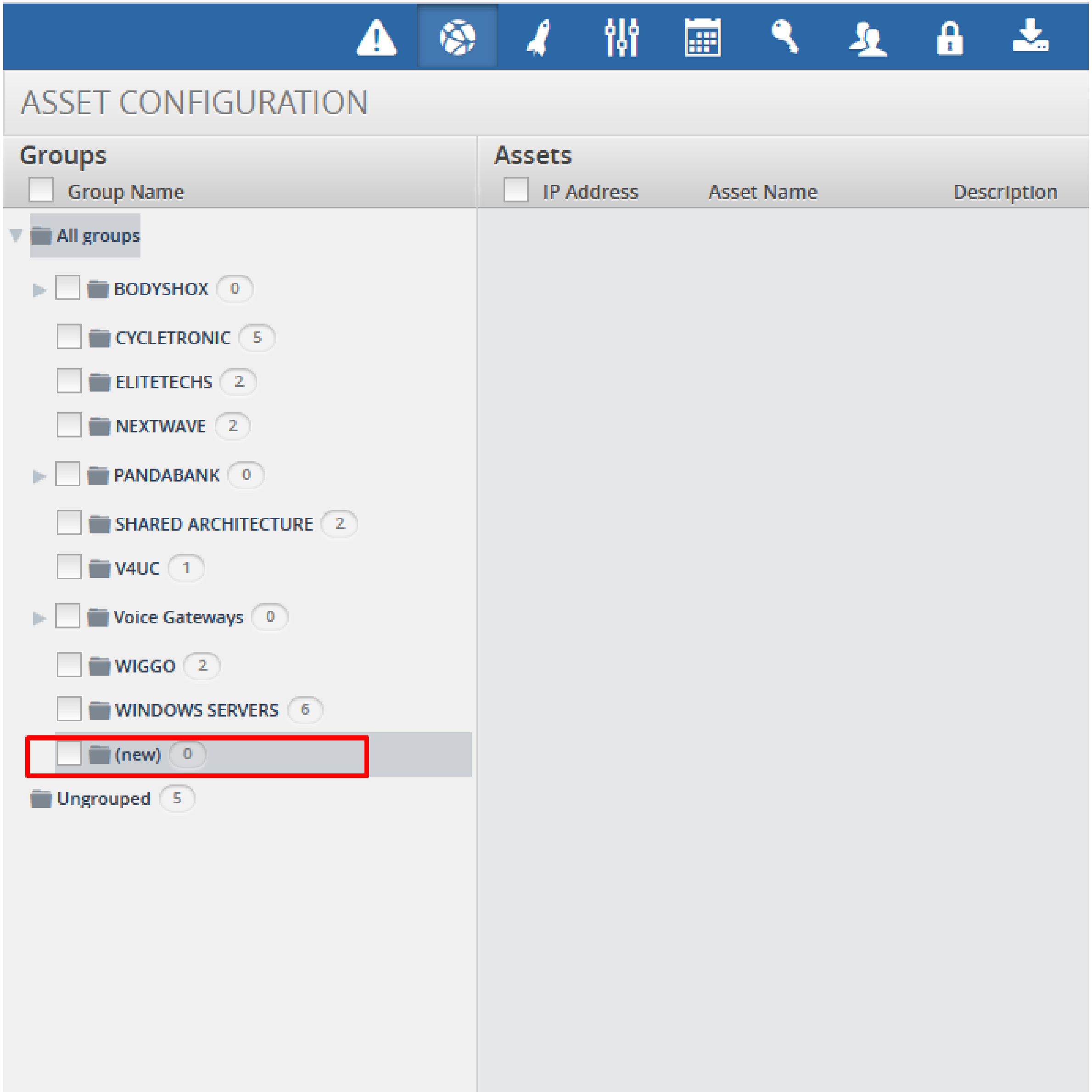
Rules

□ Name	Threshold	Window	Severity	Response Procedure
□ E1-Down	1 time	1 minute	Critical	Default IRP
□ E1-Down 2	1 time	1 minute	Critical	Default IRP

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

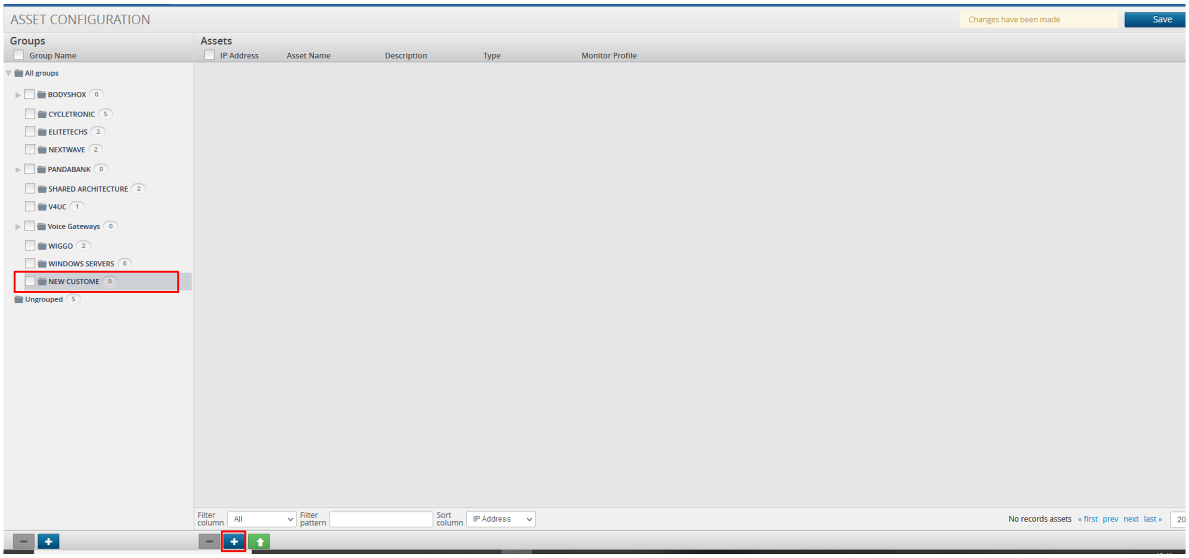


4. Select **All groups**, then select the Plus (+) icon to add a new folder.

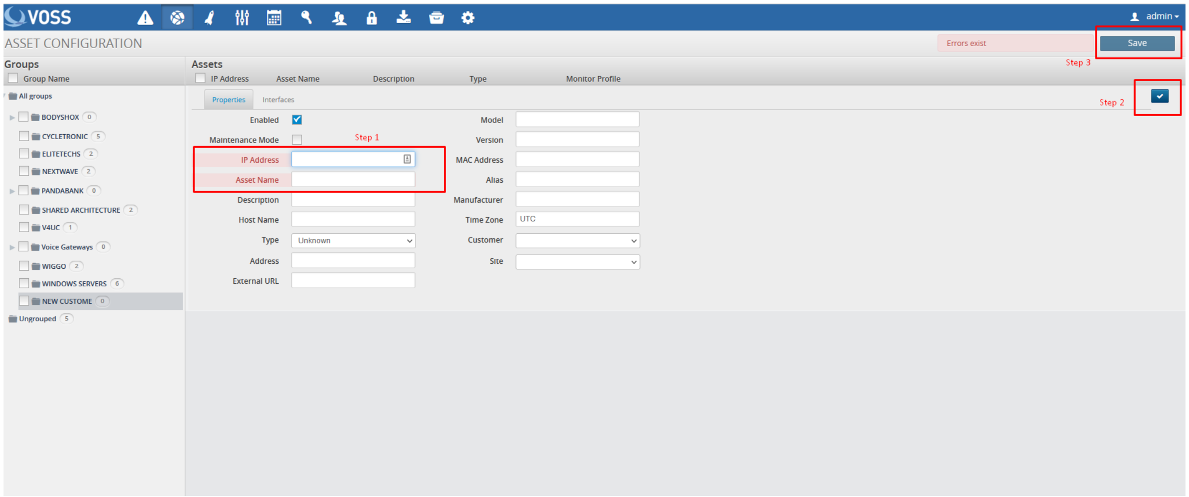


ASSET CONFIGURATION

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.



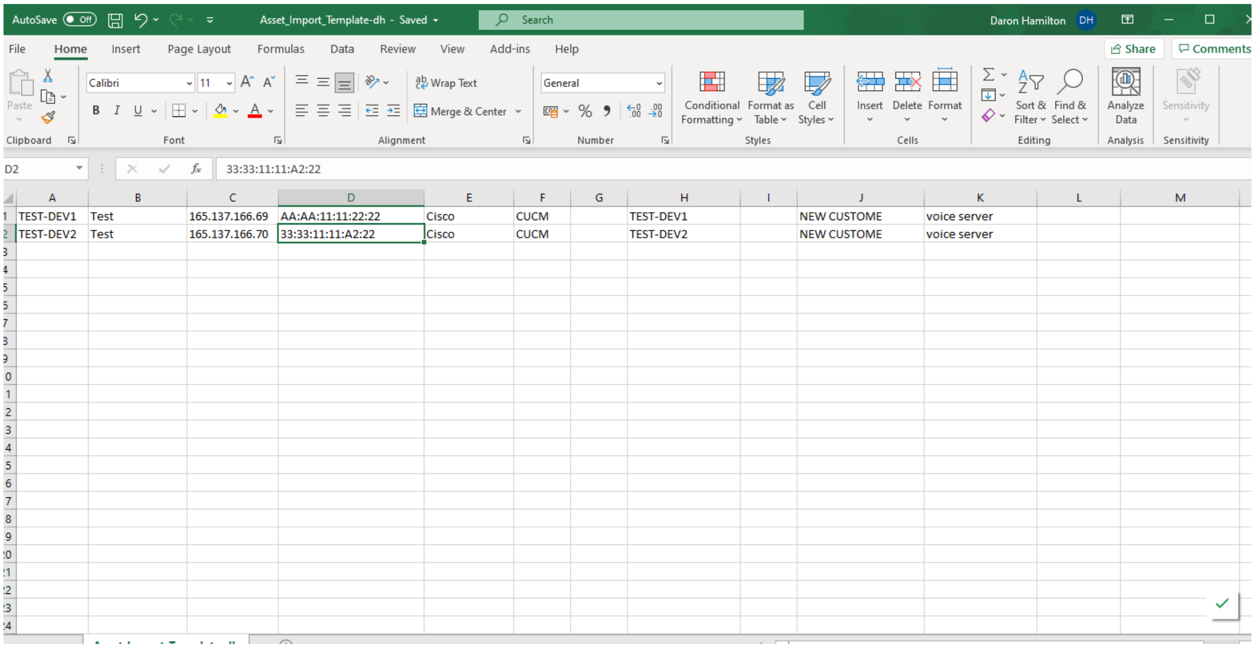
- Fill out the IP address (mandatory).
- Fill out the asset name (mandatory).
- Fill out any other information you have into the relevant fields.
- Click the Checkmark ✓.
- Click **Save**.

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.

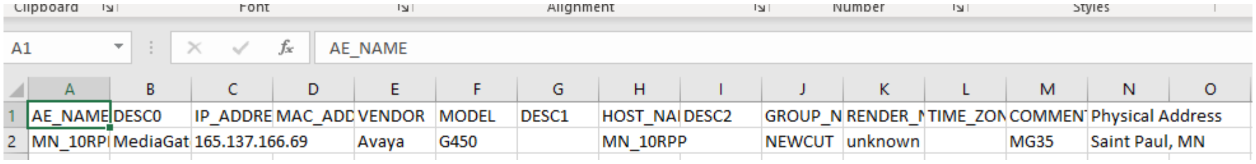
It is possible to upload multiple assets using a CSV file.



D2 | 33:33:11:11:A2:22

	A	B	C	D	E	F	G	H	I	J	K
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.



A1 | AE_NAME

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	AE_NAME	DESC0	IP_ADDRE	MAC_ADD	VENDOR	MODEL	DESC1	HOST_NA	DESC2	GROUP_N	RENDER_	TIME_ZON	COMMEN	Physical Address
2	MN_10RP	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
```

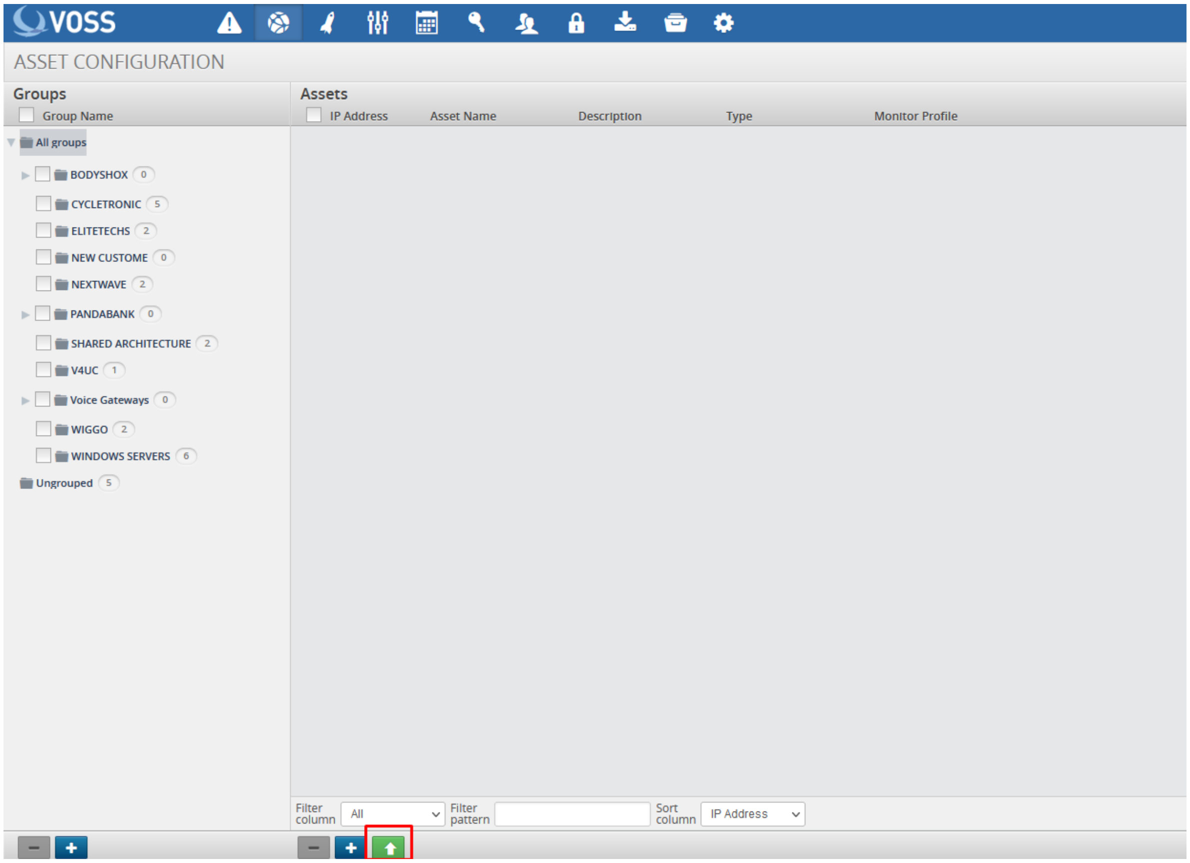
(continues on next page)

(continued from previous page)

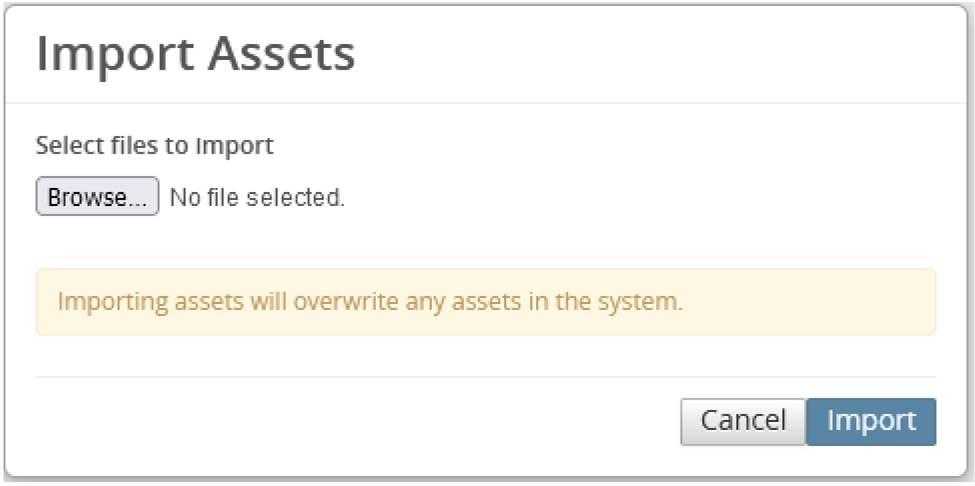
```
switch voice
server
voice server
server voice
workstation
phone
```

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.



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



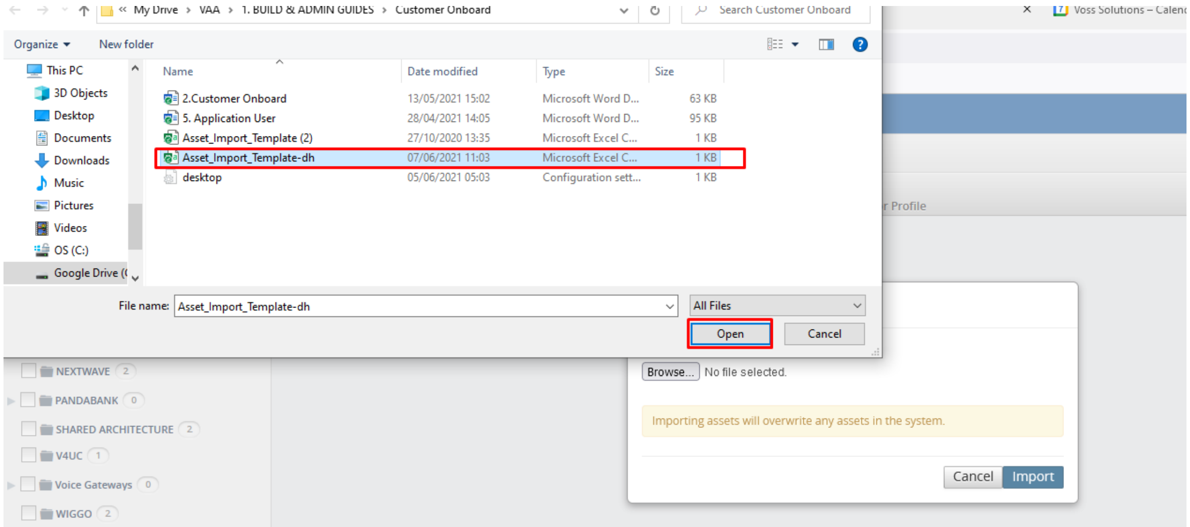
Import Assets

Select files to Import

No file selected.

Importing assets will overwrite any assets in the system.

5. Browse to your csv file.



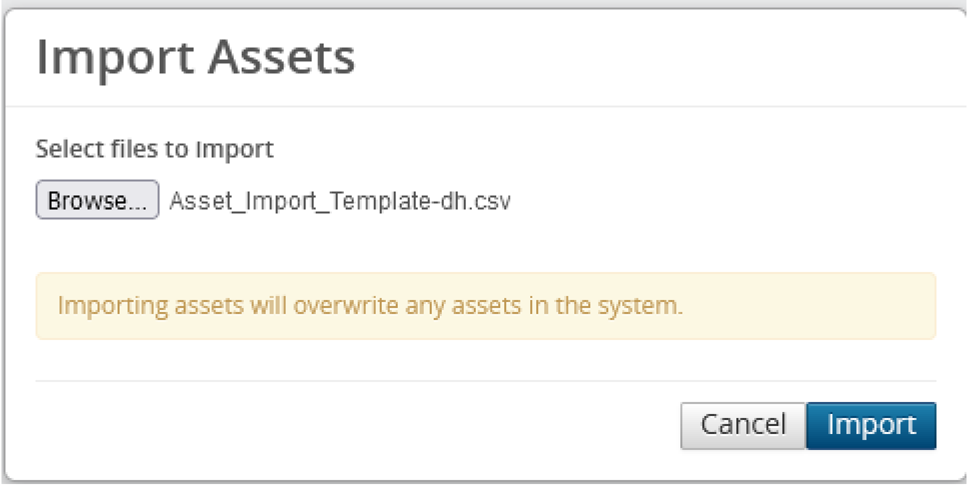
Name	Date modified	Type	Size
2.Customer Onboard	13/05/2021 15:02	Microsoft Word D...	63 KB
5. Application User	28/04/2021 14:05	Microsoft Word D...	95 KB
Asset_Import_Template (2)	27/10/2020 13:35	Microsoft Excel C...	1 KB
Asset_Import_Template-dh	07/06/2021 11:03	Microsoft Excel C...	1 KB
desktop	05/06/2021 05:03	Configuration sett...	1 KB

File name: Asset_Import_Template-dh

No file selected.

Importing assets will overwrite any assets in the system.

6. Click **Open**.



Import Assets

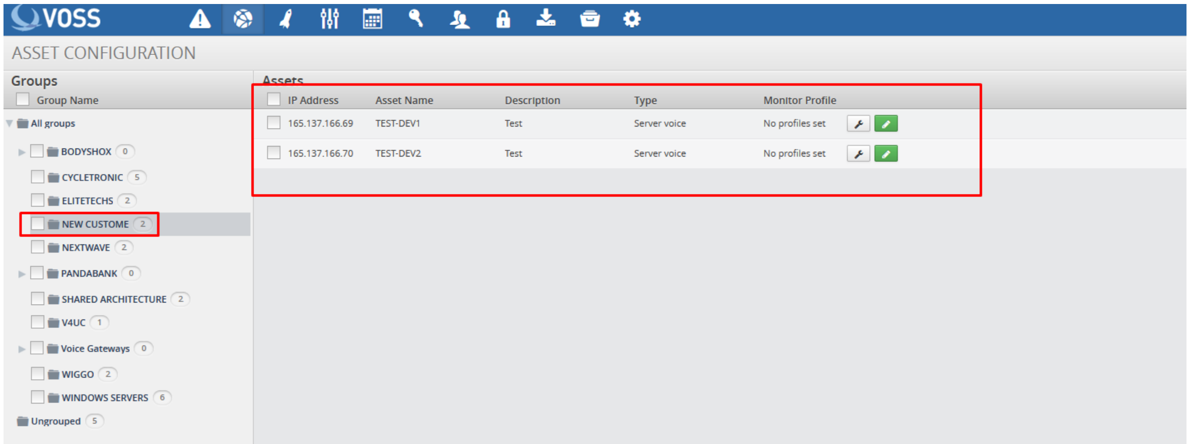
Select files to Import

Asset_Import_Template-dh.csv

Importing assets will overwrite any assets in the system.

7. Click **Import**

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



ASSET CONFIGURATION

Groups

Group Name
All groups
BODYSHOX 0
CYCLETRONIC 5
ELITETECHS 2
NEW CUSTOME 2
NEXTWAVE 2
PANDABANK 0
SHARED ARCHITECTURE 2
V4UC 1
Voice Gateways 0
WIGGO 2
WINDOWS SERVERS 6
Ungrouped 5

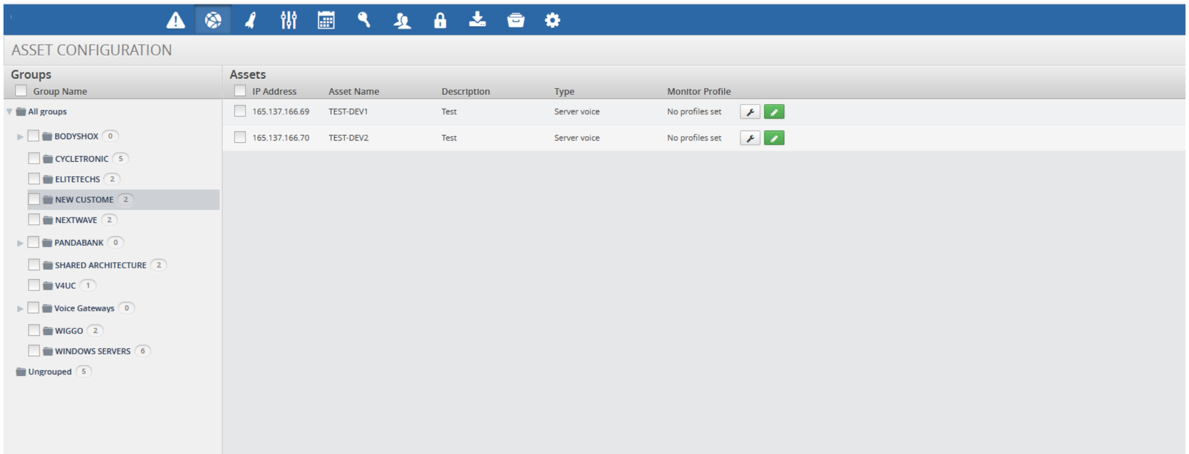
Assets

IP Address	Asset Name	Description	Type	Monitor Profile
165.137.166.69	TEST-DEV1	Test	Server voice	No profiles set
165.137.166.70	TEST-DEV2	Test	Server voice	No profiles set

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



ASSET CONFIGURATION

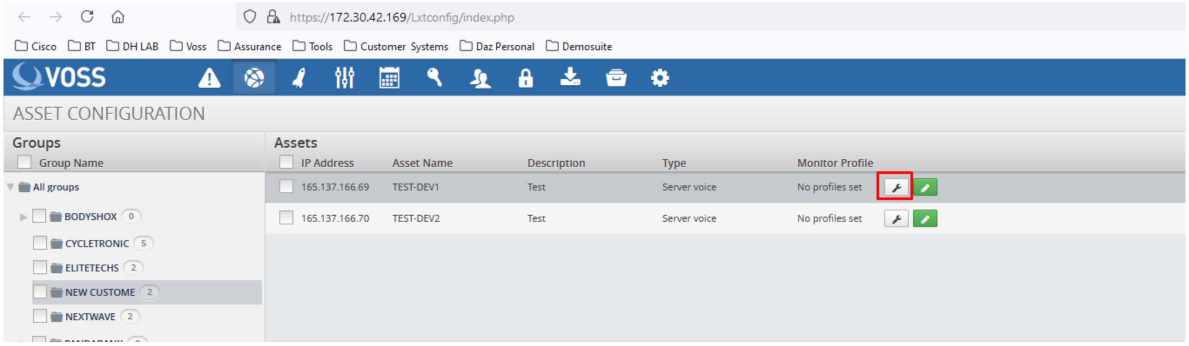
Groups

Group Name
All groups
BODYSHOX 0
CYCLETRONIC 5
ELITETECHS 2
NEW CUSTOME 2
NEXTWAVE 2
PANDABANK 0
SHARED ARCHITECTURE 2
V4UC 1
Voice Gateways 0
WIGGO 2
WINDOWS SERVERS 6
Ungrouped 5

Assets

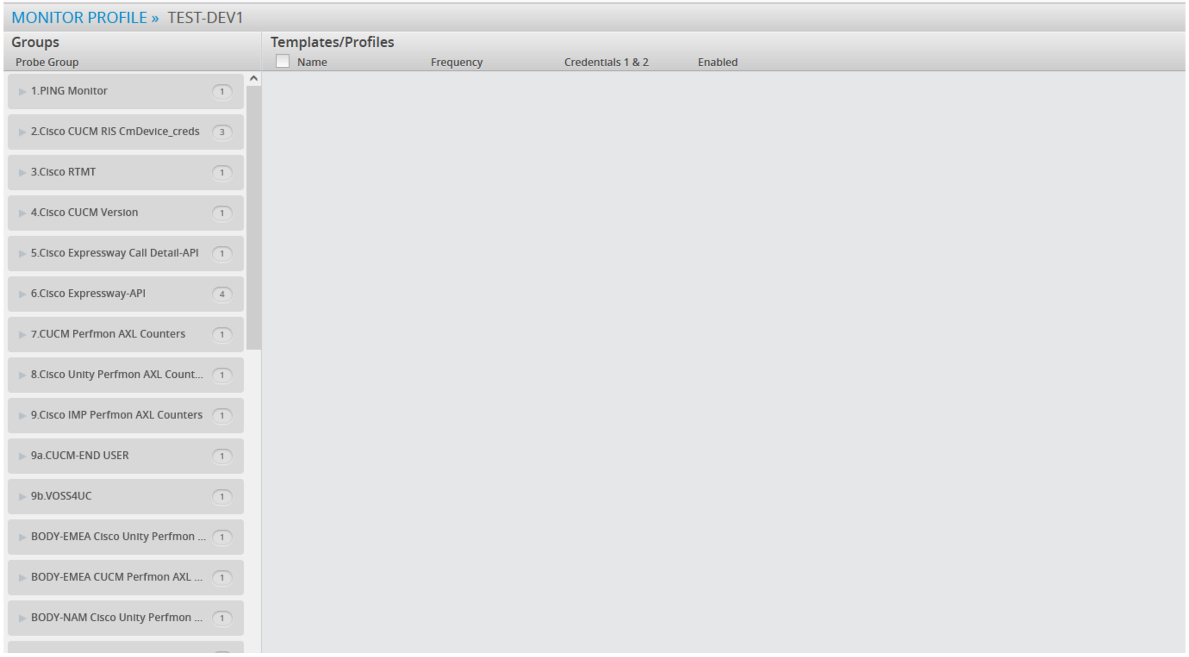
IP Address	Asset Name	Description	Type	Monitor Profile
165.137.166.69	TEST-DEV1	Test	Server voice	No profiles set
165.137.166.70	TEST-DEV2	Test	Server voice	No profiles set

5. Click on the wrench icon as shown below.

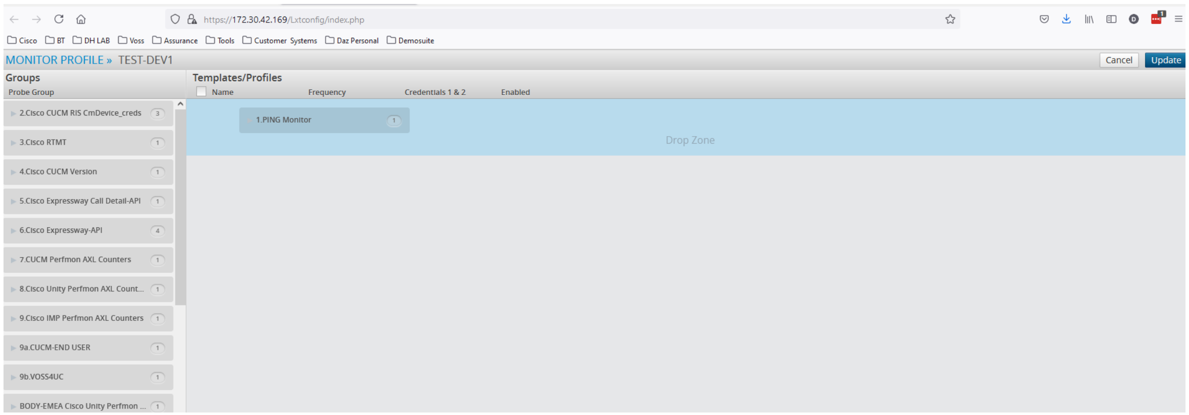


IP Address	Asset Name	Description	Type	Monitor Profile
165.137.166.69	TEST-DEV1	Test	Server voice	No profiles set
165.137.166.70	TEST-DEV2	Test	Server voice	No profiles set

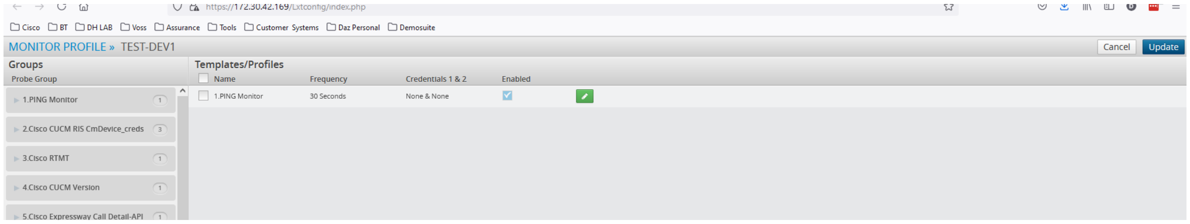
This will then open the Assignment screen.


MONITOR PROFILE » TEST-DEV1
Groups
Probe Group
1.PING Monitor 1
2.Cisco CUCM RIS CmDevice_creds 3
3.Cisco RTMT 1
4.Cisco CUCM Version 1
5.Cisco Expressway Call Detail-API 1
6.Cisco Expressway-API 4
7.CUCM Perfmon AXL Counters 1
8.Cisco Unity Perfmon AXL Count... 1
9.Cisco IMP Perfmon AXL Counters 1
9a.CUCM-END USER 1
9b.VOSS4UC 1
BODY-EMEA Cisco Unity Perfmon ... 1
BODY-EMEA CUCM Perfmon AXL ... 1
BODY-NAM Cisco Unity Perfmon ... 1
Templates/Profiles
Name
Frequency
Credentials 1 & 2
Enabled

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


https://172.30.42.169/Lxtconfig/index.php
Cisco
BT
DH LAB
Voss
Assurance
Tools
Customer Systems
Daz Personal
Demosuite
MONITOR PROFILE » TEST-DEV1
Cancel
Update
Groups
Probe Group
2.Cisco CUCM RIS CmDevice_creds 3
3.Cisco RTMT 1
4.Cisco CUCM Version 1
5.Cisco Expressway Call Detail-API 1
6.Cisco Expressway-API 4
7.CUCM Perfmon AXL Counters 1
8.Cisco Unity Perfmon AXL Count... 1
9.Cisco IMP Perfmon AXL Counters 1
9a.CUCM-END USER 1
9b.VOSS4UC 1
BODY-EMEA Cisco Unity Perfmon ... 1
Templates/Profiles
Name
Frequency
Credentials 1 & 2
Enabled
1.PING Monitor 1
Drop Zone

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



MONITOR PROFILE » TEST-DEV1

Groups

Probe Group	
1.PING Monitor	1
2.Cisco CUCM RIS CmDevice_creds	3
3.Cisco RTMT	1
4.Cisco CUCM Version	1
5.Cisco Expressway Call Detail-API	1

Templates/Profiles

□	Name	Frequency	Credentials 1 & 2	Enabled	
□	1.PING Monitor	30 Seconds	None & None	☑	✎

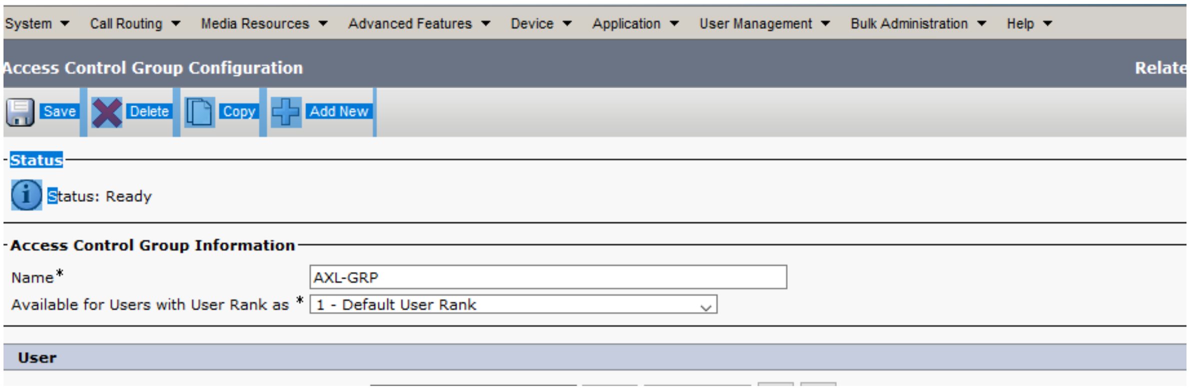
8. If you then click on ✎ you can set any time schedules / credentials required for this probe
9. Once finished click **Update** and then click **Save**.

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.



Access Control Group Configuration

Status

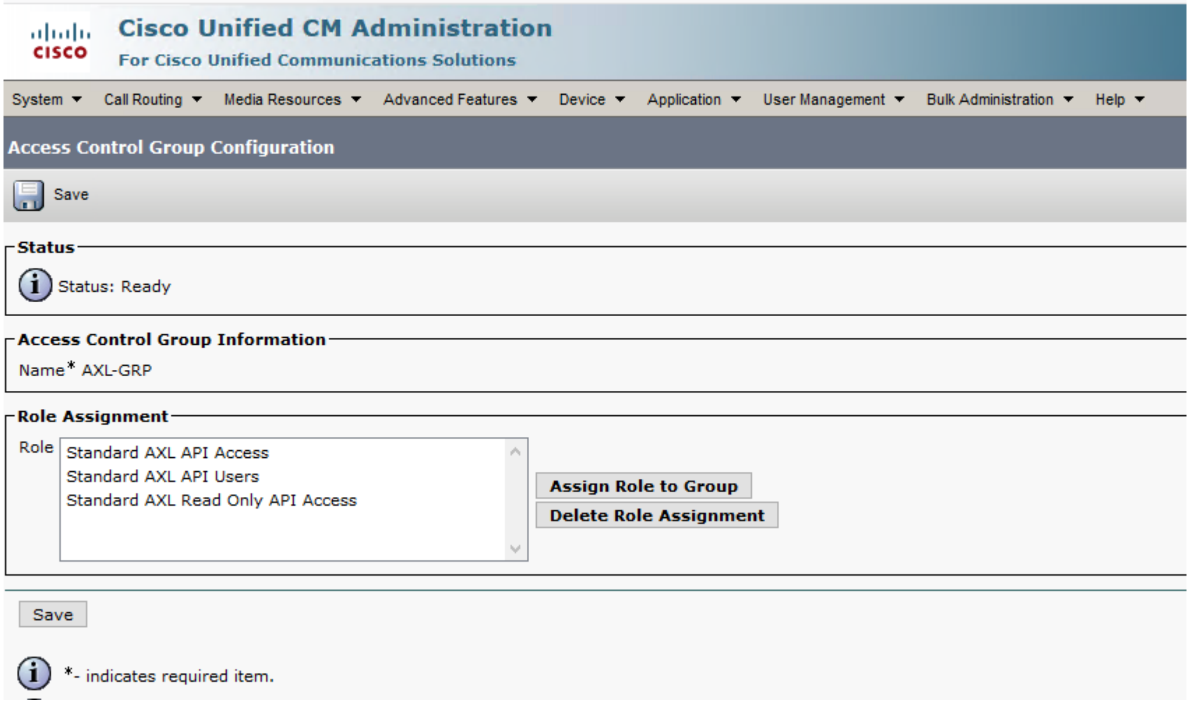
Status: Ready

Access Control Group Information

Name* AXL-GRP

Available for Users with User Rank as * 1 - Default User Rank

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 ▾
Save
Assign Role to Group
Delete Role Assignment
Save

Access Control Group Configuration

Status

Status: Ready

Access Control Group Information

Name* AXL-GRP

Role Assignment

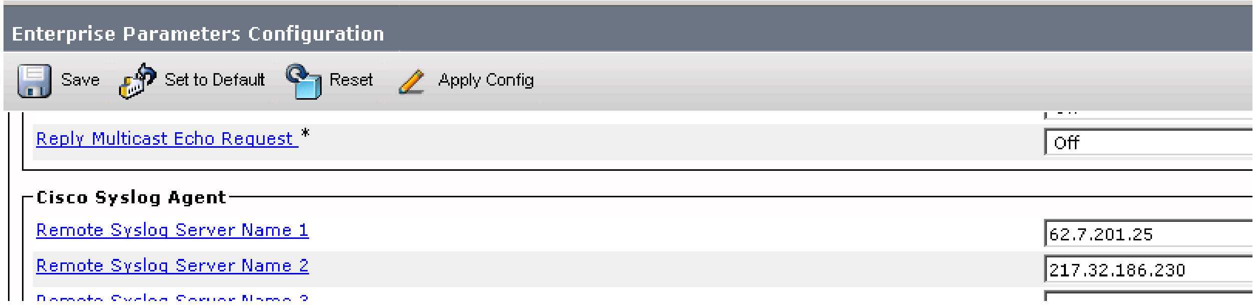
Role: Standard AXL API Access, Standard AXL API Users, Standard AXL Read Only API Access

*- 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

Reply Multicast Echo Request * Off

Cisco Syslog Agent

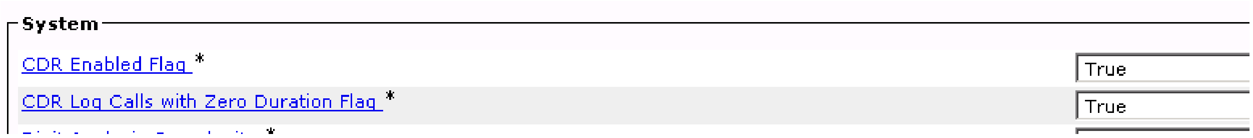
Remote Syslog Server Name 1 62.7.201.25

Remote Syslog Server Name 2 217.32.186.230

CUCM Service Parameters

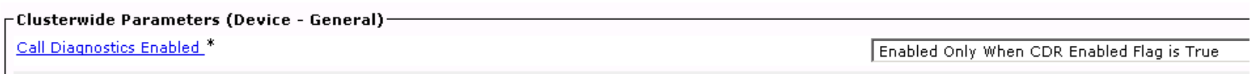
Ensure CDR Service Parameters are set:

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



System

CDR Enabled Flag *	True
CDR Log Calls with Zero Duration Flag *	True

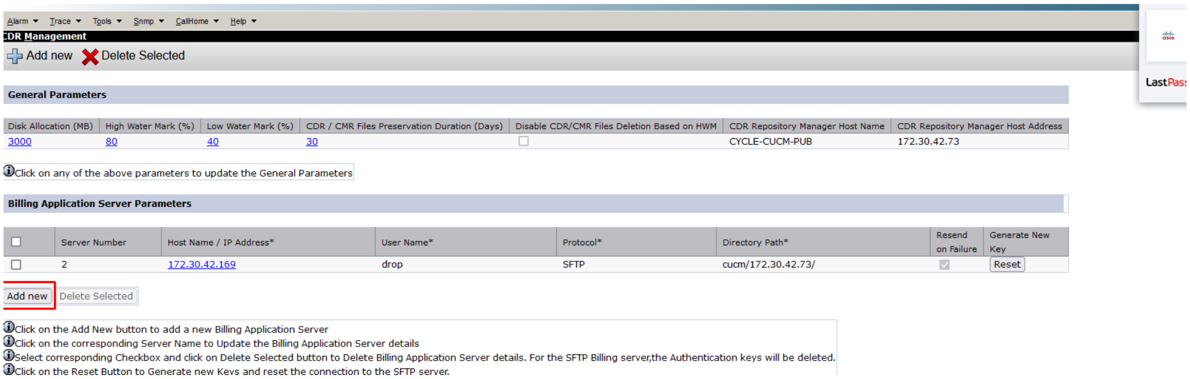


Clusterwide Parameters (Device - General)

Call Diagnostics Enabled *	Enabled Only When CDR Enabled Flag is True

CUCM Serviceability

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



CDR Management

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	□	CYCLE-CUCM-PUB	172.30.42.73

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

Billing Application Server Parameters

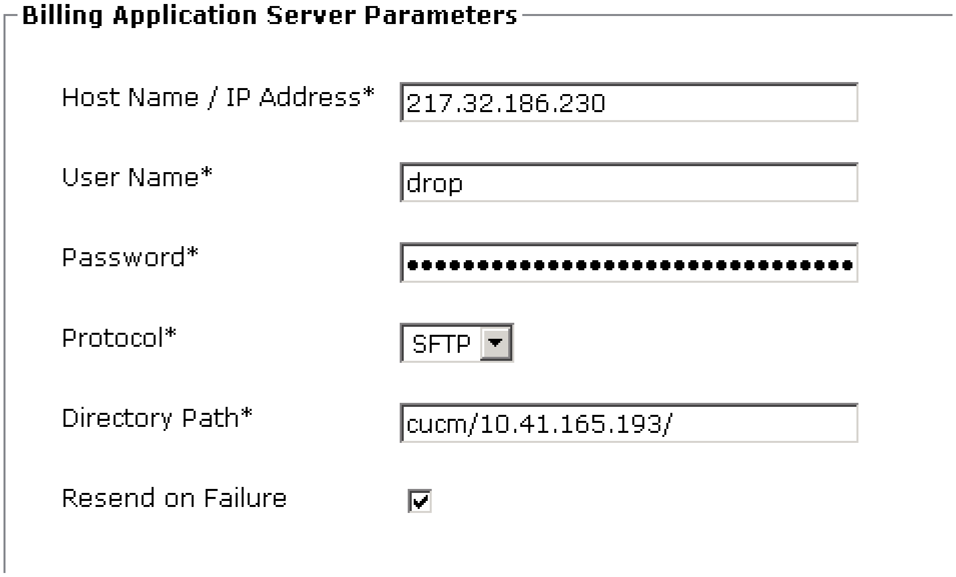
□	Server Number	Host Name / IP Address*	User Name*	Protocol*	Directory Path*	Resend on Failure	Generate New Key
□	2	172.30.42.169	drop	SFTP	cucm/172.30.42.73/	☑	Reset

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 Kevs 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.

     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



Billing Application Server Parameters

Host Name / IP Address*	217.32.186.230
User Name*	drop
Password*	••••••••••••••••••••••••••••••••••
Protocol*	SFTP
Directory Path*	cucm/10.41.165.193/
Resend on Failure	☑

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:

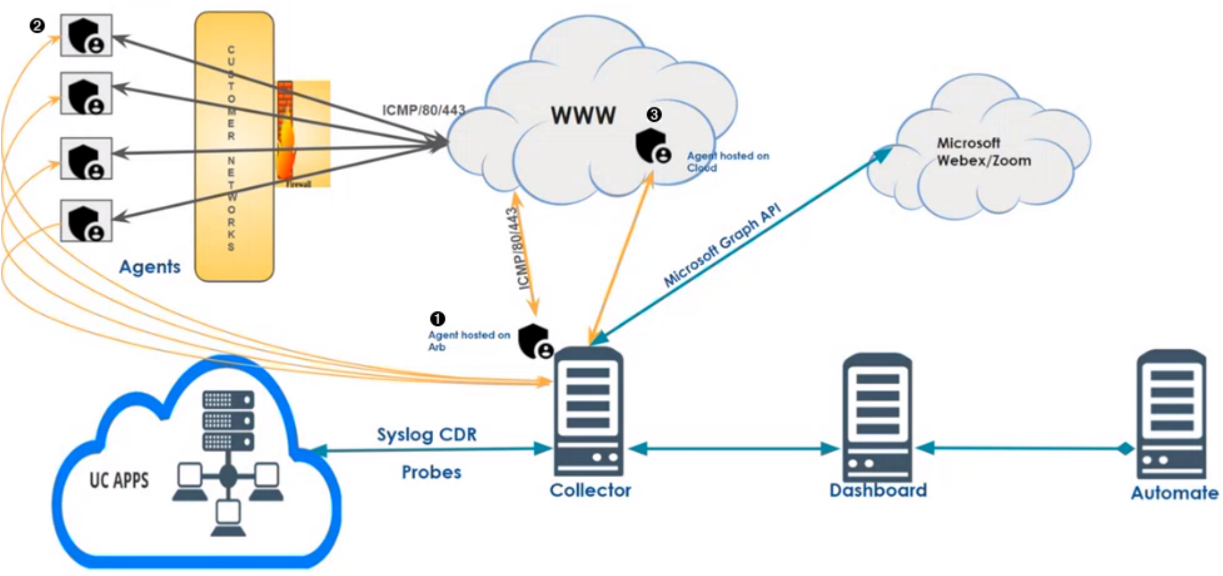
- Measure hops
- Measure latency
- Measure web performance
- Provide alarms on for example: too many hops, latency, bad response

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.

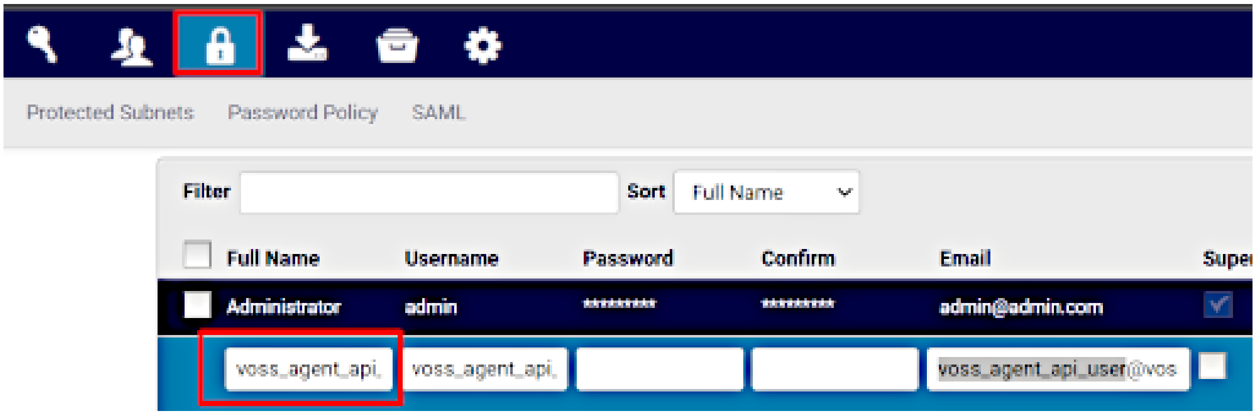
The recommended tests require the following connectivity if you intend to use them. Additional/alternate connectivity may be required if other tests are intended to be used.

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`



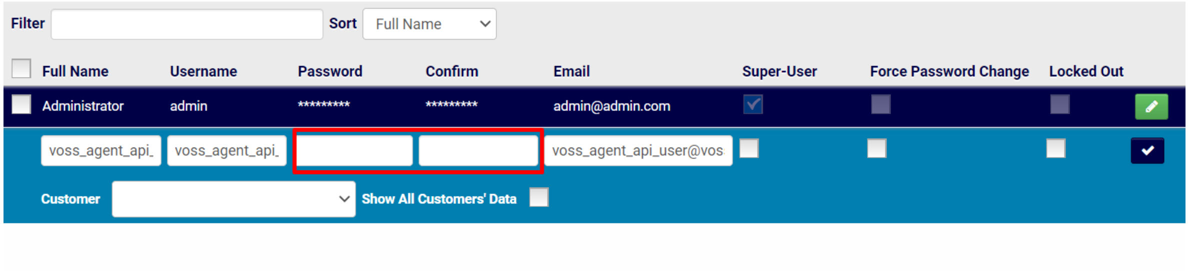
Filter Sort Full Name

□	Full Name	Username	Password	Confirm	Email	Supe
□	Administrator	admin	*********	*********	admin@admin.com	☑
	voss_agent_api	voss_agent_api			voss_agent_api_user@vos	□

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** Users.
3. Click on the green pencil ✎ to modify.
4. Set the password.



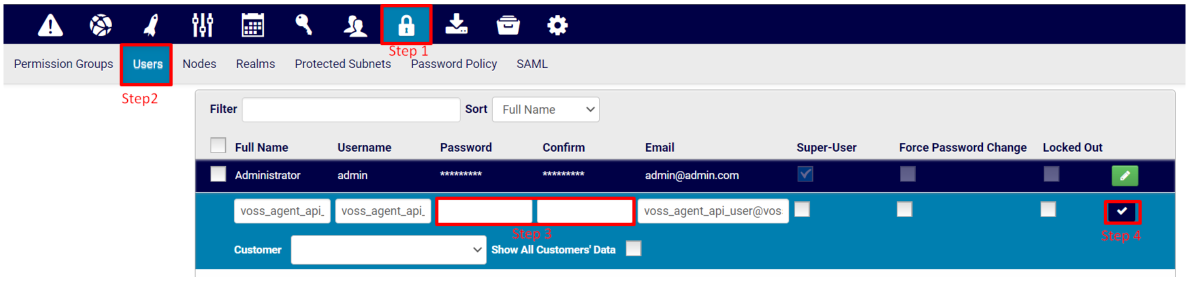
Filter Sort Full Name

□	Full Name	Username	Password	Confirm	Email	Super-User	Force Password Change	Locked Out	
□	Administrator	admin	*********	*********	admin@admin.com	☑	□	□	✎
	voss_agent_api_	voss_agent_api_			voss_agent_api_user@vos	□	□	□	✔

Customer Show All Customers' Data □

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.



Filter Sort Full Name

□	Full Name	Username	Password	Confirm	Email	Super-User	Force Password Change	Locked Out	
□	Administrator	admin	*********	*********	admin@admin.com	☑	□	□	✎
	voss_agent_api_	voss_agent_api_			voss_agent_api_user@vos	□	□	□	✔

Customer Show All Customers' Data □

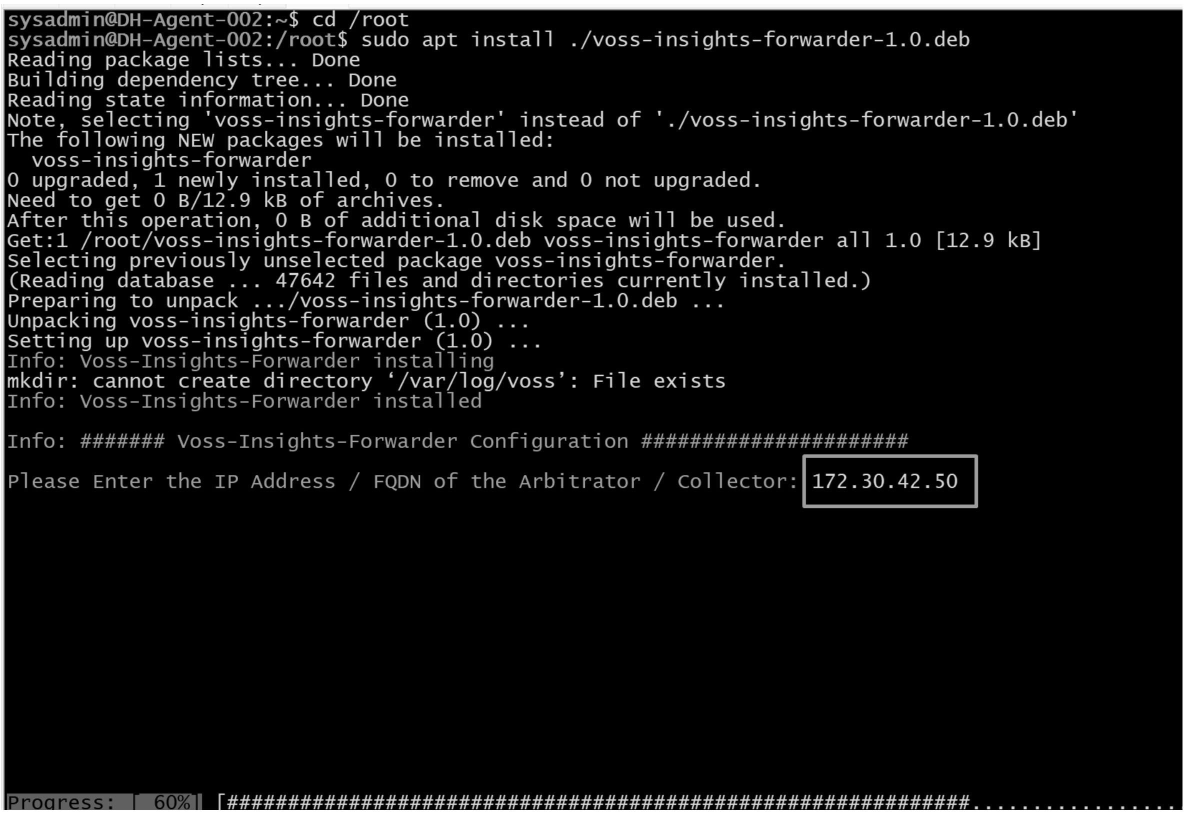
Agent Installation

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`

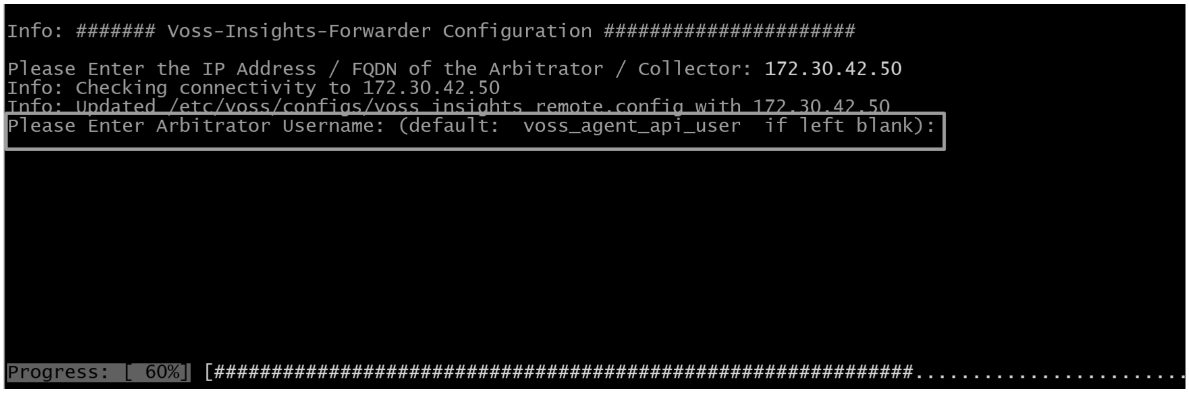
1. At the host prompt, run: `sudo apt install ./voss-insights-forwarder-1.0.deb`

   ```
   sysadmin@DH-Agent-002:~$ cd /root
   sysadmin@DH-Agent-002:/root$ sudo apt install ./voss-insights-forwarder-1.0.deb
   Reading package lists... Done
   Building dependency tree... Done
   Reading state information... Done
   Note, selecting 'voss-insights-forwarder' instead of './voss-insights-forwarder-1.0.deb'
   The following NEW packages will be installed:
     voss-insights-forwarder
   0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
   Need to get 0 B/12.9 kB of archives.
   After this operation, 0 B of additional disk space will be used.
   Get:1 /root/voss-insights-forwarder-1.0.deb voss-insights-forwarder all 1.0 [12.9 kB]
   Selecting previously unselected package voss-insights-forwarder.
   (Reading database ... 47642 files and directories currently installed.)
   Preparing to unpack .../voss-insights-forwarder-1.0.deb ...
   Unpacking voss-insights-forwarder (1.0) ...
   Setting up voss-insights-forwarder (1.0) ...
   Info: Voss-Insights-Forwarder installing
   mkdir: cannot create directory ‘/var/log/voss’: File exists
   Info: Voss-Insights-Forwarder installed

   Info: ####### Voss-Insights-Forwarder Configuration ######################

   Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50









   Progress: [ 60%] [##############################################################.................
   ```

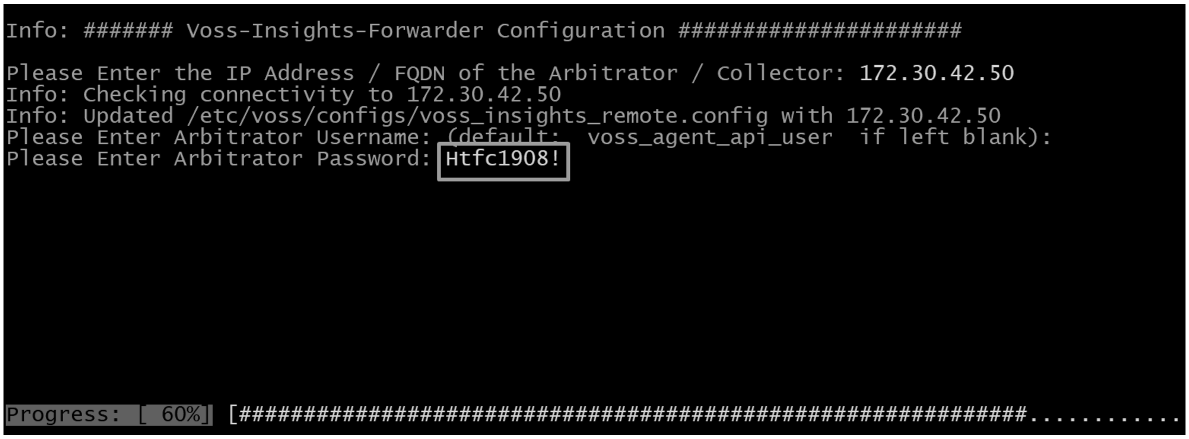
2. Enter the IP Address or FQDN of the Arbitrator that the agent is to report to then press Enter. The agent will now do a connectivity check via ICMP (Ping) to the Arbitrator.

   - If connectivity is good, move on to the next step.
   - If there is no connectivity after 4 attempts, the package will exit.

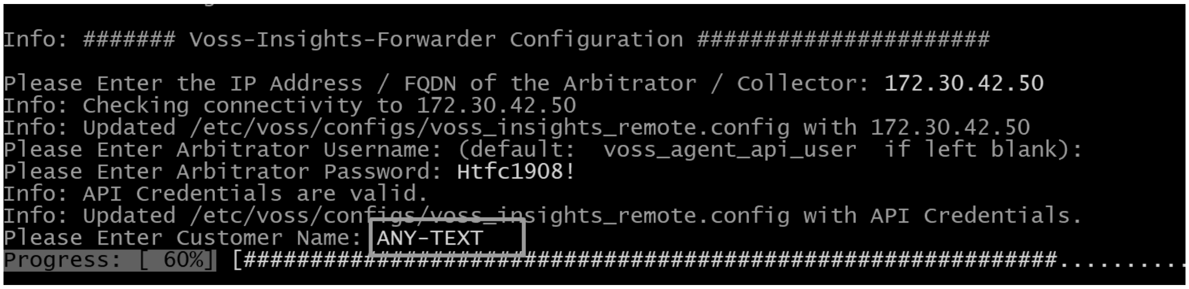
   ```
   Info: ####### Voss-Insights-Forwarder Configuration ######################

   Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
   Info: Checking connectivity to 172.30.42.50
   Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
   Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):






   Progress: [ 60%] [##############################################################........................
   ```

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



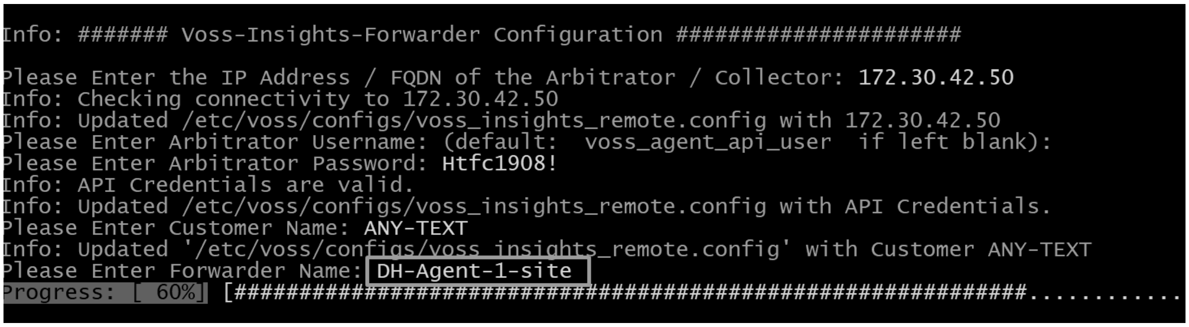
```
Info: ####### Voss-Insights-Forwarder Configuration #####################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
Info: Checking connectivity to 172.30.42.50
Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):
Please Enter Arbitrator Password: Htfc1908!








Progress: [ 60%] [#############################################################............
```

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.



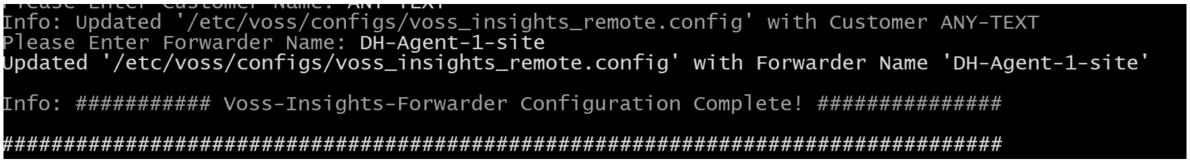
```
Info: ####### Voss-Insights-Forwarder Configuration #####################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
Info: Checking connectivity to 172.30.42.50
Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):
Please Enter Arbitrator Password: Htfc1908!
Info: API Credentials are valid.
Info: Updated /etc/voss/configs/voss_insights_remote.config with API Credentials.
Please Enter Customer Name: ANY-TEXT
Progress: [ 60%] [#############################################################.........
```

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



```
Info: ####### Voss-Insights-Forwarder Configuration #####################

Please Enter the IP Address / FQDN of the Arbitrator / Collector: 172.30.42.50
Info: Checking connectivity to 172.30.42.50
Info: Updated /etc/voss/configs/voss_insights_remote.config with 172.30.42.50
Please Enter Arbitrator Username: (default:  voss_agent_api_user  if left blank):
Please Enter Arbitrator Password: Htfc1908!
Info: API Credentials are valid.
Info: Updated /etc/voss/configs/voss_insights_remote.config with API Credentials.
Please Enter Customer Name: ANY-TEXT
Info: Updated '/etc/voss/configs/voss_insights_remote.config' with Customer ANY-TEXT
Please Enter Forwarder Name: DH-Agent-1-site
Progress: [ 60%] [#############################################################............
```

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



```
Please Enter Customer Name: ANY-TEXT
Info: Updated '/etc/voss/configs/voss_insights_remote.config' with Customer ANY-TEXT
Please Enter Forwarder Name: DH-Agent-1-site
Updated '/etc/voss/configs/voss_insights_remote.config' with Forwarder Name 'DH-Agent-1-site'

Info: ########### Voss-Insights-Forwarder Configuration Complete! ###############

#################################################################################
```

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