VOSS

VOSS Insights
Analytics Install Guide

Release 25.2

August 27, 2025

Legal Information

DOCUMENT ID: 20250827134114

Contents

1. What’s New

1.1. Analytics Install Guide: Release 25.2

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

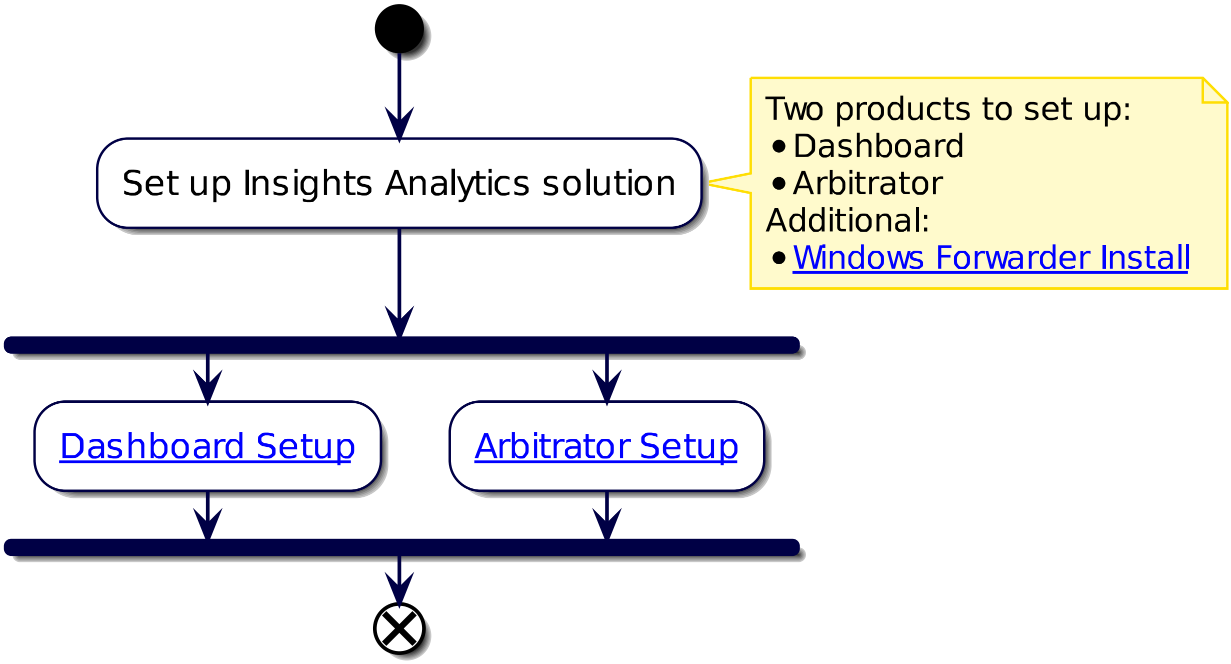
  Added steps for creating GUI admin passwords for Arbitrator and Dashboard.

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

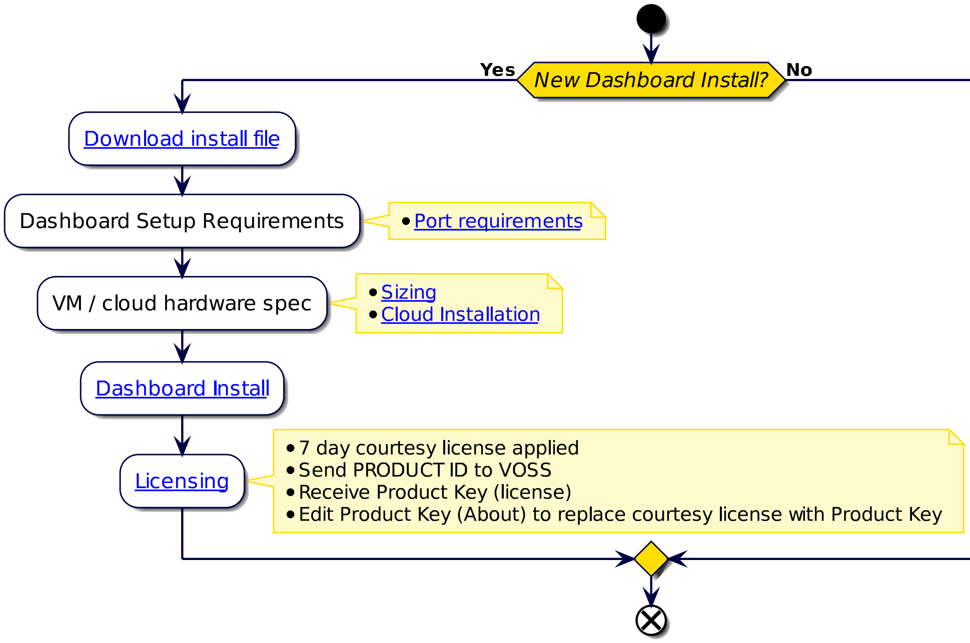
  Added details on the support for SSL certificates using 4096-bit encryption.

2. Insights Analytics Quickstart

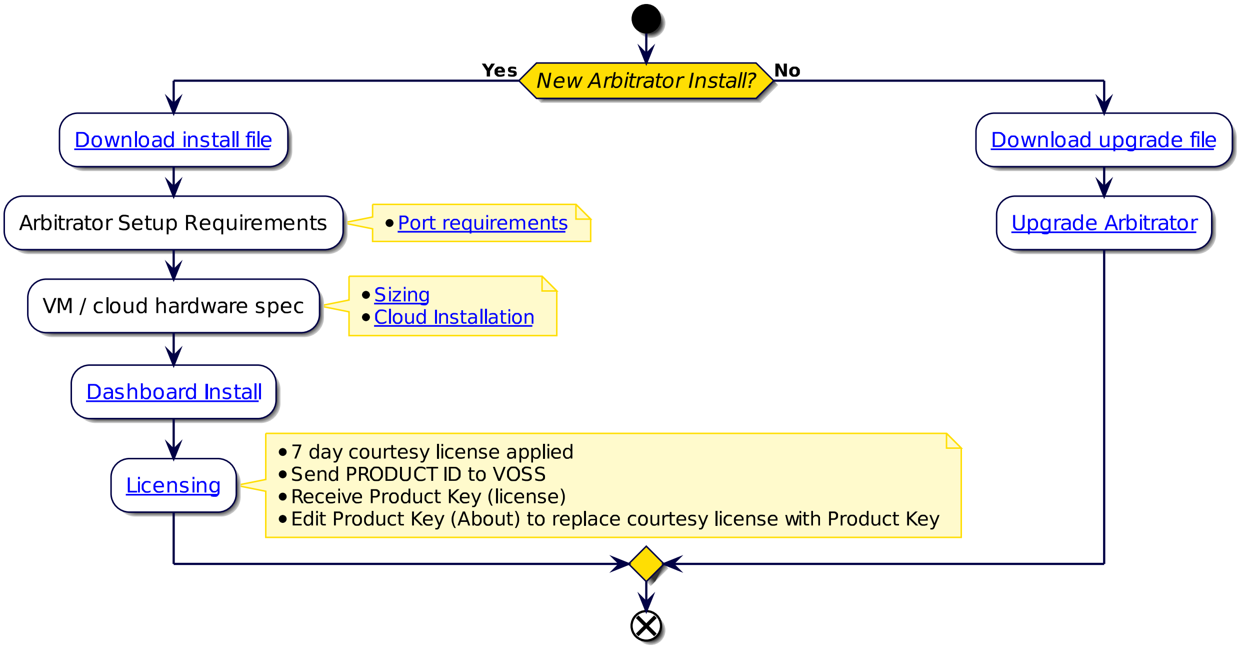
2.1. Insights Analytics Setup Overview



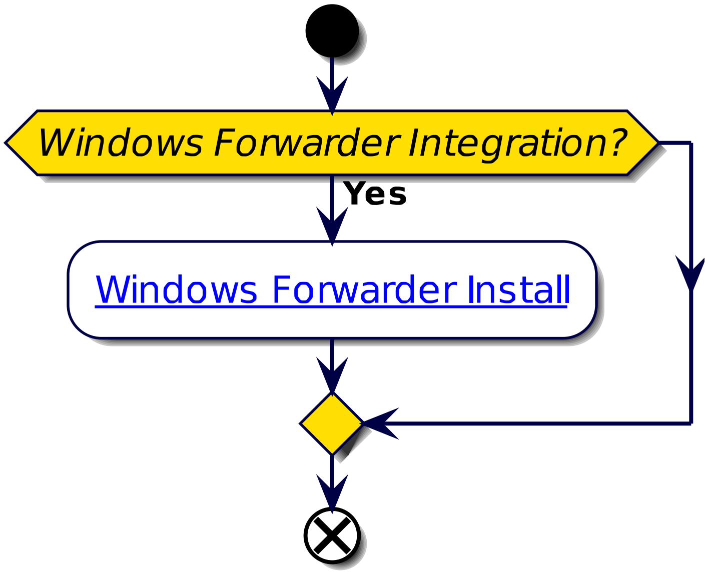
2.2. Dashboard Setup


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

2.3. 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

2.4. Dashboard Integrations



2.5. Analytics Solution Documentation

2.5.1. Additional Reference Documentation

- Dashboard Release Notes
- Compatibility Matrix
- Dashboard Install Guide
- Dashboard and Arbitrator Maintenance and Upgrade Guide
- Dashboard Administration Guide
- Dashboard API Guide
- Platform Guide
- Arbitrator Release Notes
- Compatibility Matrix
- Arbitrator Install Guide
- Dashboard and Arbitrator Maintenance and Upgrade Guide
- Arbitrator Administration Guide
- Arbitrator API Guide
- Platform Guide
- VOSS Insights Windows Forwarder Install Guide

3. Download

3.1. Dashboard download

- Dashboard OVA file:

  1. Log in on the VOSS Customer Portal
  2. Go to **Downloads > VOSS Insights > Insights Dashboard > <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>
     ```

- Dashboard upgrade file:

  1. Log in on the VOSS Customer Portal
  2. Go to **Downloads > VOSS Insights > Insights Dashboard > <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. 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 recommended 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.

4.2. 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. Ports

5.1. Ports, protocols, and access rights

5.1.1. Overview

This topic details the ports, protocols, and access rights (including login and permissions) required for Insights to interact with assets and to monitor and collect analytics data. The topic has the following sections:

- *Ports*
- *Permissions*

5.1.2. Ports

Source: UC assets/devices

The table describes the destinations, protocols, and ports for various UC assets/devices sources required for Insights to interact with assets and to monitor and collect analytics data:

Source	Destination	Protocol	Port
UC Assets/Devices			
Cisco UC / CUBE (Syslog, CDR/CMR)	Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	TCP/UDP	22, 514
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco UC / CUBE (AXL, SNMP query, and SSH)	TCP/UDP	22, 161, 162, 443, 8443
Cisco UCCE (CVP, Finesse, CUIC, VVB, PG/HDS/Roggr/Logger) (SNMP traps)	VOSS Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	TCP/UDP	161, 162
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco UCCE (CVP, Finesse, CUIC, VVB, PG/HDS/Roggr/Logger) (read-only SNMP query)	TCP/UDP	161, 162
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco UCCE (Finesse) (read-only API query)	HTTPS	8443, 443
Cisco Analog Gateways (SNMP trap)	Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	UDP	161, 162
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Microsoft Teams	HTTPS, Graph API	443
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco WebEx Calling DI	HTTPS, AXL API & RIS API	443
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	AudioCodes Mediant Session Border Controllers (SNMP query, API)	TCP/UDP	161, 162, 443
AudioCodes Mediant Session Border Controllers (SNMP traps)	Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	UDP	161, 162

Source: Other applications

The table describes the destinations, protocols, and ports for various other applications (non-UC assets/devices sources) required for Insights to interact with assets and to monitor and collect analytics data:

Source	Destination	Protocol	Port
Other Applications			
Insights Dashboard Server (Cloud)	Microsoft Active Directory LDAP Server	LDAPS	TCP 636
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Microsoft Active Directory LDAP Server	LDAPS	TCP 636
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Mail Server (SMTPS)	SSL/TLS	TCP 465/587
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	ServiceNow	HTTPS	TCP 443

5.1.3. Permissions

The table describes applications and their access rights (including login and permissions) required for Insights to interact with assets and to monitor and collect analytics data.

Application	Permissions
Cisco UC / CUBE / Cisco WebEx DI	Configure the appropriate Cisco UC device: • To forward SNMP trap to the local Insights Arbitration servers • Syslog settings to direct log messages • Forward CDR to the local VOSS Insights Arbitration servers • Create SNMPv2 or SNMPv3 connection string • System user with read-only access and Standard AXL API Access role
Cisco UCCE	Create a system user on UCCE Finesse to enable Insights to execute Finesse API. The role that is applied to the system user should include: • “Read Only Agent Data” • “Read Only Queue Data” privileges
Cisco Analog Gateways	Forward SNMP trap to the local Insights Arbitration servers
AudioCode Mediant eSBC	Configure the appropriate eSBC device: • To forward SNMP traps to the local Insights Arbitration servers • Create SNMPv2 or SNMPv3 connection string • Syslog settings to direct log messages • Read-only System user with API access for system monitoring

Application	Permissions
Microsoft Teams	The following credential info is required: a. Application (client) ID b. Directory (tenant) ID c. Client secret Value The following permissions need to be granted for the application: • AuditLog.Read.All • CallRecord-PstnCalls.Read.All • CallRecords.Read.All • Device.Read.All • DeviceManagementApps.Read.All • DeviceManagementConfiguration.Read.All • DeviceManagementRBAC.Read.All • DeviceManagementServiceConfig.Read.All • Directory.Read.All • Group.Read.All • GroupMember.Read.All • Organization.Read.All • OrgSettings-Microsoft365Install.Read.All • OnlineMeetings.Read.All • Reports.Read.All • ServiceHealth.Read.All • ServiceMessage.Read.All • Team.ReadBasic.All • TeamsActivity.Read.All • TeamSettings.Read.All • TeamworkAppSettings.Read.All • TeamworkDevice.Read.All • TeamworkTag.Read.All • User.Read.All • User.ReadBasic.All • VirtualEvent.Read.All

Application	Permissions
SMTP server	A dedicated service account to be utilized by Insights with the following minimum necessary permissions to: • Send Email • Relay Access (if applicable) • Send As/On Behalf Of (optional but recommended for improved security) • Create a user group that the mail can be sent to.
ServiceNow	A dedicated service account with a role like: `rest_service` **Note:** These are the minimum permissions required. Additional permissions may be required based on specific use case.

5.2. Arbitrator and Dashboard system connectivity

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

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

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

5.3. 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

5.4. MS Teams System Connectivity

Source	Destination	Port / protocol	Notes
Cloud Arbitrator	Dashboard Server	5432 TCP	Pushes data to the dashboard to display dashboard data
Client PC - GUI Interface and CLI Management Access	Correlation Server / Dashboard Server	443, 8443, 22, 80 TCP	User Interface Access
Arbitrator	Microsoft (https://graph.microsoft.com/v1.0)	443 TCP	The Arbitrator pulls the full call record details directly from Microsoft, using the https://graph.microsoft.com/v1.0 API.

5.5. NetFlow and DS9 Monitoring System Connectivity

5.5.1. 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

5.5.2. 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)

5.5.3. Communication ports between the DS9 Server and Dashboard Server

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

Source	Destination	Protocol	Port	Direction	Description
Dashboard Server	DS9	TCP	5432	Unidirectional	Data repository access
Dashboard Server	DS9	TCP	8082	Unidirectional	Data repository access
Dashboard Server	DS9	TCP	443	Unidirectional	DS9 System Stats and management
DS9	Dashboard Server	UDP	514	Unidirectional	DS9 System Logs

5.5.4. 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

5.6. 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

5.7. 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

6. Deploy and Networking Setup

6.1. Deploy and VM installation

6.1.1. Base install and configuration

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

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

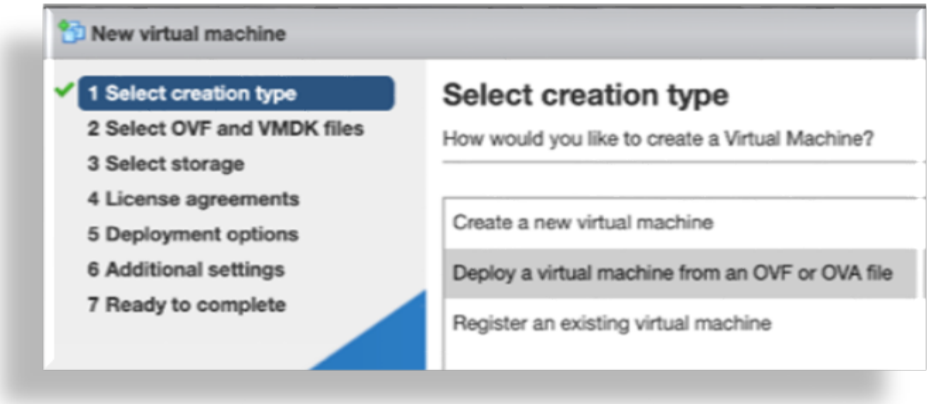
Step 1: Download OVA

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

Step 2: Deploy the OVA

To deploy the OVA:

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


New virtual machine
1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete
Select creation type
How would you like to create a Virtual Machine?
Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

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

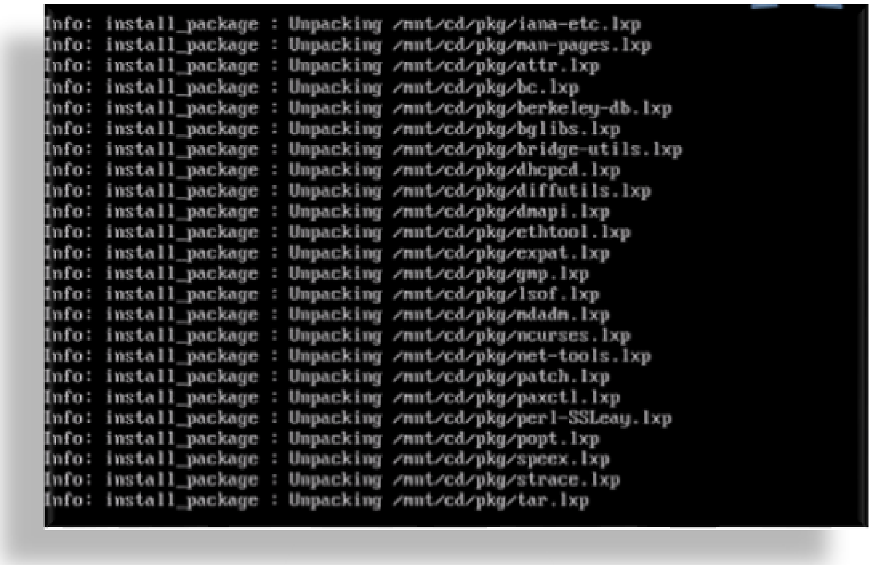
   See the *VMWare Specification and Requirements* for your system.

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

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

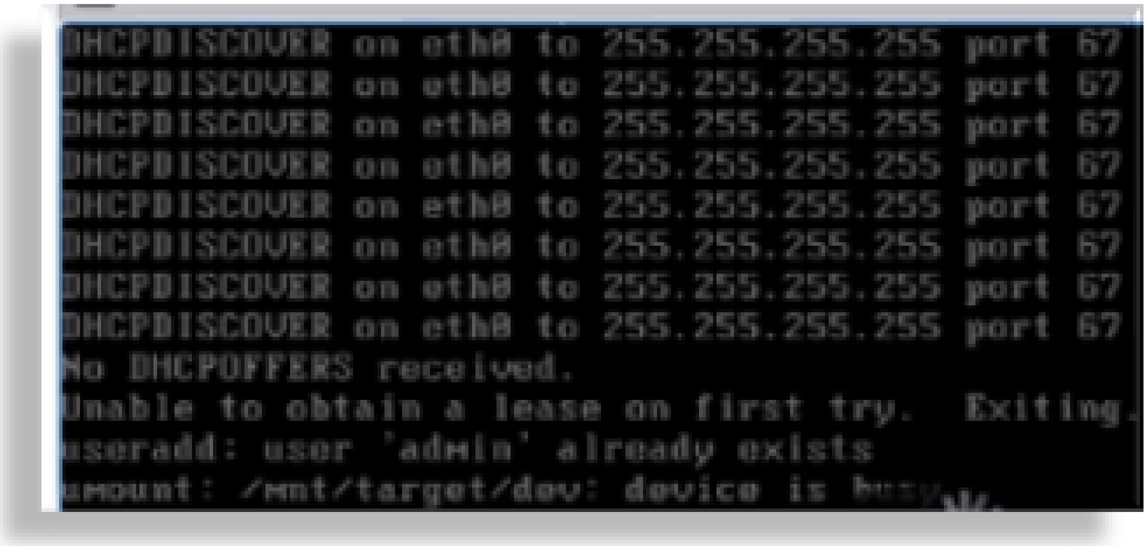
Step 3: Run the VM

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



```
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.
```

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

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

<hostname> login:
```

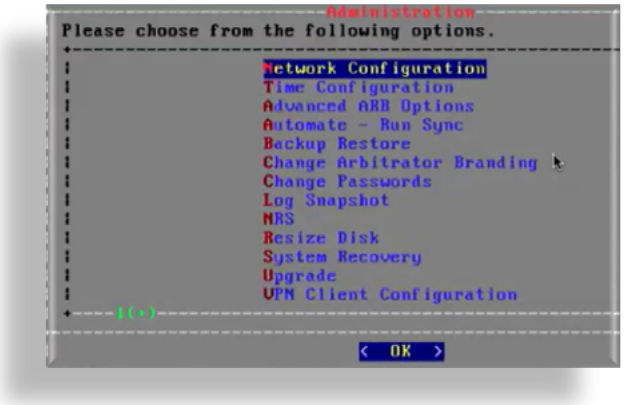
Step 4: Log in to the Administration console

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

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

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

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



```
Administration
Please choose from the following options.
Network Configuration
Time Configuration
Advanced ARB Options
Automate - Run Sync
Backup Restore
Change Arbitrator Branding
Change Passwords
Log Snapshot
NRS
Resize Disk
System Recovery
Upgrade
VPN Client Configuration
↓(+)
< OK >
```

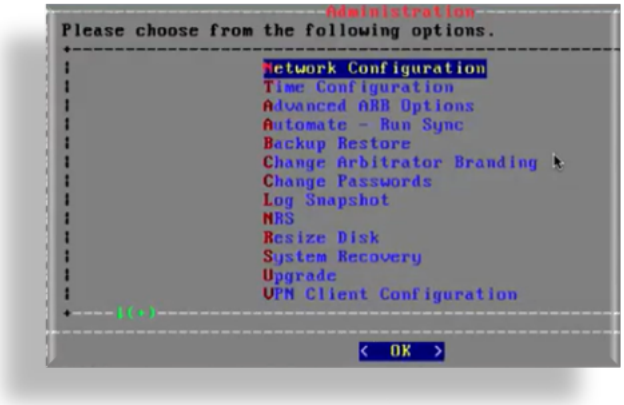
Step 5: Change the admin user password

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

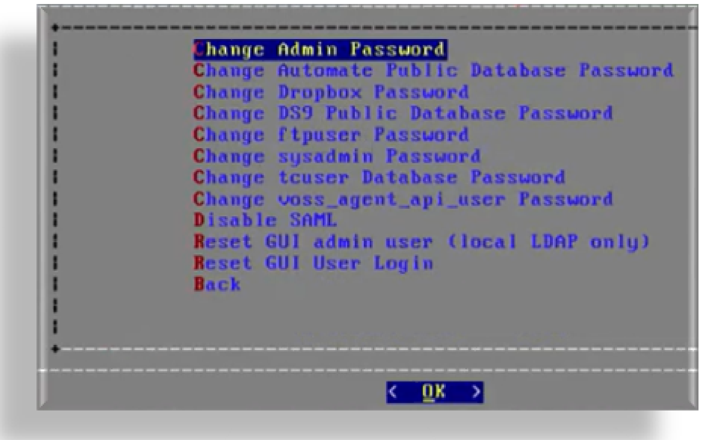
Note: The admin password will need to be updated for all Insights products you install. For security purposes, it is recommended that you update this admin password prior to configuring the VM networking address.

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

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



```
Administration
Please choose from the following options.
Network Configuration
Time Configuration
Advanced ARB Options
Automate - Run Sync
Backup Restore
Change Arbitrator Branding
Change Passwords
Log Snapshot
NRS
Resize Disk
System Recovery
Upgrade
VPN Client Configuration
↓(+)
< OK >
```



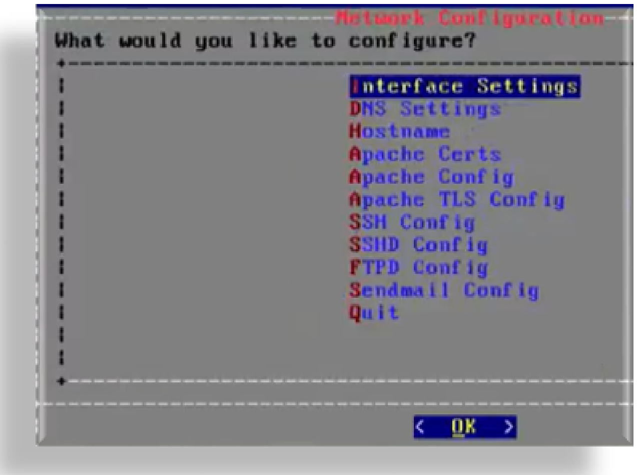
```
Change Admin Password
Change Automate Public Database Password
Change Dropbox Password
Change DS9 Public Database Password
Change ftpuser Password
Change sysadmin Password
Change tcuser Database Password
Change voss_agent_api_user Password
Disable SAML
Reset GUI admin user (local LDAP only)
Reset GUI User Login
Back

< OK >
```

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

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

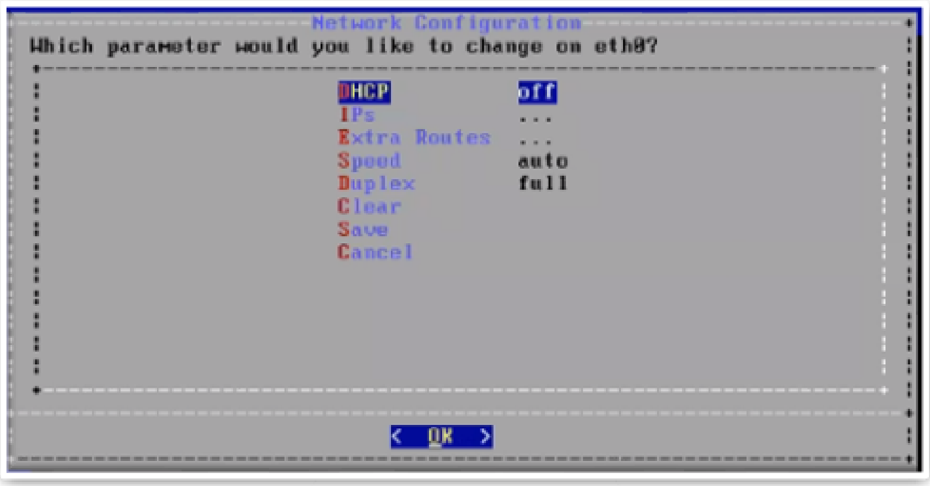
Step 6: Configure network settings

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



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

Interface Settings
DNS Settings
Hostname
Apache Certs
Apache Config
Apache TLS Config
SSH Config
SSHD Config
FTPD Config
Sendmail Config
Quit

< OK >
```

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

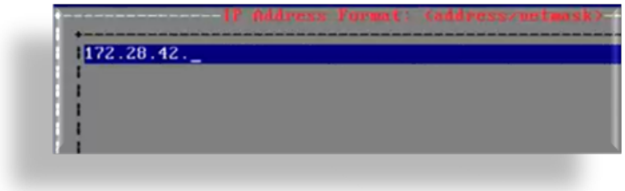


Network Configuration

Which parameter would you like to change on eth0?

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

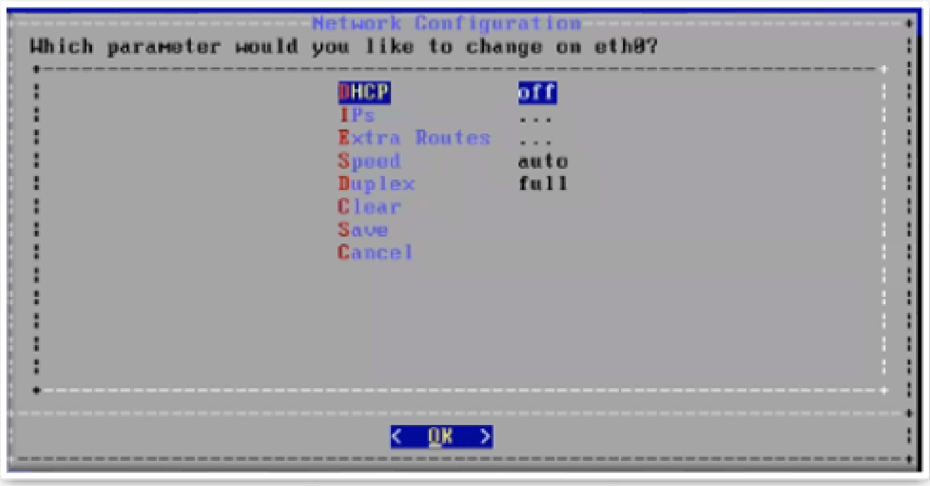
iii. Select **IPs**. Set the IP address and netmask in the format `nn.nn.nn.nn/24`. Click **OK**.



IP Address Format: (address/netmask)

```
172.28.42._
```

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

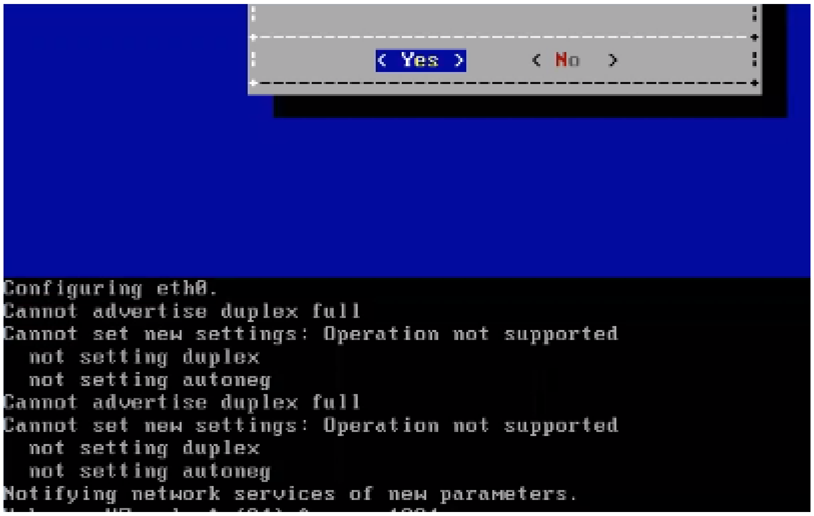


Network Configuration

Which parameter would you like to change on eth0?

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

- 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.

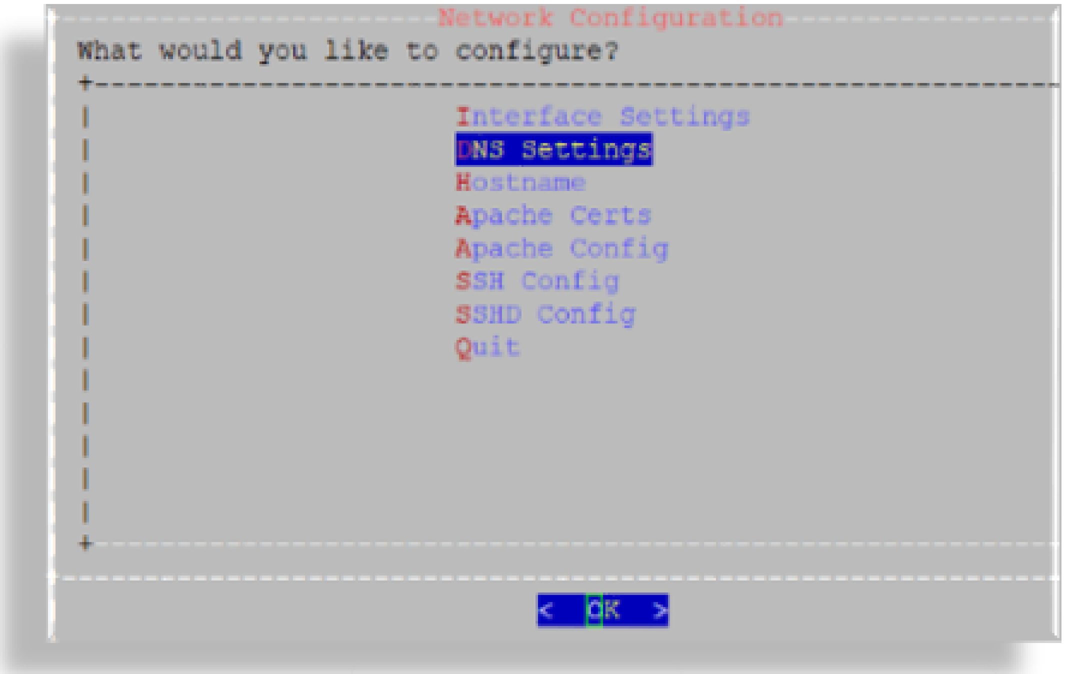


```
Configuring eth0.
Cannot advertise duplex full
Cannot set new settings: Operation not supported
  not setting duplex
  not setting autoneg
Cannot advertise duplex full
Cannot set new settings: Operation not supported
  not setting duplex
  not setting autoneg
Notifying network services of new parameters.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

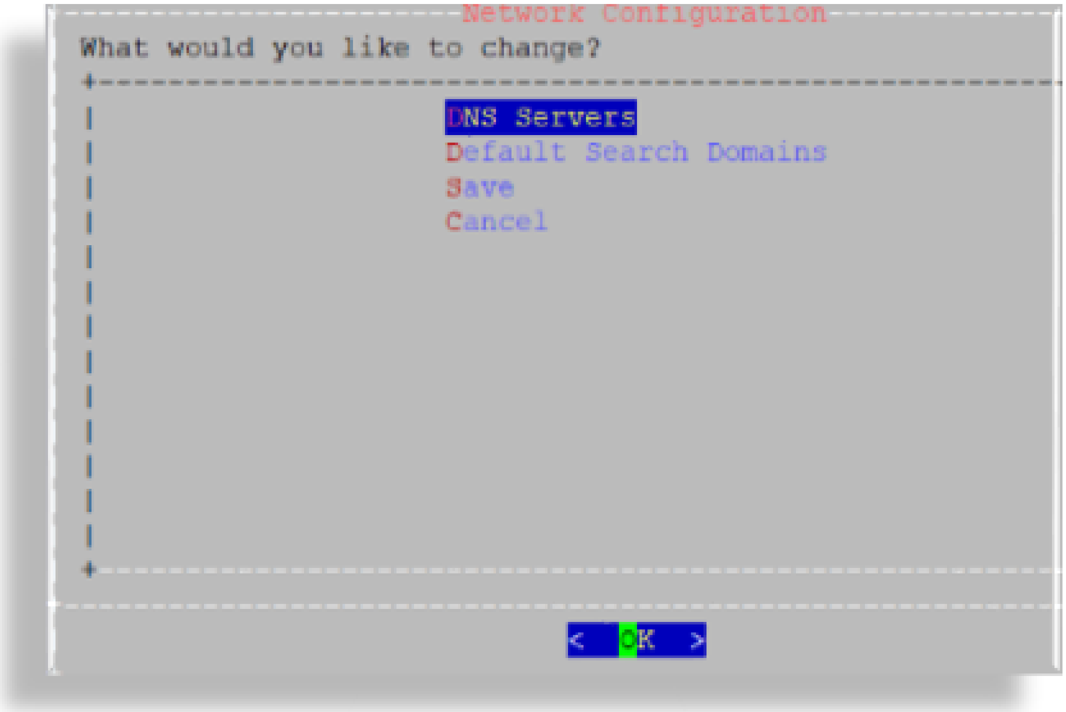
v. Save your changes.

3. Configure DNS settings:

i. Select **DNS Settings**

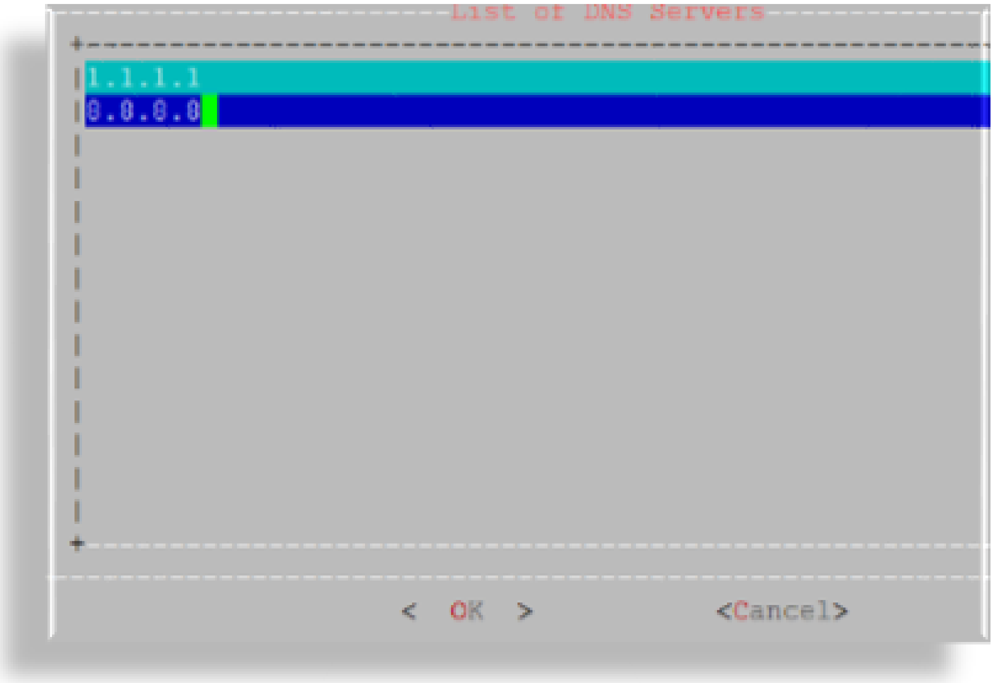


ii. Select **DNS Servers**.



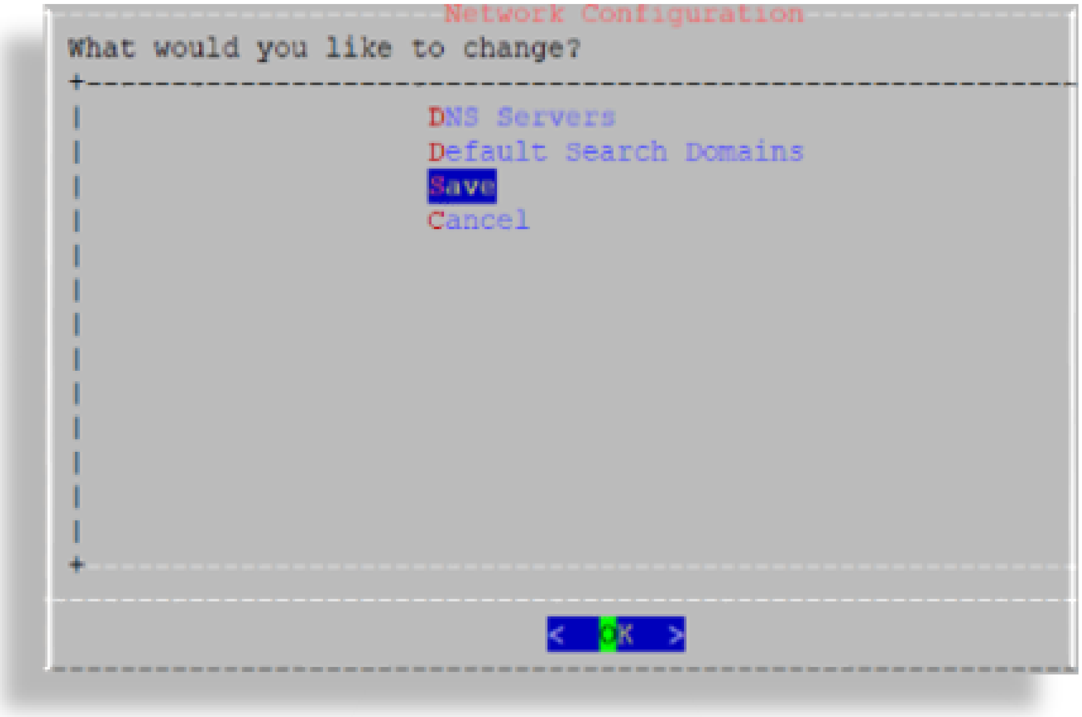
What would you like to change?

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



```
1.1.1.1
8.8.8.8
```

iv. Click **Save**.

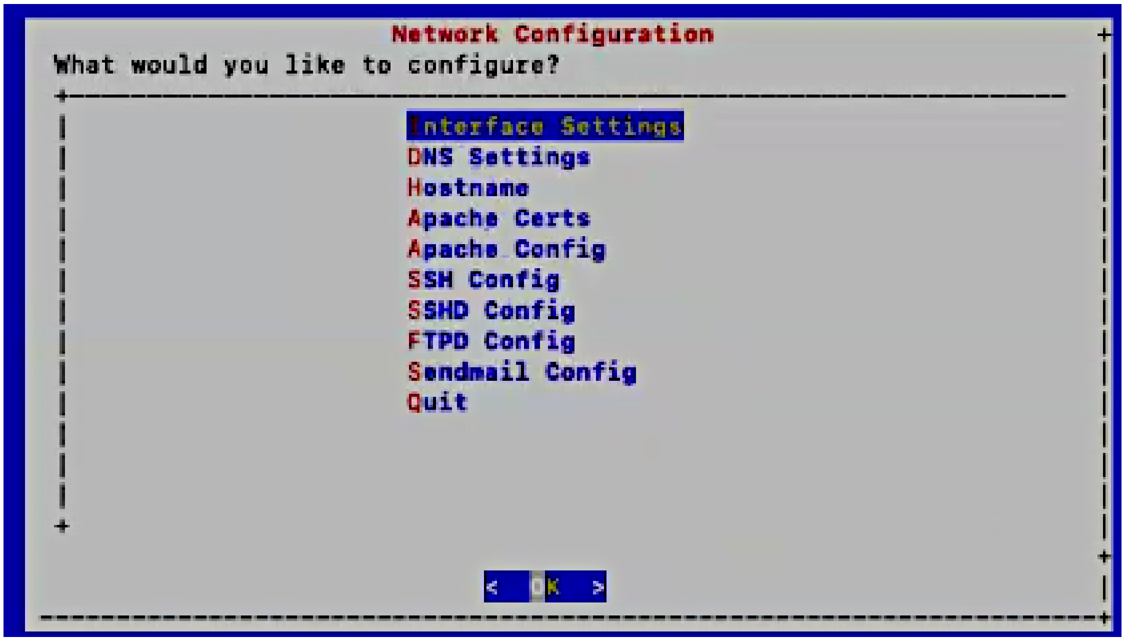


Network Configuration

What would you like to change?

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

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



Network Configuration

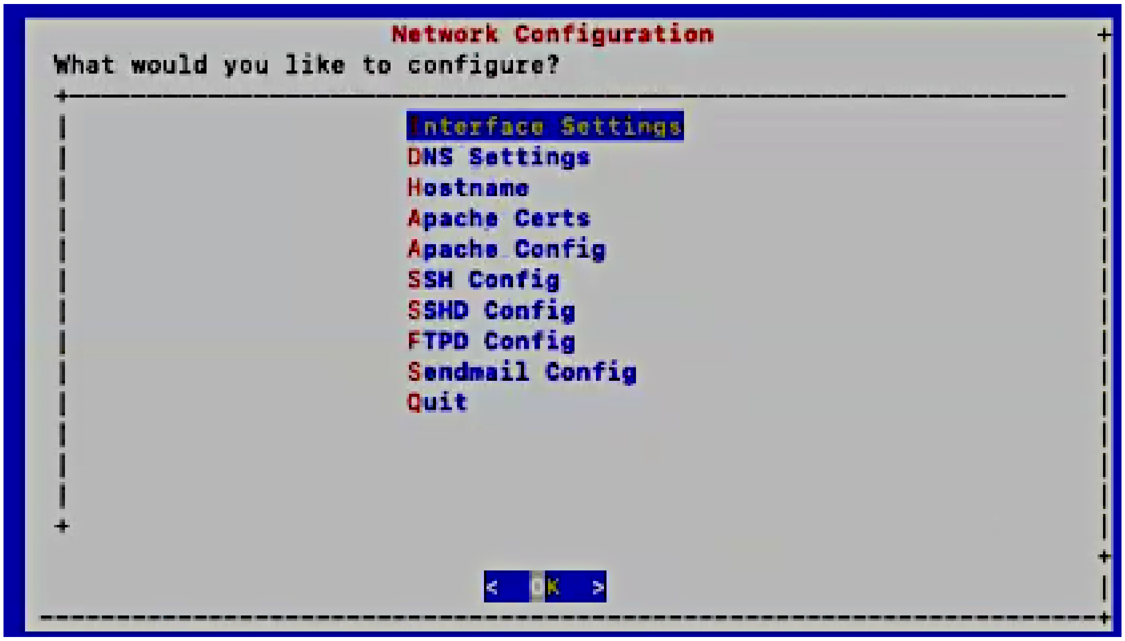
What would you like to configure?

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

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

Note:

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



Network Configuration

What would you like to configure?

6. Configure SSH settings:

   i. Select **SSH Config**.

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

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

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

7. Configure SSHD:

   i. Select **SSHD Config**.

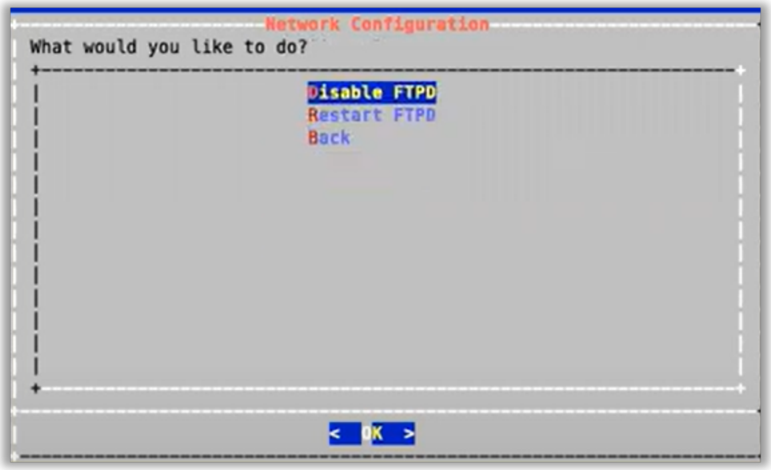
Note:

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

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

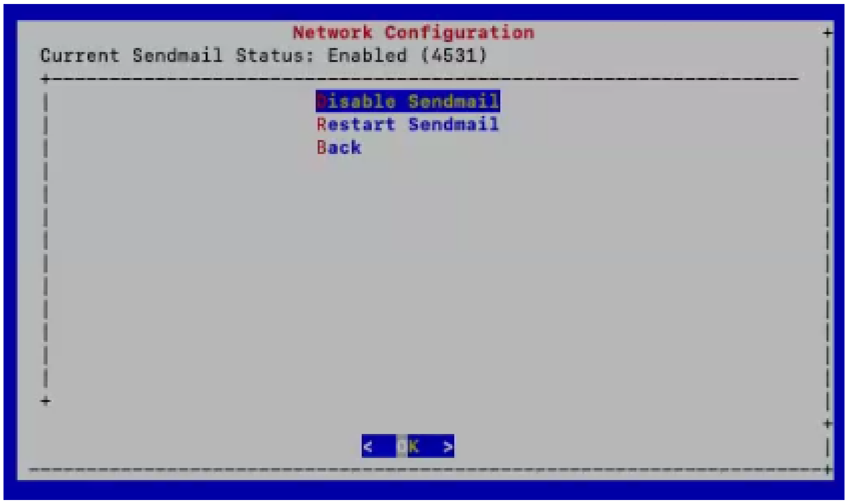
    1. Select **FTPD Config**.

Important: On new installs, the FTPD daemon is disabled by default. It is strongly recommended that the FTPD daemon remains disabled, unless there is a good reason you need to use it. It has been seen that enabling the FTPD daemon may introduce a system vulnerability. FTPD is typically *only* required in rare situations, where FTP is the only way to transfer files to the server. Instead of using FTPD, it is recommended that you use the drop account with SCP or SFTP. The drop account username is “drop”. You can set the password via the **Administration** menu.



What would you like to do?

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



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

   i. Select **Sendmail Config**. The current status of the service displays on the menu.
   ii. Choose to enable, disable, or restart the service as required.

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

Next steps

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

Step 7: Create GUI admin password for Arbitrator and Dashboard

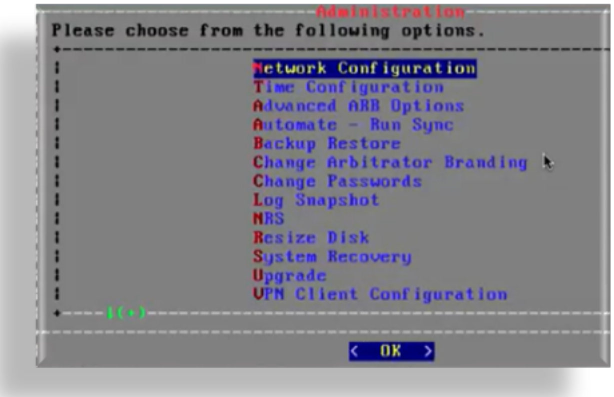
This procedure creates the GUI admin password, which is the password you will need to log in to Arbitrator or Dashboard via the browser.

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

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

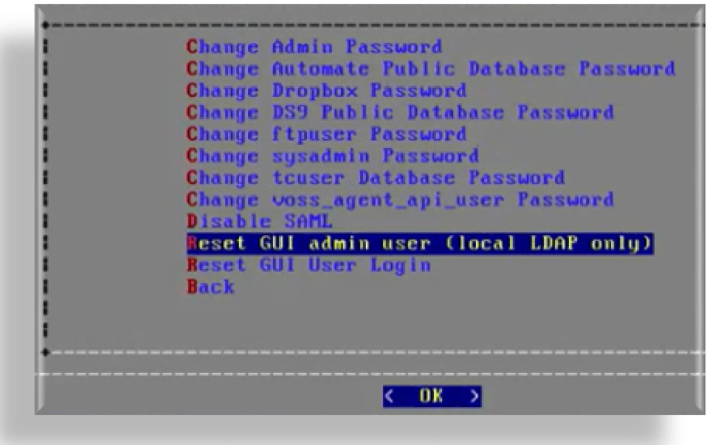
The steps to create the GUI admin password for Arbitrator and Dashboard are the same.

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



```
Administration
Please choose from the following options.

                    Network Configuration
                    Time Configuration
                    Advanced ARB Options
                    Automate - Run Sync
                    Backup Restore
                    Change Arbitrator Branding
                    Change Passwords
                    Log Snapshot
                    NRS
                    Resize Disk
                    System Recovery
                    Upgrade
                    VPN Client Configuration
    ↓(+)

                              < OK >
```

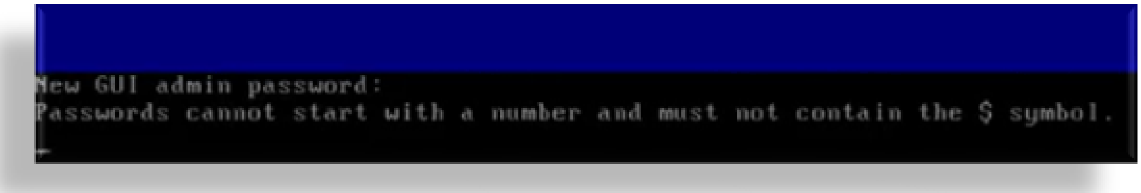
2. Select **Reset GUI admin user (local LDAP only)**.



```
                Change Admin Password
                Change Automate Public Database Password
                Change Dropbox Password
                Change DS9 Public Database Password
                Change ftpuser Password
                Change sysadmin Password
                Change tcuser Database Password
                Change voss_agent_api_user Password
                Disable SAML
                Reset GUI admin user (local LDAP only)
                Reset GUI User Login
                Back

                              < OK >
```

3. Fill out a new GUI admin password.

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



```
New GUI admin password:
Passwords cannot start with a number and must not contain the $ symbol.
```

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

Next steps

- *Product registration and system configuration*

6.1.2. Product registration and system configuration

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

- Insights Arbitrator (relevant only to an Insights Assurance solution and its integration with Cisco UC systems)

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

- Insights DS9

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

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

6.1.3. Configure multi-line CUCM cipher support

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

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

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

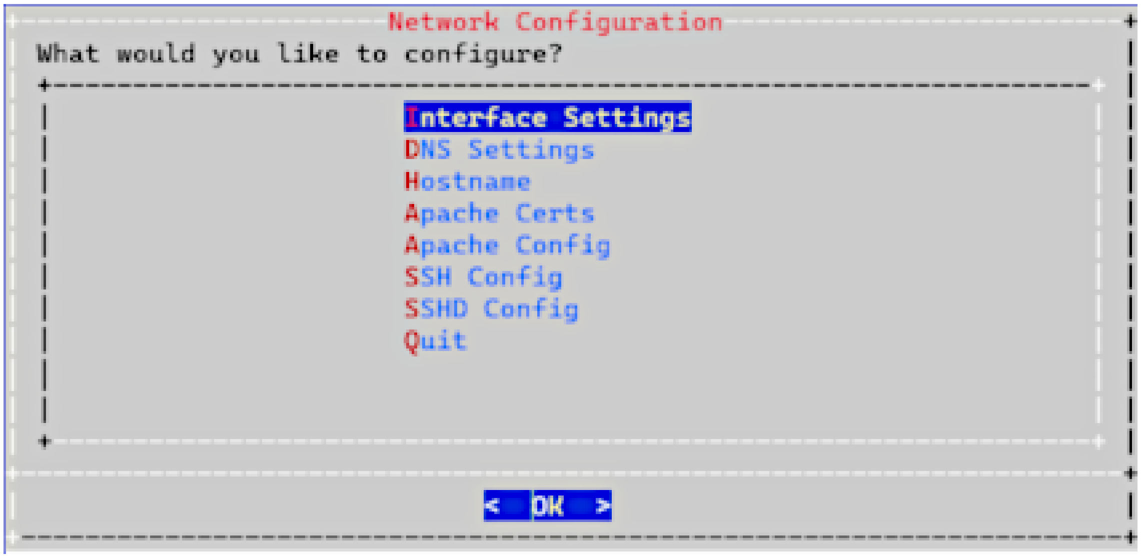
For CUCM v11.5 support:

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

7. Certificates

7.1. 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  >
```

7.1.1. Add certificates

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

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

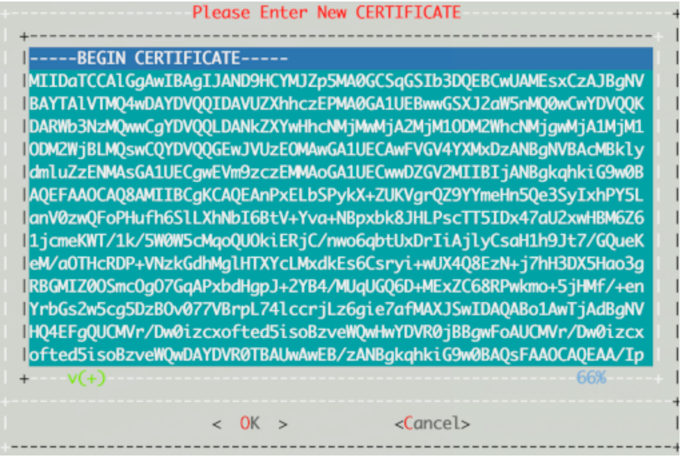
   A certificate has the following headers and footers:

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

(continues on next page)

(continued from previous page)

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



```
-----BEGIN CERTIFICATE-----
MIIDaTCCAlGgAwIBAgIJAND9HCYMJZp5MA0GCSqGSIb3DQEBCwUAMEsxCzAJBgNV
BAYTAlVTMQ4wDAYDVQQIDAVUZXhhczEPMA0GA1UEBwwGSXJ2aW5nMQ0wCwYDVQQK
DARWb3NzMQwwCgYDVQQLDANkZXYwHhcNMjMwMjA2MjM1ODM2WhcNMjgwMjA1MjM1
ODM2WjBLMQswCQYDVQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBkly
dmluZzENMAsGA1UECgwEVm9zczEMMAoGA1UECwwDZGV2MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAnPxELbSPykX+ZUKVgrQZ9YYmeHn5Qe3SyIxhPY5L
anV0zwQFoPHufh6SlLXhNbI6BtV+Yva+NBpxbk8JHLPscTT5IDx47aU2xwHBM6Z6
1jcmeKWT/1k/5W0W5cMqoQUOkiERjC/nwo6qbtUxDrIiAjlyCsaH1h9Jt7/GQueK
eM/aOTHcRDP+VNzkGdhMglHTXYcLMxdkEs6Csryi+wUX4Q8EzN+j7hH3DX5Hao3g
RBGMIZ0OSmcOg07GqAPxbdHgpJ+2YB4/MUqUGQ6D+MExZC68RPwkmo+5jHMf/+en
YrbGs2w5cg5DzBOv077VBrpL74lccrjLz6gie7afMAXJSwIDAQABo1AwTjAdBgNV
HQ4EFgQUCMVr/Dw0izcxofted5isoBzveWQwHwYDVR0jBBgwFoAUCMVr/Dw0izcx
ofted5isoBzveWQwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAA/Ip
```

Error checking and solutions:

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

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

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

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

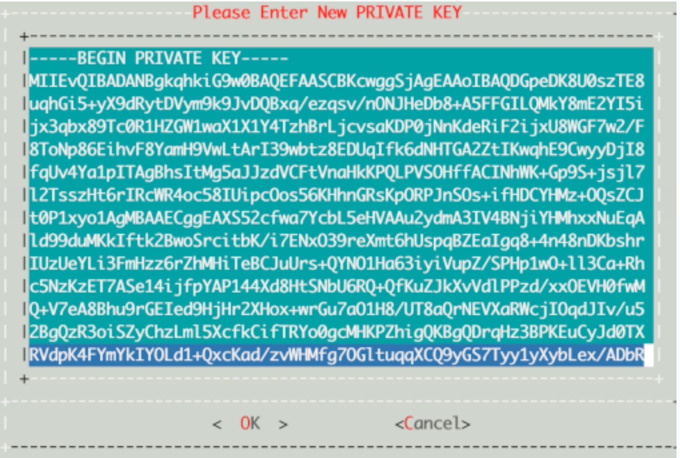
-
  ```
  Error loading file /etc/apache2/server.crt.tmp
  error:05800088:x509 certificate routines unknown function):
  no certificate or crl found:crypto/x509
  ```

  No certificate; invalid format; or blank.

6. Select **Insert Private Key**.
7. Paste in customer private key.

   A private key has the following header and footer

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



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

7.1.2. Generate a CSR from an existing certificate

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

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

7.1.3. Create new certificates

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

1. SSH to the system using admin account
2. Select **Network Configuration**
3. Select **Apache Certs**
4. Select **Generate New Unsigned Cert**
5. When prompted, fill in the information requested.
    - For `the number of days the certificate should be valid. (default 365):`, the value should be a positive number from 1 to 3650.

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

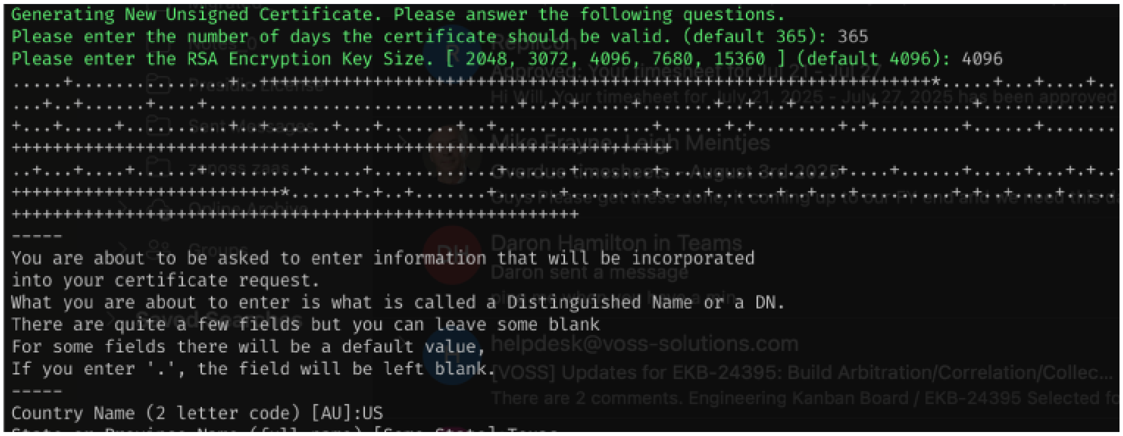
Self-Signed Certificates: When you are using OpenSSL to create a certificate for a private network or for testing purposes, you can set a much longer validity period. The tool itself does not prevent you from setting a very high number of days, but you may run into issues with the system's date and time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

- The default RSA Encryption Key Size is 4096.

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

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

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



```
Generating New Unsigned Certificate. Please answer the following questions.
Please enter the number of days the certificate should be valid. (default 365): 365
Please enter the RSA Encryption Key Size. [ 2048, 3072, 4096, 7680, 15360 ] (default 4096): 4096
.....+...............+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+...+....+..
...+..+......+....+...........................+..+.+.....+.......+..+..+.......+........+............
+...+.....+...............+..+.......+...+.......+..+................+.......+.+........+.+.........+......+.......
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+...+....+.......+.........+.....+.........................................+....+......+.....+...+.+..
+++++++++++++++++++++++++++*......+.+..+.......+.........+.........+.....+..........+...+..+....+.+..+.....+.....
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----
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]:US
```

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

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

Index