



VOSS Insights Install Guide

Release 22.1

Jun 02, 2022

Legal Information

Please take careful note of the following legal notices:

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

Security Information

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

DOCUMENT ID: 20220602123531

Contents

- 1 VMWare Specification and Requirements 1**
 - 1.1 Dashboard Reporting VM Sizing Specifications 1
 - 1.2 Arbitrator VM Sizing Specifications 2
 - 1.3 Arbitrator Correlation Consolidation VM Sizing Specifications 3
 - 1.4 DS-9 Netflow VM Sizing Specifications 3
 - 1.5 Raptor Call Path Generation VM Sizing Specifications 6

- 2 Port Requirements 7**
 - 2.1 Correlation and Dashboard System Connectivity 7
 - 2.2 Cisco UC Monitoring System Connectivity 7
 - 2.3 MS Teams System Connectivity 8
 - 2.4 Netflow and DS9 Monitoring System Connectivity 8
 - 2.5 VOSS Automate Port Usage 9
 - 2.6 Skype for Business Monitoring System Connectivity 10
 - 2.7 Avaya Call Manager Connectivity 11

- 3 Deploy and Networking Setup 12**
 - 3.1 Deploy and VM Installation Steps 12

- 4 Database and System Setup 16**
 - 4.1 VOSS Automate Database Setup 16
 - 4.2 Install Arbitrator System 19
 - 4.3 Set up Arbitrator to Arbitrator Communication 22
 - 4.4 Install Dashboard System 25

- 5 Certificates 28**
 - 5.1 Add Certificates 28

- 6 CUCM Asset Onboarding 29**
 - 6.1 Customer Onboard 29
 - 6.2 Call Manager Configuration 41

1. VMWare Specification and Requirements

1.1. Dashboard Reporting VM Sizing Specifications

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

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

1.2. Arbitrator VM Sizing Specifications

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

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

Scalability questions to consider:

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

Notes:

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

1.3. Arbitrator Correlation Consolidation VM Sizing Specifications

Arbitrator Correlation Consolidation recommended option:

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

Scalability questions to consider:

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

Notes:

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

1.4. DS-9 Netflow VM Sizing Specifications

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.

1.4.1. 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	

1.4.2. 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	

1.4.3. 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.

1.5. Raptor Call Path Generation VM Sizing Specifications

1.5.1. Raptor Server

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

1.5.2. Raptor Client

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

2. Port Requirements

2.1. Correlation and Dashboard System Connectivity

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

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

2.2. Cisco UC Monitoring System Connectivity

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

2.3. MS Teams System Connectivity

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

2.4. Netflow and DS9 Monitoring System Connectivity

2.4.1. Communication ports between Netflow Source and DS9

Source	Destination	Protocol	Port	Direction	Description
Netflow Source	DS9	UDP	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

2.4.2. 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)

2.4.3. 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
DS9	Dashboard Server	TCP	443	Unidirectional	DS9 System Stats and management
DS9	Dashboard Server	UDP	514	Unidirectional	DS9 System Logs

2.4.4. 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

2.5. VOSS Automate Port Usage

VOSS Automate port usage for each node type:

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

2.6. Skype for Business Monitoring System Connectivity

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

2.7. Avaya Call Manager Connectivity

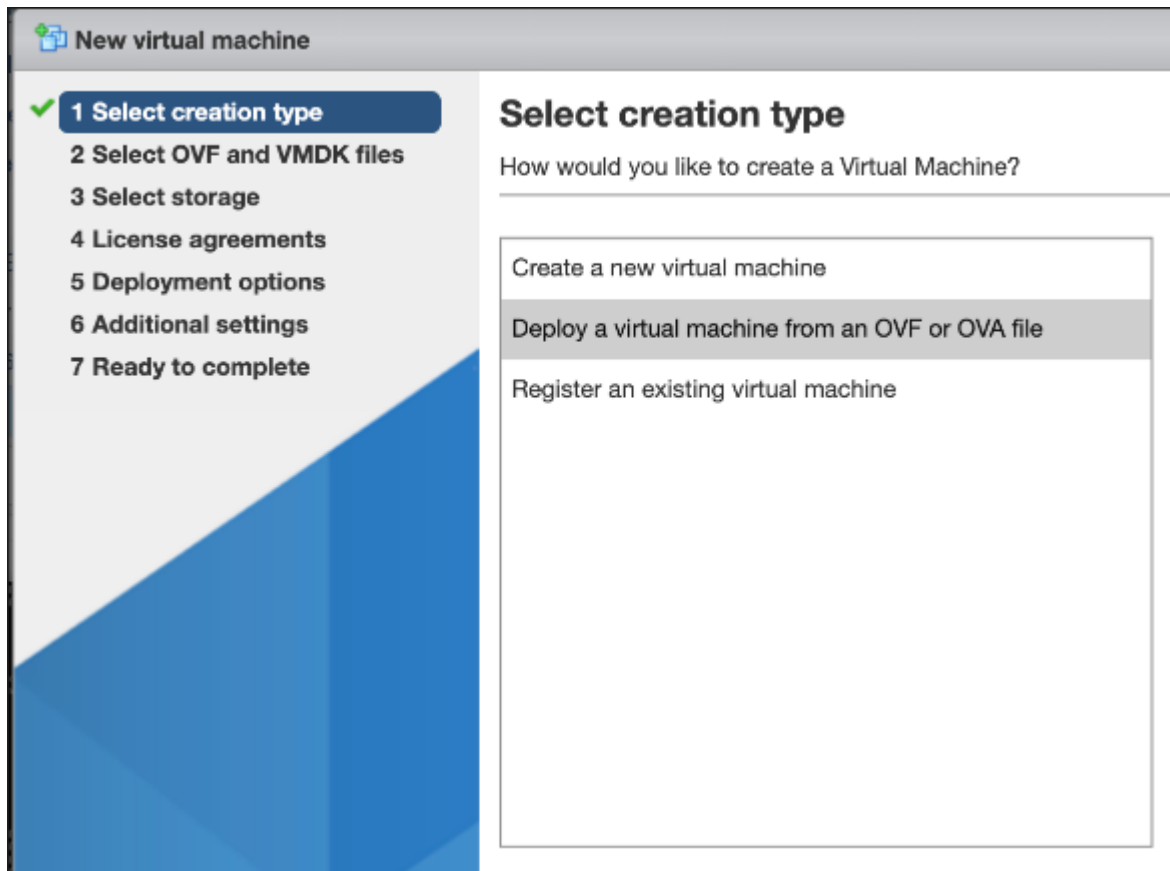
Source	Destination	Port / protocol	Notes
Avaya Call Manager	Insights Arbitrator	9000 TCP	To stream CDRs to the arbitrator

3. Deploy and Networking Setup

3.1. Deploy and VM Installation Steps

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

Select the downloaded OVA file and choose a VM name.



3. Select *storage* according to the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.
4. Select *network* mappings according to the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.
5. When you run the VM, you will see `.1xp` packages being installed. This takes a while.

```

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

```

6. After all the packages are installed, the VM is automatically powered off.

```

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 DHCP OFFERS received.
Unable to obtain a lease on first try. Exiting.
useradd: user 'admin' already exists
mount: /mnt/target/dev: device is busy

```

You will see the auto-poweroff message on the console.

7. After the system boots, wait at the login: prompt until a banner with an About console display shows displaying values for the placeholders below:

```

-----
                          About
-----
Hostname: <hostname>
Version: <version>
Theme: <theme>
Flavor:
License: NNNNN-NNNN-NNNN-NNNN-NNNN
Days Licensed: nnnnn
Days Remaining: nnnnn
Product Key:
Website: <website>
Kernel: Linux n.nn.nn-lxt-3 x86_64 GNU/Linux

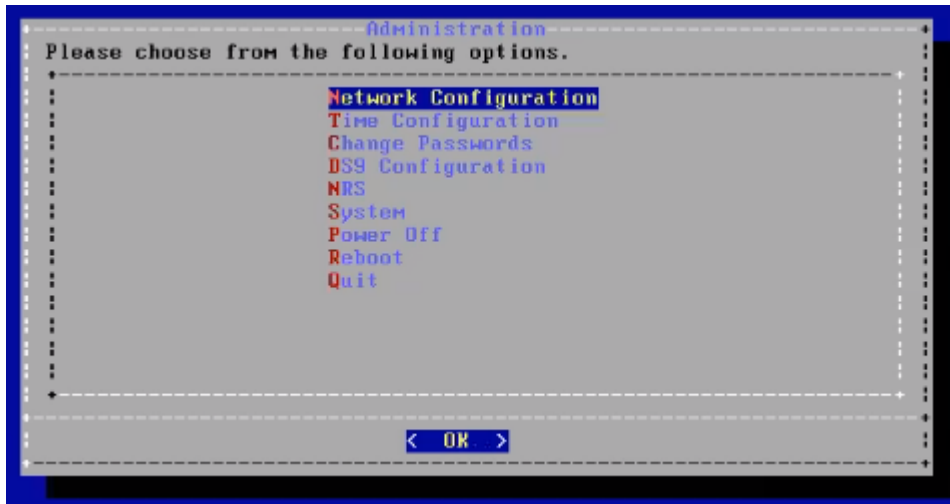
<hostname> login:

```

8. At the login: prompt, log in as admin with password as the last 10 characters of the License: value, *excluding the dash*.

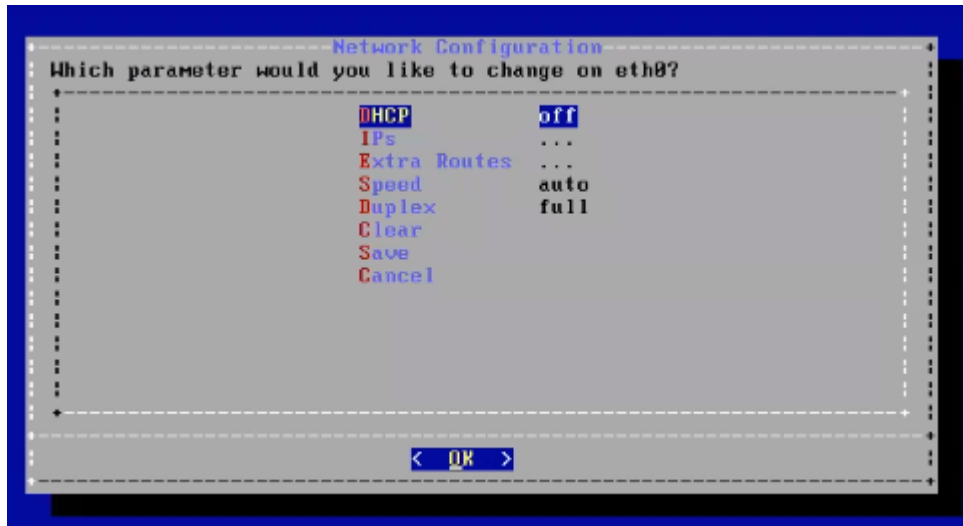
Note: Since the Licence key value is only displayed here. When you ssh in it will not be seen. Be sure to copy out your admin password from this console.

9. After login, the **Administration** menu shows, as in the example below for DS9:



10. Under **Network Configuration**, provide ip/netmask, default gateway and hostname.

- a. Under **Interface Settings**, set the IP Address and netmask in the format, for example: nn.nn.nn.nn/24 and save.



Set up the default gateway under the **Extra Routes** menu.

```

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.

```

b. Set hostname

```

Network Configuration
What would you like to configure?
Interface Settings
DNS Settings
Hostname
Apache Config
SSHD Config
Quit

```

The console will show the Updating hosts: message. Note that this setup takes a few minutes.

11. When this setup completes, you can quit the **Administration** menu on the console and continue 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

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

- Insights DS9

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

4. Database and System Setup

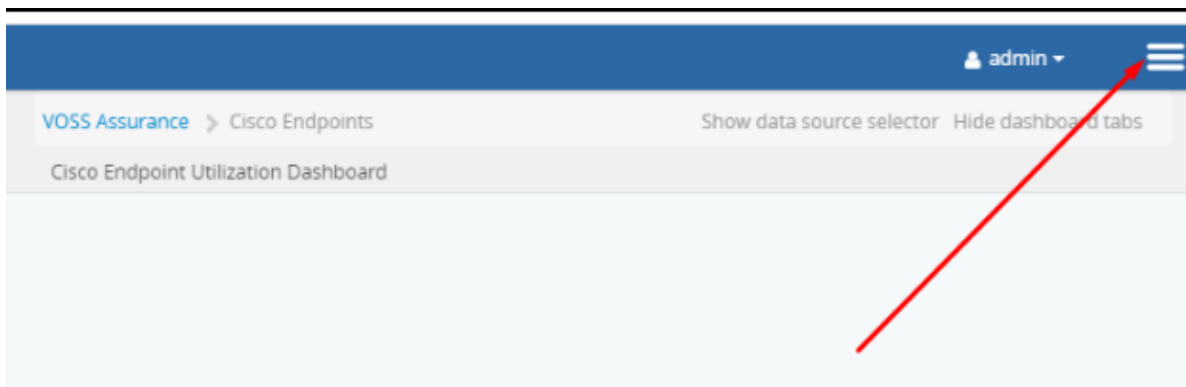
4.1. VOSS Automate Database Setup

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

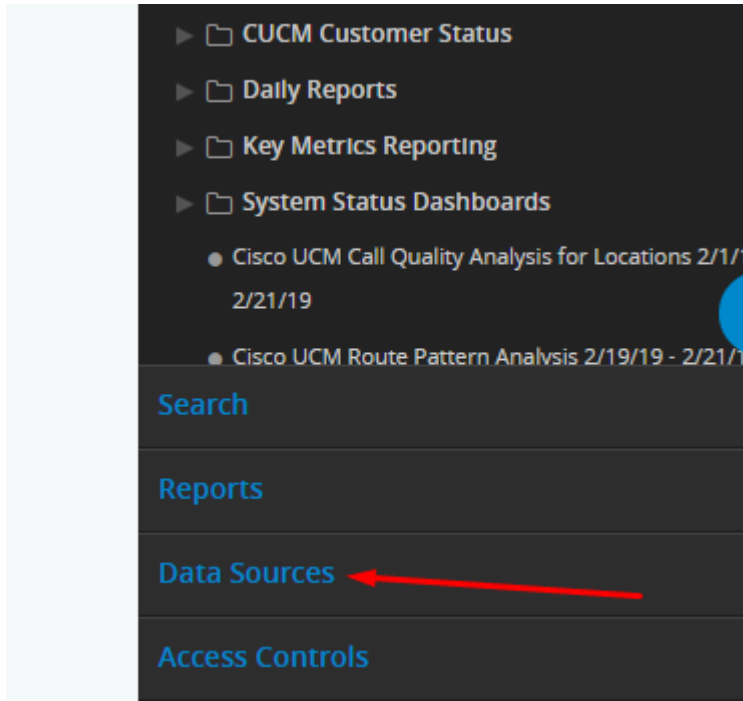
```
platform@gsr10-un1:~$ database user add 1.1.1.1 Analytix
```

IP Address of Dashboard Server

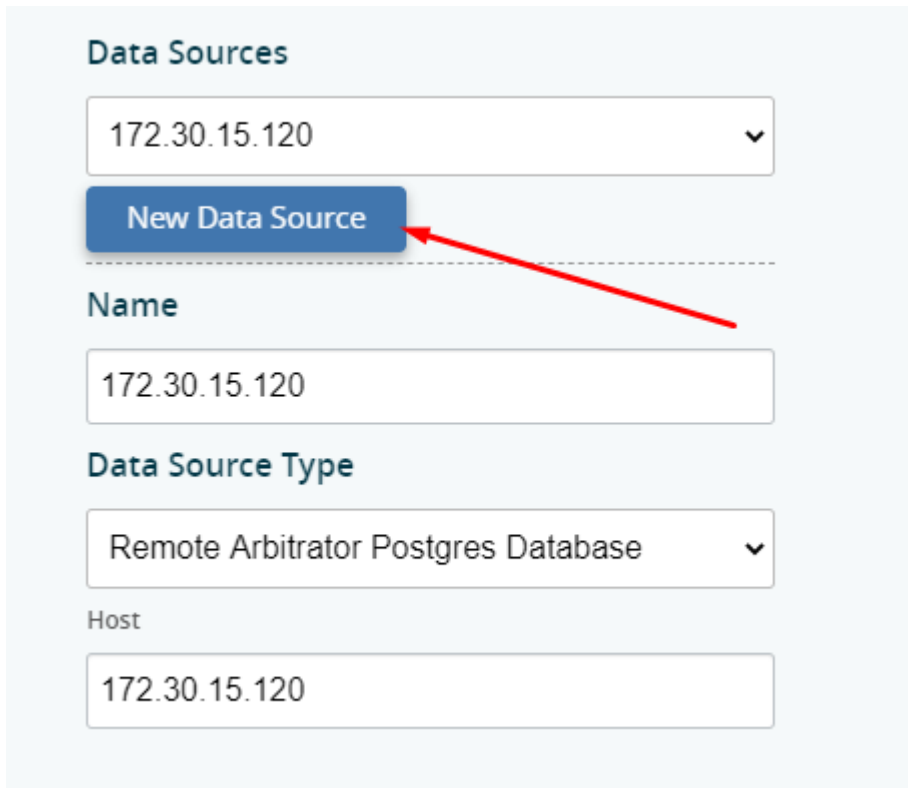
2. Take note of the username and password you just configured
3. Log in to the GUI on the Dashboard Server username admin — password admin
4. Click the toolbar Hamburger Menu icon adjacent to the admin menu.



5. Click **Data Sources**.



6. Click **New Data Source**.



7. Choose **Voss Mongo Database**.

Data Source Type

Voss Mongo Database

Ip

localhost

Port

27020

Db

VOSS

Username

admin

AuthSource

admin

Password

.....

Ssl

true

Alias

Cancel Save

8. Fill out the form presented:

- At **Name**, fill out a name for the data source.
- At **Data Source Type**, choose the data source type.
- At **IP**, set the IP address of VOSS Automate UN1/primary database node.
- Fill out values for **Port** and **DB**.
- At **Username**, fill out the username you set on VOSS Automate.
- At **AuthSource**, change the AuthSource from admin to VOSS.
- Fill out the password set up in VOSS Automate.
- Set SSL to True.

9. Repeat the steps above to add the Arbitrator as a Data Source:

- Fill out a name for the data source.
- Select the data source type (Remote Arbitrator Postgre Database), and fill in the rest of the fields.

- At **Host** set the IP address of the Arbitrator.
- Fill out the port.

4.2. Install Arbitrator System

4.2.1. Policy Configuration Files

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

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

Component	Purpose	Filename
Controls	<p>Controls are actions that the system can automate, user actions to support data collection, analysis before presenting to an operational user as an alert to help reduce user input and provide information and actions faster.</p> <ul style="list-style-type: none"> • 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 <p>Other options that can be developed:</p> <ul style="list-style-type: none"> • 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	<p>A script to poll a system to collect data from a remote system. This is important if the data required can't be streamed from a system to the Arbitrator to be consumed, the Arbitrator and collect data remotely by periodic probing of the system. Examples of probes that collect</p> <ul style="list-style-type: none"> • 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

4.2.2. Installation Steps

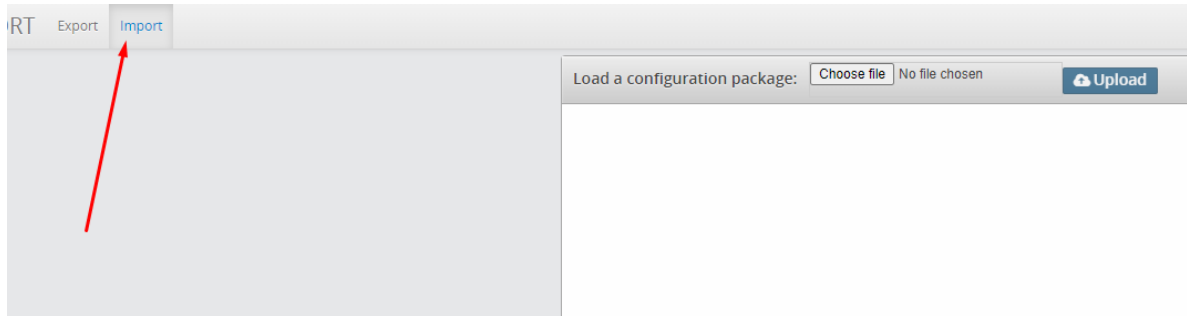
1. Log in to the Arbitrator: admin/admin
2. Click the Wrench icon.



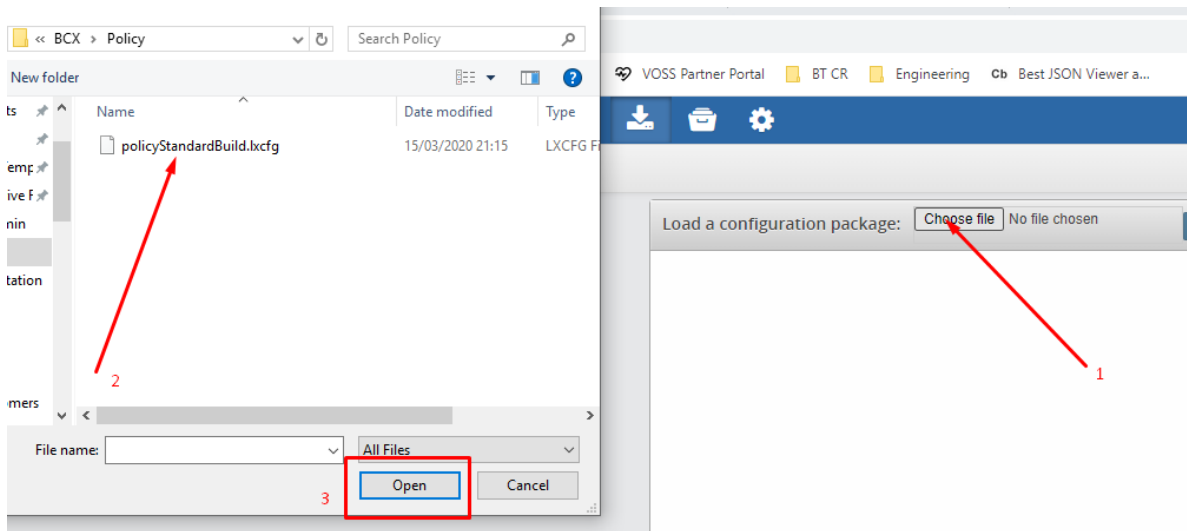
3. Click on the icon shown below



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**.

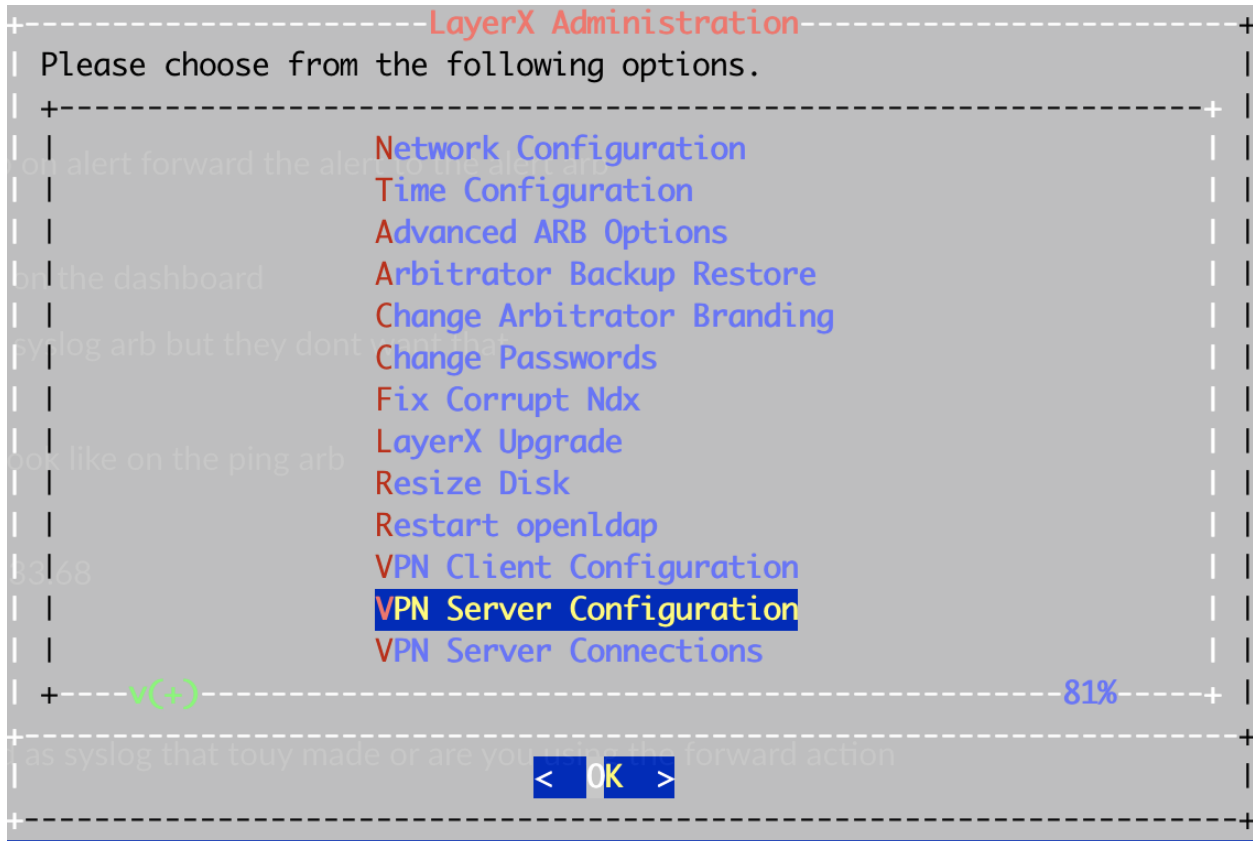
8. Repeat this procedure for the following:

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

See: *Policy Configuration Files*

4.3. Set up Arbitrator to Arbitrator Communication

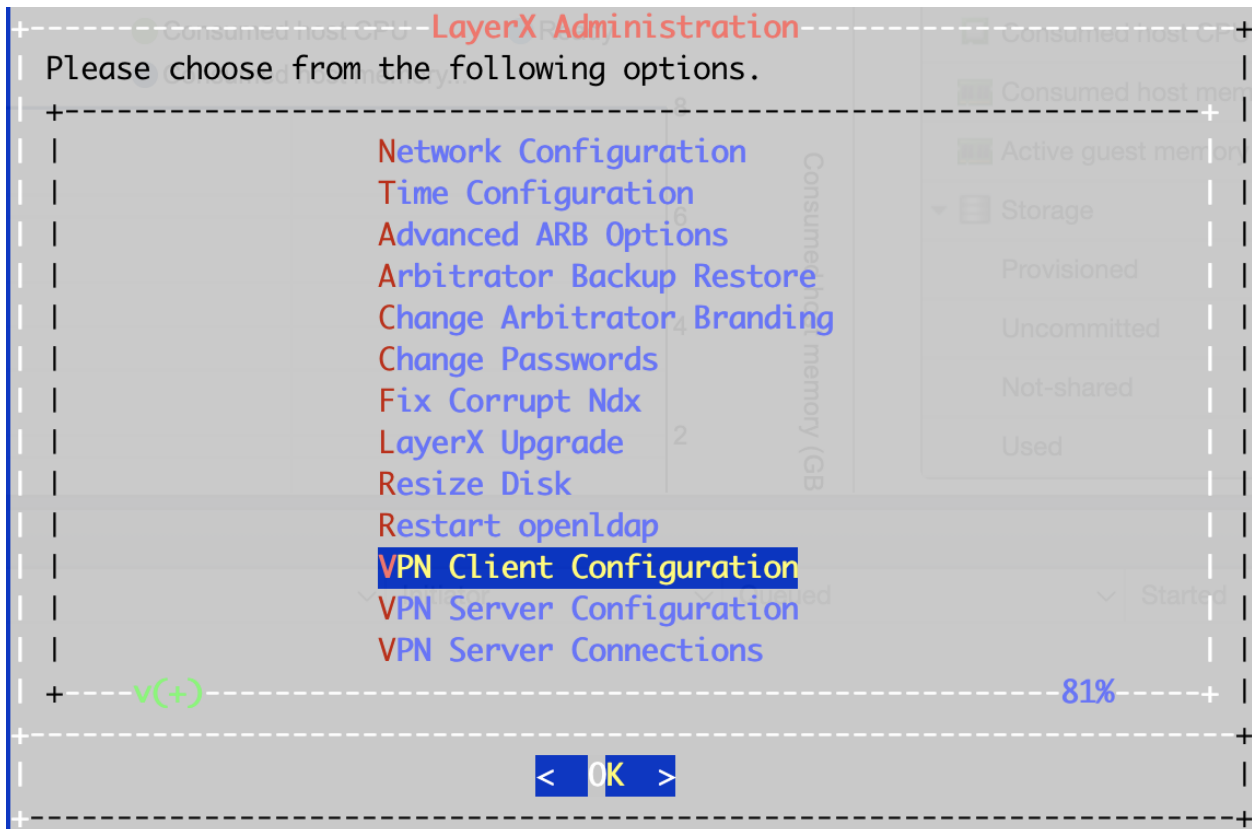
Log in as admin on the central/lead arbitrator and go to VPN Server Configuration



Then Clear Fabric Configuration, then reset this up:

- 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:



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

A Tunnel will now be set up between the Arbitrators.

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

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

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

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

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

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

Methods

Control Type: LinkIPToAlert ✎

Destination: As Event? Click here then click save

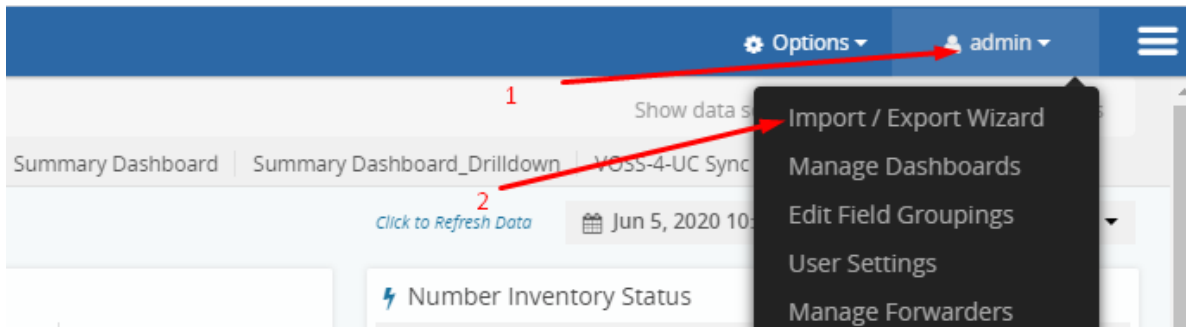
2. Insert the name of the Central ARB

Ensure as event is ticked

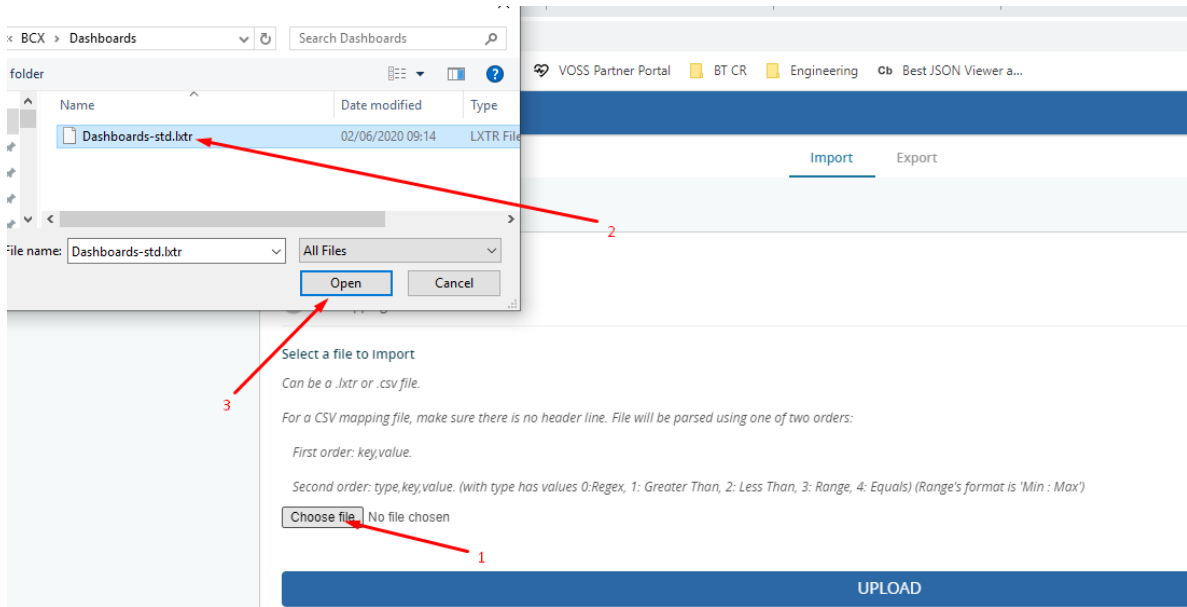
1. Click Forwarder to add

4.4. Install Dashboard System

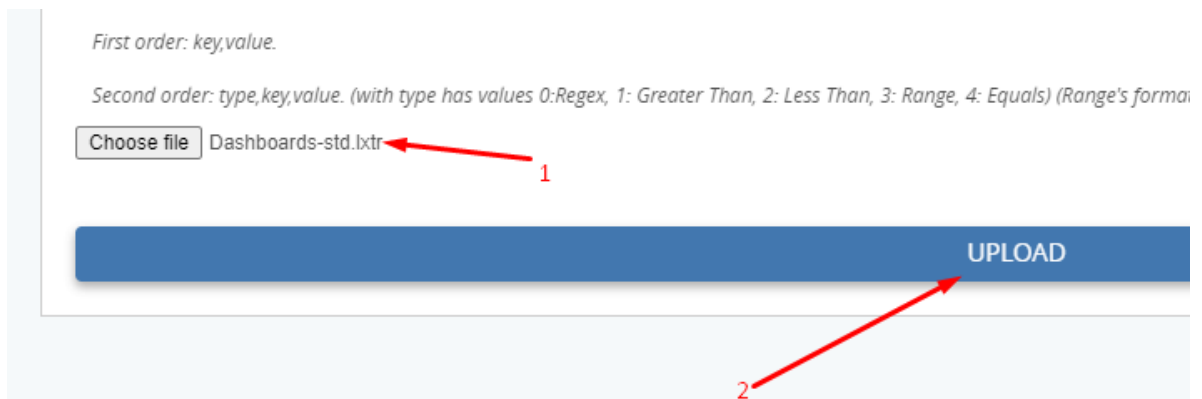
1. Access the Dashboard Server: admin/admin
2. In the top banner bar click on admin, then click on **Import/Export Wizard**.



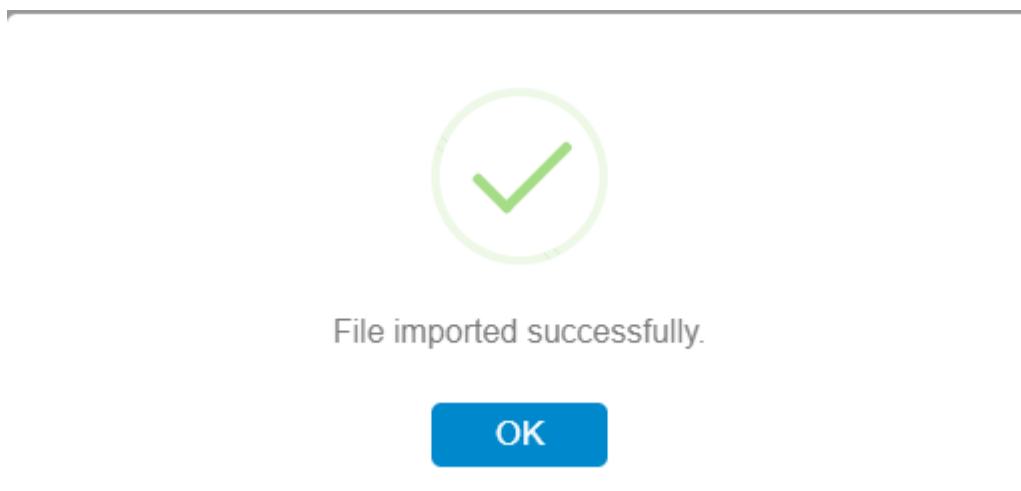
3. Click on **Choose file**, then navigate to the file you wish to import (dashboard files have the .lxtf file extension) then click **OK**.



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

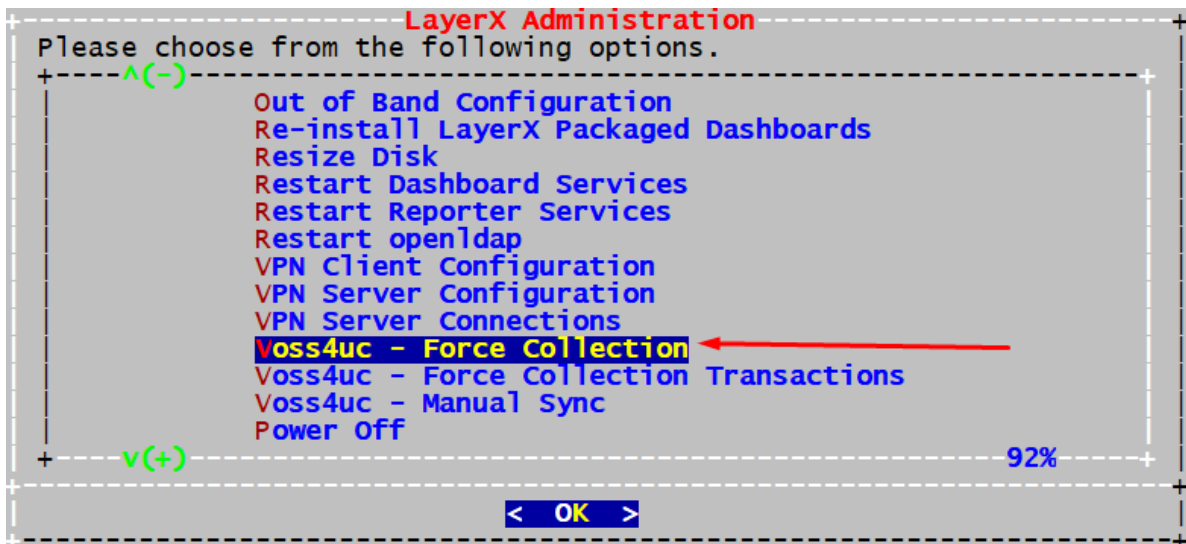


5. Your file will then upload, and you will see the below — click **OK**.



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

the dashboard.



5. Certificates

5.1. Add Certificates

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

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

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

6. CUCM Asset Onboarding

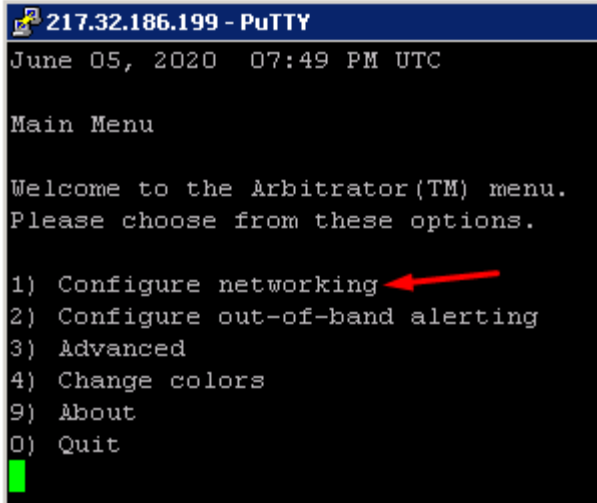
6.1. Customer Onboard

6.1.1. Add Customer CDR Folders

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

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

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



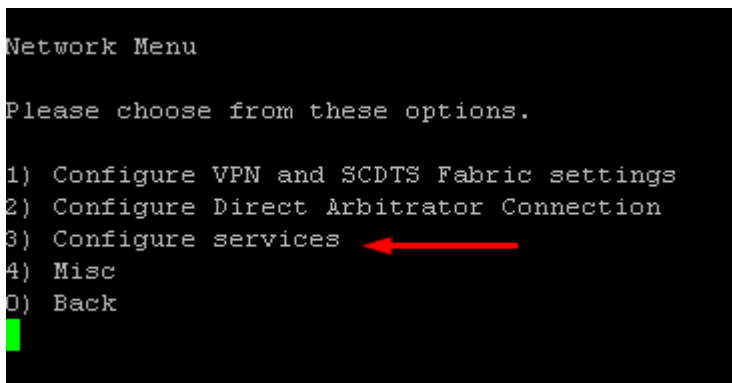
```
217.32.186.199 - PuTTY
June 05, 2020 07:49 PM UTC

Main Menu

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

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

4. Now press 1.

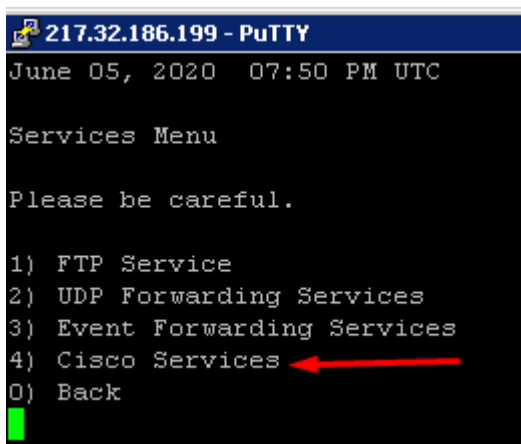


```
Network Menu

Please choose from these options.

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

5. Now press 3.



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

Services Menu

Please be careful.

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

6. Press 4.

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

Cisco Services Menu

Please be careful.

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

7. Press 1.

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

Cisco Call Manager Menu

View Add, Delete, or Clear Cisco Call Manager configur

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

8. Press 2.

This will open the screen below.

```

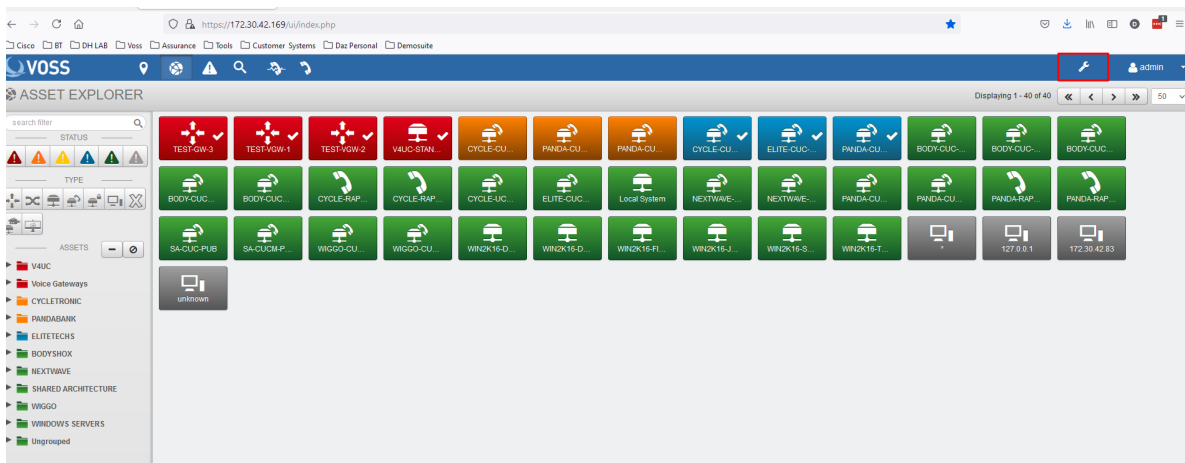
217.32.186.199 - PuTTY
10.144.30.161
10.25.212.1
10.25.212.129
10.25.212.193
10.25.212.65
10.25.213.1
10.25.213.129
10.41.224.1
10.41.224.129
10.41.224.193
10.41.225.1
10.41.225.129
10.41.225.193
10.41.225.65
10.41.240.33
10.41.240.56
10.44.88.1
10.44.88.129
10.44.88.193
10.44.88.65
10.59.247.129
x.x.x.x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

```

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

6.1.2. 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.

The top screenshot shows the 'POLICY CONFIGURATION' page in the VOSS web interface. The 'Rules' tab is selected and highlighted with a red box. The 'Rules' table contains the following data:

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

The bottom screenshot shows the 'ASSET CONFIGURATION' page. The 'All groups' link is highlighted with a red box. At the bottom left, there is a plus icon (+) also highlighted with a red box. The 'Assets' table is currently empty, and the status at the bottom indicates 'No records assets'.

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

VOSS

ASSET CONFIGURATION

Groups

Group Name

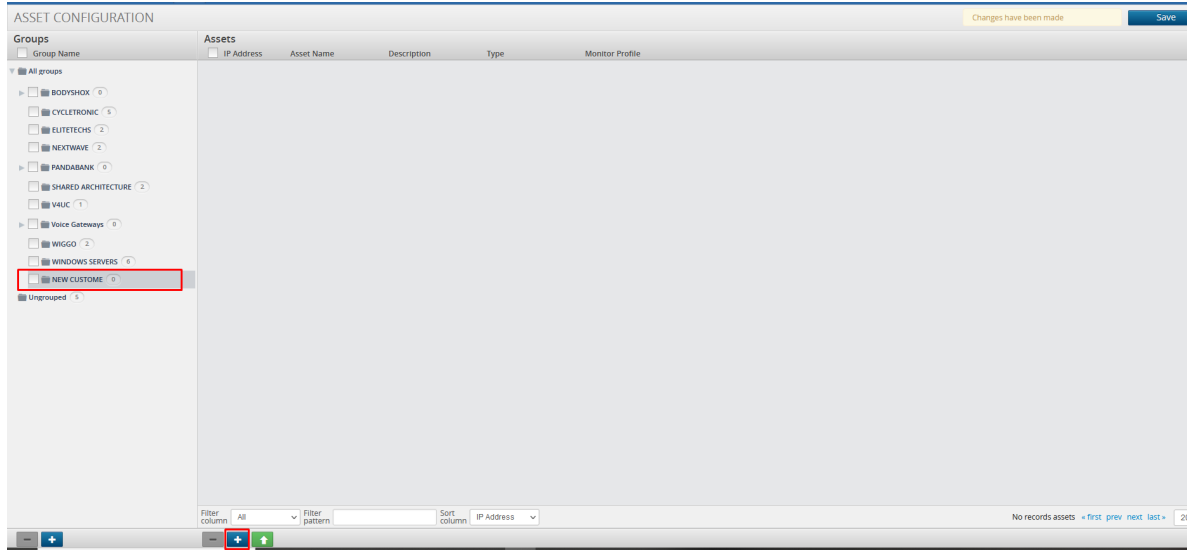
Assets

IP Address Asset Name Description

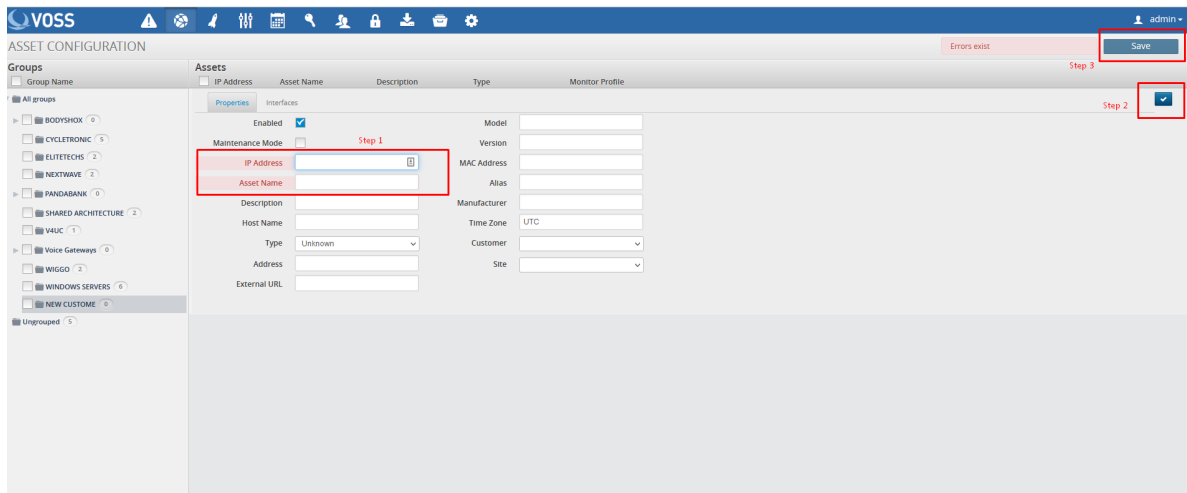
▼ All groups


- ▶ BODYSHOX (0)
- CYCLETRONIC (5)
- ELITETECHS (2)
- NEXTWAVE (2)
- ▶ PANDABANK (0)
- SHARED ARCHITECTURE (2)
- V4UC (1)
- ▶ Voice Gateways (0)
- WIGGO (2)
- WINDOWS SERVERS (6)
- (new) (0)
- Ungrouped (5)

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



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



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

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

CSV Import of Assets

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

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

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

The CSV file is available in the Google Drive.

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

Above is an example.

The mandatory fields are:

- AE_NAME
- IP_ADDRESS

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

Note:

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



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

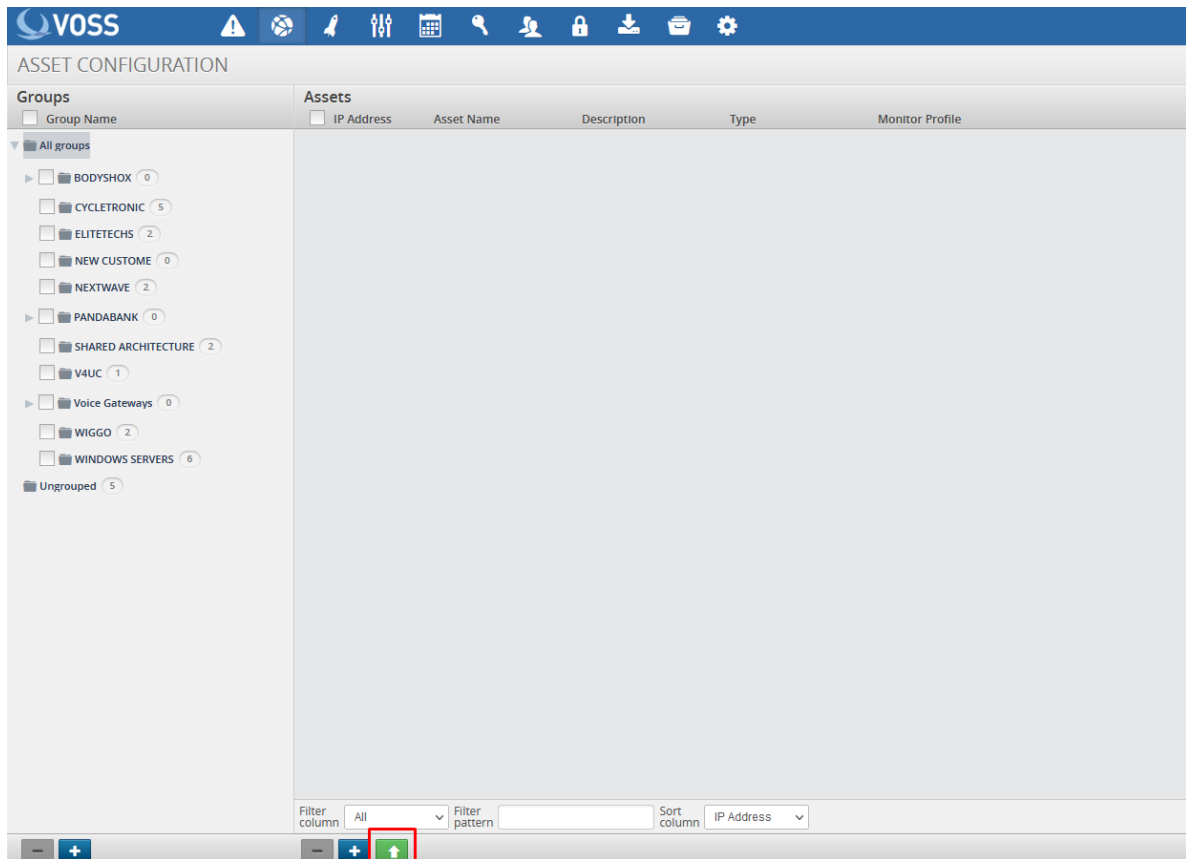
(continues on next page)

(continued from previous page)


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

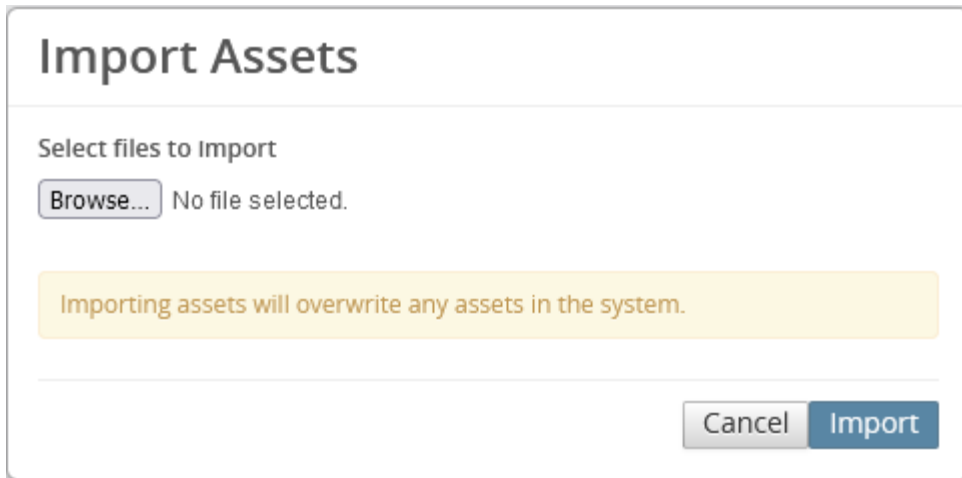
How to Import using CSV

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

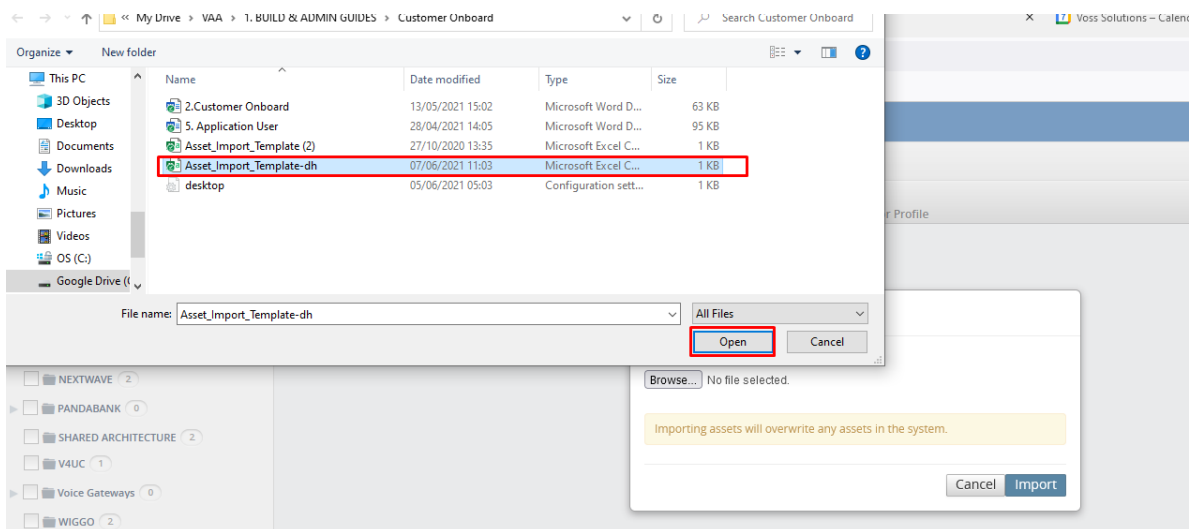


The screenshot displays the VOSS ASSET CONFIGURATION interface. The top navigation bar includes the VOSS logo and several icons. The main content area is divided into two sections: 'Groups' on the left and 'Assets' on the right. The 'Groups' section shows a tree view of asset groups, including 'All groups',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

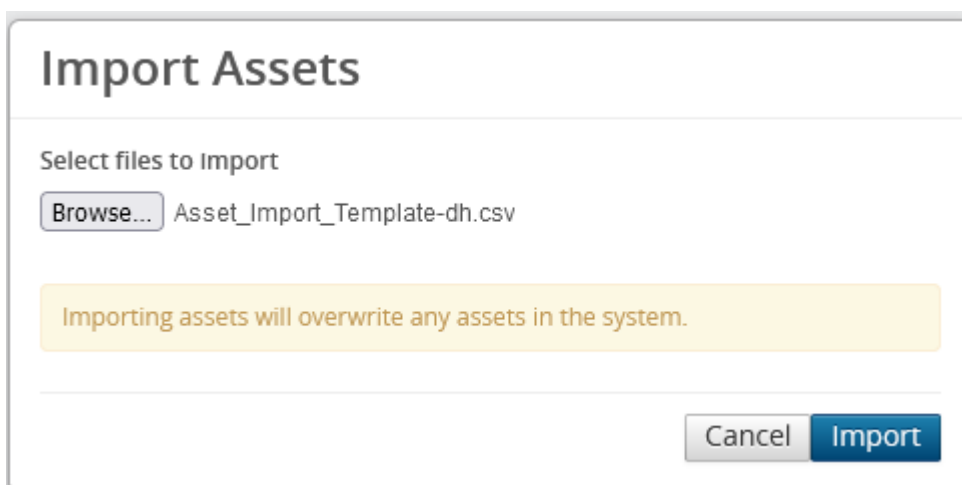
4. Click the Up-arrow  to open the **Import Assets** dialog.



5. Browse to your csv file.



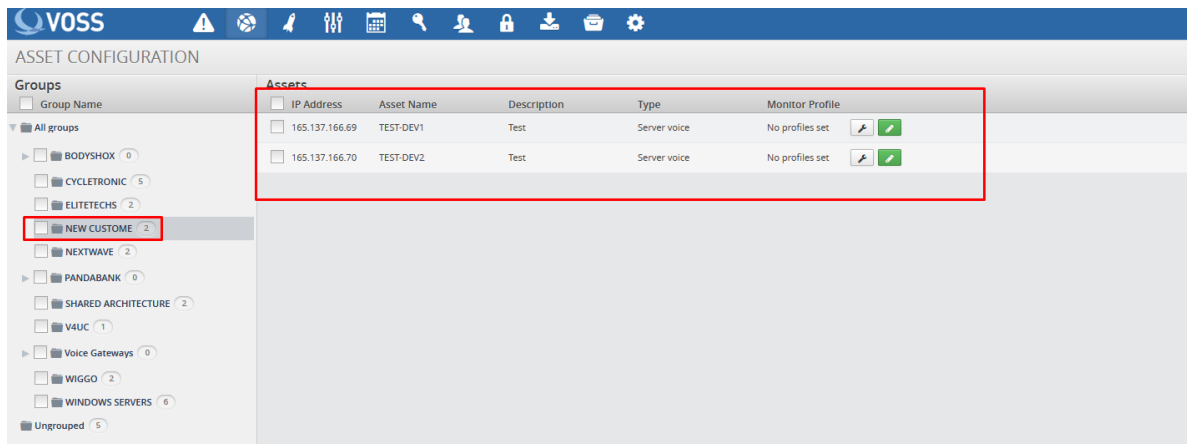
6. Click **Open**.



7. Click **Import**



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

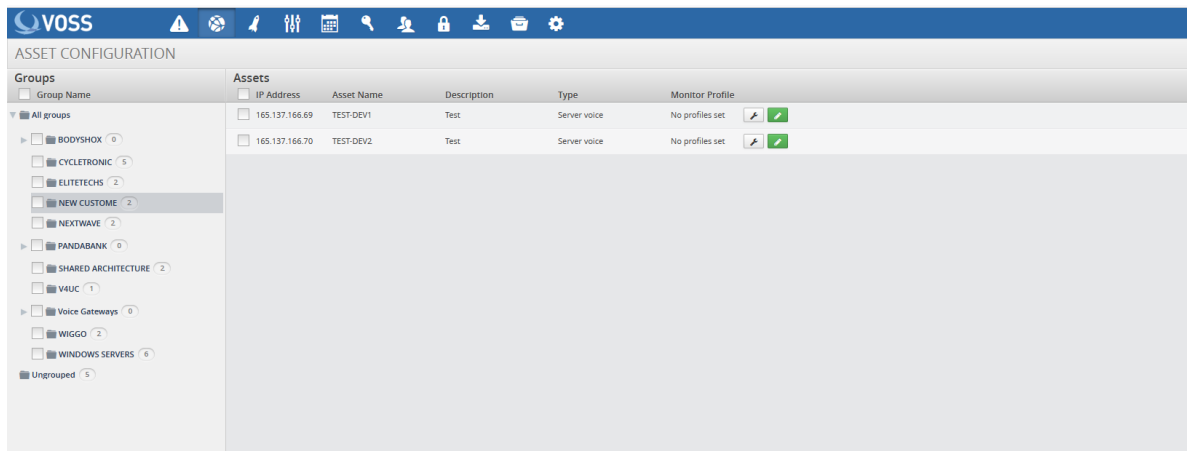
present and in the correct location.



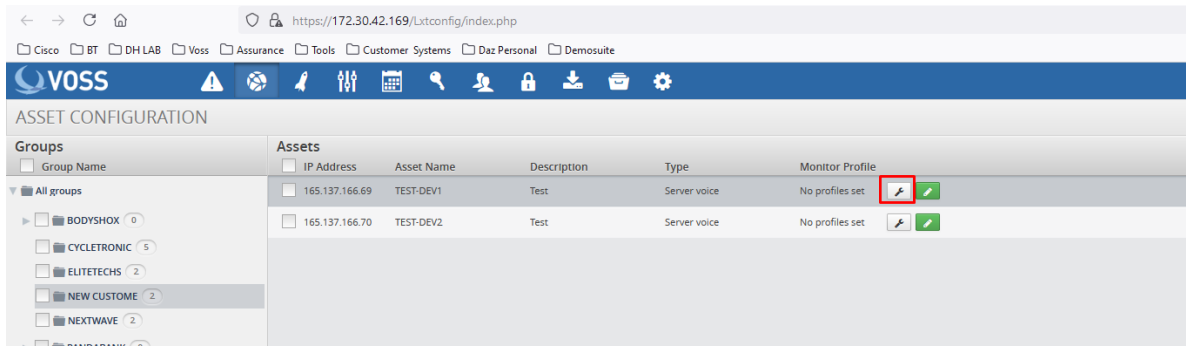
6.1.3. Assigning Probes to Assets

Assign Standard Probes

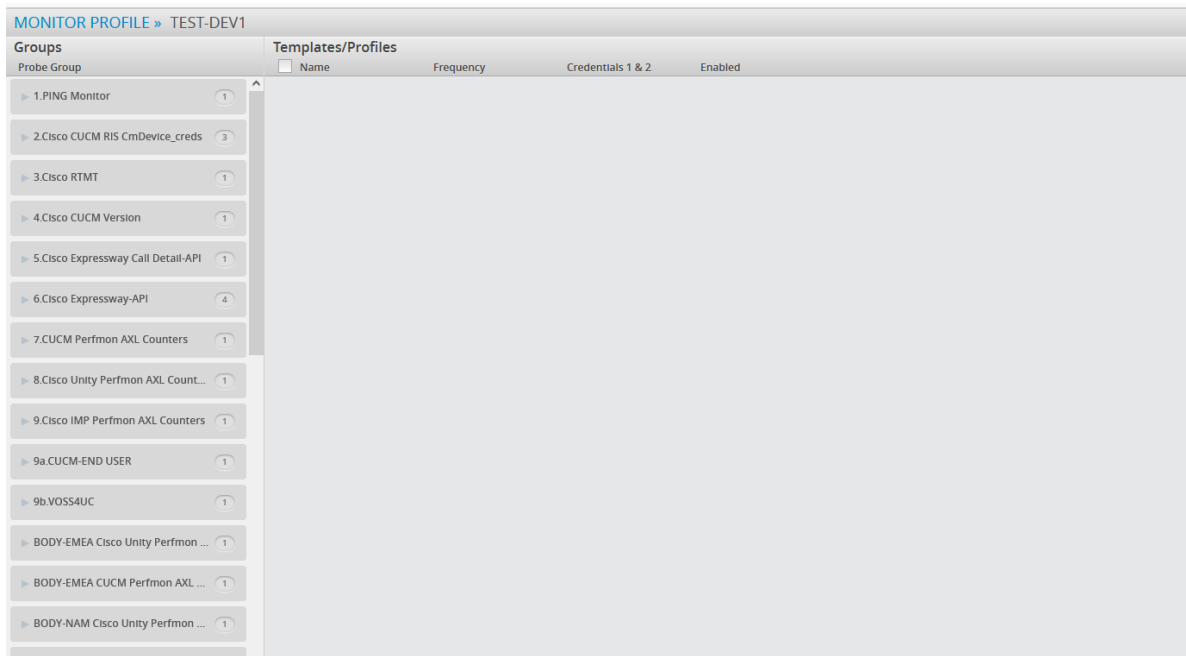
1. Log in to the Arbitrator with admin privileges.
2. Click on the  to open the configuration screen.
3. Click on the  to open the Asset Configuration screen.
4. Select the Asset Group that contains the assets you wish to configure



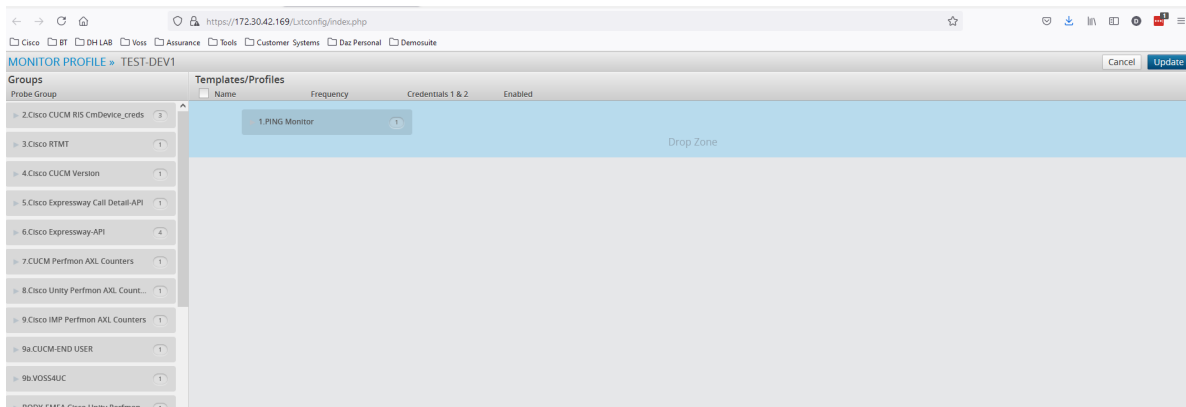
5. Click on the wrench icon as shown below.



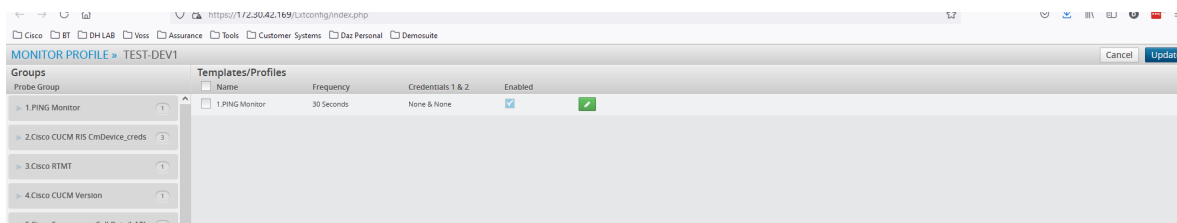
This will then open the Assignment screen.




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.



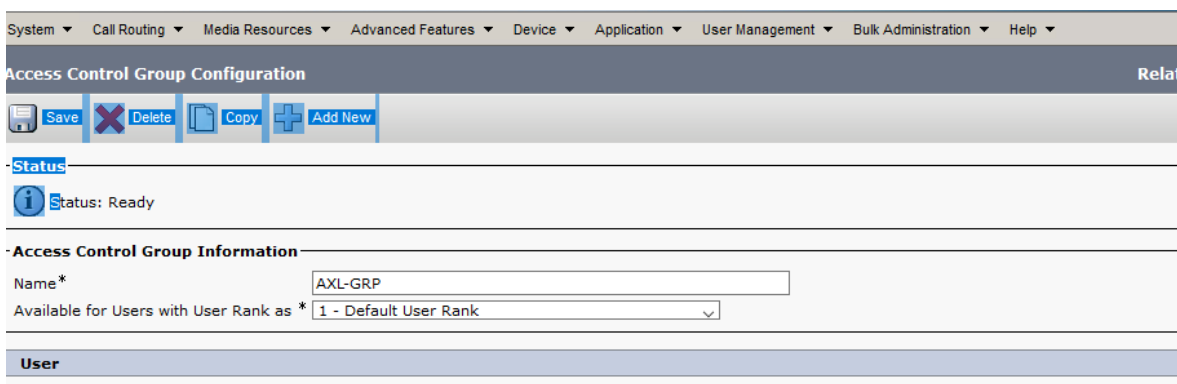
8. If you then click on  you can set any time schedules / credentials required for this probe
9. Once finished click **Update** and then click **Save**.

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

6.2. Call Manager Configuration

6.2.1. Application User

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



4. Add roles to this new group.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

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

Access Control Group Configuration

Save

Status

Status: Ready

Access Control Group Information

Name* AXL-GRP

Role Assignment

Role

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

Save

*- indicates required item.

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

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

6.2.2. Enterprise Parameters

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

Enterprise Parameters Configuration

Save Set to Default Reset Apply Config

[Reply Multicast Echo Request](#)*

Cisco Syslog Agent

Remote Syslog Server Name 1	62.7.201.25
Remote Syslog Server Name 2	217.32.186.230
Remote Syslog Server Name 3	

CUCM Service Parameters

Ensure CDR Service Parameters are set:

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

System	
CDR Enabled Flag *	True
CDR Log Calls with Zero Duration *	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	<input type="checkbox"/>	CYCLE-CUCM-PUB	172.30.42.73

Billing Application Server Parameters

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

① Click on the Add New button to add a new Billing Application Server

② Click on the corresponding Server Name to Update the Billing Application Server details

③ 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.

④ Click on the Reset Button to Generate new Keys and reset the connection to the SFTP server.

3. Fields:

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

Billing Application Server Parameters

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