

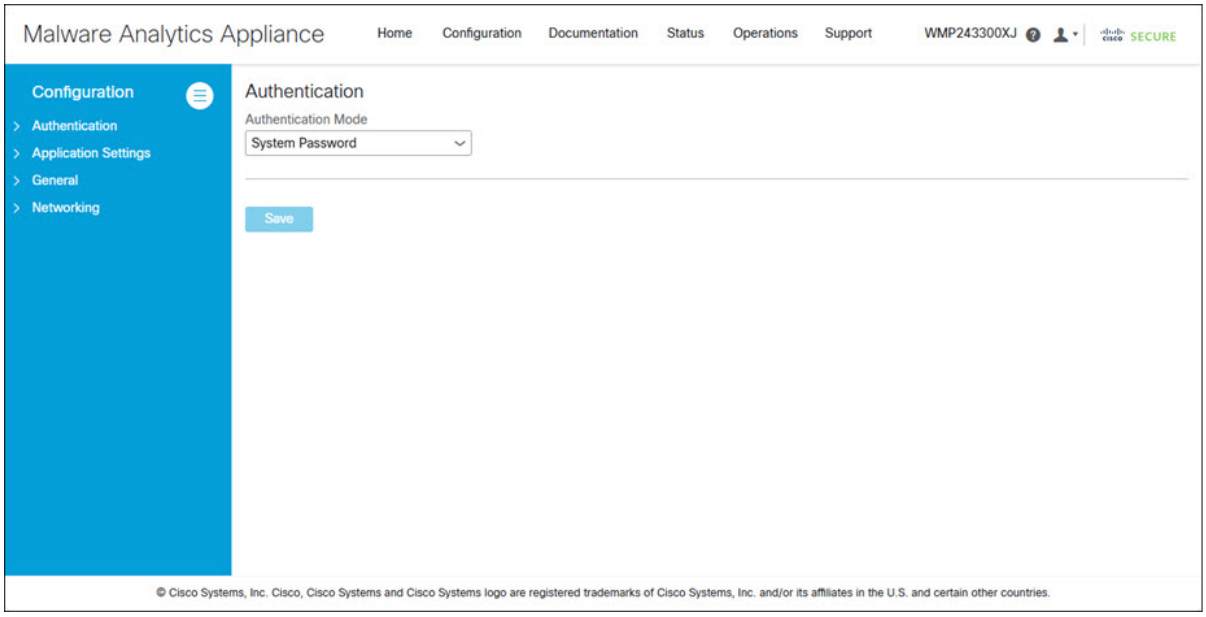
Configuration

The initial setup and configuration wizard is described in the Cisco Threat Grid Appliance Getting Started Guide. Secure Malware Analytics Appliance requires the administrator to complete additional configuration, and OpAdmin settings require updates over time. This chapter provides information about using the OpAdmin to make configuration changes to your appliance.

- Configuration, on page 1
- Applying Configuration Changes, on page 3
- Authentication, on page 5
- Application Settings, on page 19
- General, on page 27
- Networking, on page 32

Configuration

Figure 1: Configuration



The **Configuration** menu in the OpAdmin is used to configure and manage various Secure Malware Analytics Appliance configuration settings, including:

Section	Description
Authentication	
Authentication	Describes how to configure LDAP and RADIUS authentication for logging into the Secure Malware Analytics Appliance OpAdmin.
CA Certificates	Describes how to add CA certificate for outbound SSL connections for the appliance to trust the Cisco Secure Endpoint Private Cloud.
Password	Describes how to change your OpAdmin password.
SSH Configuration, on page 11	Describes how to configure SSH to setup some key elements via SSH.
SSH Keys, on page 12	Describes how to set up SSH keys to provide access to the Admin TUI via SSH.
SSL	Describes how to configure SSL certificates to support Secure Malware Analytics Appliance connections with Email Security Appliance (ESA), Web Security Appliance (WSA), Secure Endpoint Private Cloud, and other integrations; replacing SSL certificates.
Application Settings	
Integrations	Describes how to configure third-party detection and enrichment services (OpenDNS, TitaniumCloud, VirusTotal); enable or disable ClamAV automatic updates.
License	Describes how to upload your Secure Malware Analytics Appliance license or retrieve it from the server.
Network Exit	Describes how to configure the network exit options that are available in the Secure Malware Analytics portal when submitting samples for analysis.
Updates Proxy, on page 26	Describes how to configure the SOCKS5 proxy to download the updates.
General	
Content Update, on page 27	Describes how to enable Content Update.
Date and Time	Describes how to add Network Time Protocol (NTP) server to configure date and time.
Email	Describes how to configure your email settings (SMTP) for system notifications.
Notifications	Describes how to manage notification recipients.
Syslog	Describes how to configure a system log server to receive syslog messages and notifications.
Networking	

Section	Description
Network	Describes how to adjust the IP assignment from DHCP to your permanent static IP addresses, and how to configure DNS.
NFS	Describes appliance backup, including NFS requirements, backup storage requirements, backup expectations, and configuring the strict retention period limits; how to perform a backup.
Clustering	Describes features, limitations, and requirements of clustering Secure Malware Analytics Appliances; network and NFS storage requirements; how to build a cluster, join appliances to the cluster, remove cluster nodes, and designate a tie-breaker node; failure tolerances and failure recovery; API and operational usage and characteristics for clusters, and sample deletion.



Note

- Configuration updates in the OpAdmin should be completed in one session to reduce the chance of an interruption to the IP address during configuration.
- The OpAdmin does not validate the gateway entries. If you enter the wrong gateway and save it, the OpAdmin will not be accessible. You will need to use the console to fix the networking configuration if that was done on the Admin interface. If Admin is still valid, you can fix it in the OpAdmin and reboot.
- Secure Malware Analytics uses the serial number as the hostname to improve interoperability with some NFS v4 servers.



Important The OpAdmin uses HTTPS and you must enter this in the browser address bar; pointing to only the Admin IP is not sufficient. Enter the following address in your browser:

https://adminIP/

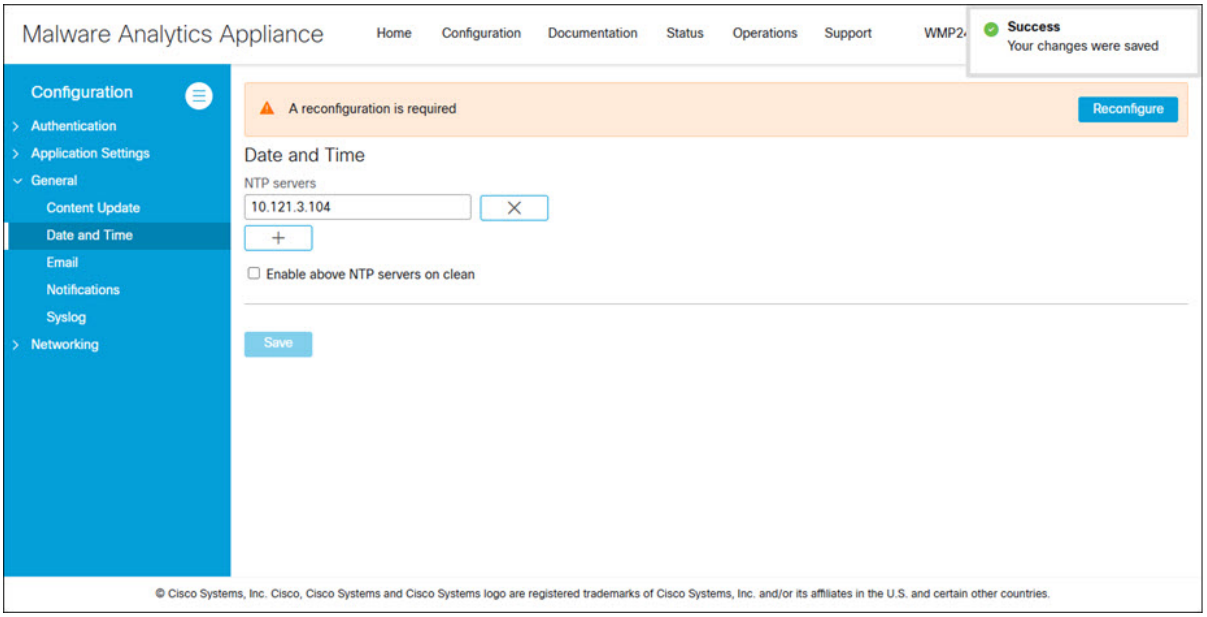
OR

https://adminHostname/

Applying Configuration Changes

Any time changes are made to configuration settings, a light orange alert message appears in a banner in the upper portion of the **Configuration** page.

Figure 2: Reconfigure Required Alert Message



After modifying configuration settings in the OpAdmin, you must first save your changes. While some settings require an additional activation step, all changes must ultimately be finalized through a separate reconfiguration process. Configuration changes do not take effect until this reconfiguration is complete. On some occasions, a reboot is necessary following a reconfiguration. If both a reboot and reconfiguration banner are present, the reconfiguration must be executed before the reboot.

Note Reconfiguration may affect other users logged in to Secure Malware Analytics portal and the OpAdmin.

Procedure

Step 1 Click **Reconfigure** on the alert message to launch the reconfiguration process. Otherwise to reconfigure, click **Operations** > **Activate**.

Step 2 On the **Activate Configuration** page, click **Reconfigure** to run the reconfiguration job.

Step 3 On the confirmation dialog, click **Reconfigure** to start the reconfiguration job.

Configuration is activated, and messages on its progress are displayed in the jobs window. Details are kept in the **Jobs** page if you need to review error messages or other information.

When completed, a confirmation message is displayed indicating the reconfiguration was successful.

Step 4 Click **Continue**.

Authentication

The Secure Malware Analytics Appliance supports LDAP authentication and authorization for logging into the OpAdmin and the Admin TUI. It also supports RADIUS authentication, which allows for single sign-on to the OpAdmin.



Important When configured for **LDAP Only** or **RADIUS Only** authentication mode, any loss of connectivity to the authentication server will result in a complete lockout from the appliance. To recover from an authentication lockout, use **Recovery Mode** to reset the administrator password and restore local authentication. Refer Resetting the Administrator Password for detailed instructions.

LDAP Authentication

The Secure Malware Analytics Appliance supports LDAP authentication and authorization for OpAdmin and Admin TUI login. You can authenticate multiple appliance administrators with different credentials that are managed on the domain controller or the LDAP server. Authentication modes include: System Password Only, System Password or LDAP, and LDAP Only.

There are three LDAP Protocol options: LDAP, LDAPS, and LDAP with STARTLS.

The following considerations should be observed:

- The dual authentication mode (**LDAP or System Password**) is required to avoid accidentally locking yourself out of the Secure Malware Analytics Appliance when setting up LDAP.

  Choosing **LDAP Only** is not allowed initially; you must first go through dual mode to make sure it works. You must log out of the OpAdmin after the initial configuration, and then log back in using LDAP credentials to toggle to **LDAP Only**.

- You can only log into the Admin TUI using LDAP if you are configured for **LDAP Only** authentication. If authentication mode is set to **LDAP or System Password**, the Admin TUI login only allows the System login.

- If the Secure Malware Analytics Appliance is configured for LDAP authentication only (**LDAP Only**), you can reset the password in recovery mode to reconfigure the authentication mode to also allow login with a system password.

- Make sure that the authentication filter is set up to restrict membership.

- The Admin TUI and the OpAdmin require LDAP credentials only in **LDAP Only** mode/ if **LDAP only** is configured, the Admin TUI only prompts for the LDAP user/password; not the system password.

- If authentication is configured for **System Password or LDAP** (or RADIUS), the Admin TUI supports dual mode. You can log in using either their LDAP/RADIUS credentials or the local system password.

- To troubleshoot LDAP issues, disable it by resetting the password in Recovery Mode.

- To access the Admin TUI via SSH, a system password or a configured SSH key is required in addition to LDAP credentials when in **LDAP Only** mode.

- LDAP is outbound from the Clean interface.

Perform the following steps to configure LDAP authentication in the OpAdmin.

Procedure

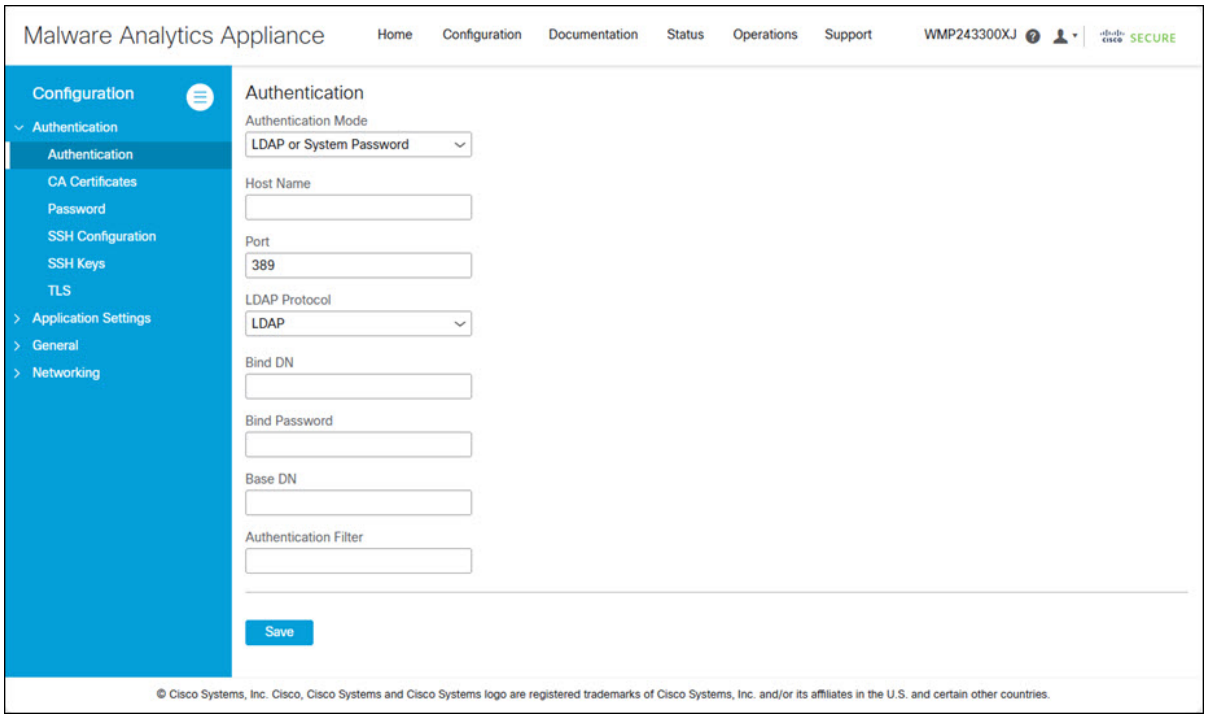
Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **Authentication**.

Step 3 From the **Authentication Mode** drop-down, choose **LDAP or System Password** to open the LDAP configuration page.

Note
The first time you configure LDAP authentication, you must choose **LDAP or System Password**, log out of the OpAdmin, and then log back in using your LDAP credentials. You can then change the setting to **LDAP**.

Figure 3: LDAP Authentication Configuration Page



Step 4 Complete the fields on the page as appropriate:

- **Hostname** - The host name to connect to via LDAP.
- **Port** - The port number to connect to via LDAP (default 389).
- **Authentication Mode** - The authentication mode to be used upon login.
- **LDAP Protocol** - The LDAP protocol in use.
- **Bind Password** - The password to use for binding via LDAP.
- **Bind DN** -The Distinguished Name to bind to via LDAP; for example: cn=admin,dc=foo,dc=com.
- **Base** - The base to bind to via LDAP; for example: ou=users,dc=foo,dc=com (LDAP only).

- **Authentication Filter** - The filter to be applied for authentication upon login; for example: (&(cn=%LOGIN%)(memberOf=cn=admingroup, ou=groups,dc=foo,dc=com)).

Step 5 Click **Save**.

When users log in to the OpAdmin or Admin TUI, they will now be prompted for their LDAP authentication.

RADIUS Authentication

Secure Malware Analytics Appliance supports RADIUS authentication, which uses Cisco Identity Services Engine with DTLS enabled. If RADIUS authentication is enabled, users can log in to the main Secure Malware Analytics application UI and OpAdmin with the appropriate single sign-on password.

The following considerations should be observed:

- The dual authentication mode (**RADIUS or System Password**) is required to avoid accidentally locking yourself out of the Secure Malware Analytics Appliance when setting up RADIUS.

  Choosing **RADIUS Only** is not allowed initially; you must first go through dual mode to make sure it works. You must log out of the OpAdmin after the initial configuration, and then log back in using RADIUS credentials to toggle to **RADIUS Only**.

- You can only log into the Admin TUI using RADIUS if you are configured for **RADIUS Only** authentication. If authentication mode is set to **RADIUS or System Password**, the Admin TUI login only allows the System login.

- If the Secure Malware Analytics Appliance is configured for RADIUS authentication only (**RADIUS Only**), you can reset the password in recovery mode to reconfigure the authentication mode to also allow login with a system password.

- The Admin TUI and the OpAdmin require RADIUS credentials only in **RADIUS Only** mode/ if **RADIUS only** is configured, the Admin TUI only prompts for the RADIUS user/password; not the system password.

- If authentication is configured for **System Password or LDAP** (or RADIUS), the Admin TUI supports dual mode. You can log in using either their LDAP/RADIUS credentials or the local system password.

- To troubleshoot RADIUS issues, disable it by resetting the password in Recovery Mode.

- To access the Admin TUI via SSH, a system password or a configured SSH key is required in addition to RADIUS credentials when in **RADIUS Only** mode.

- RADIUS is outbound from the Clean interface.

Perform the following steps in the OpAdmin to configure RADIUS authentication:

Procedure

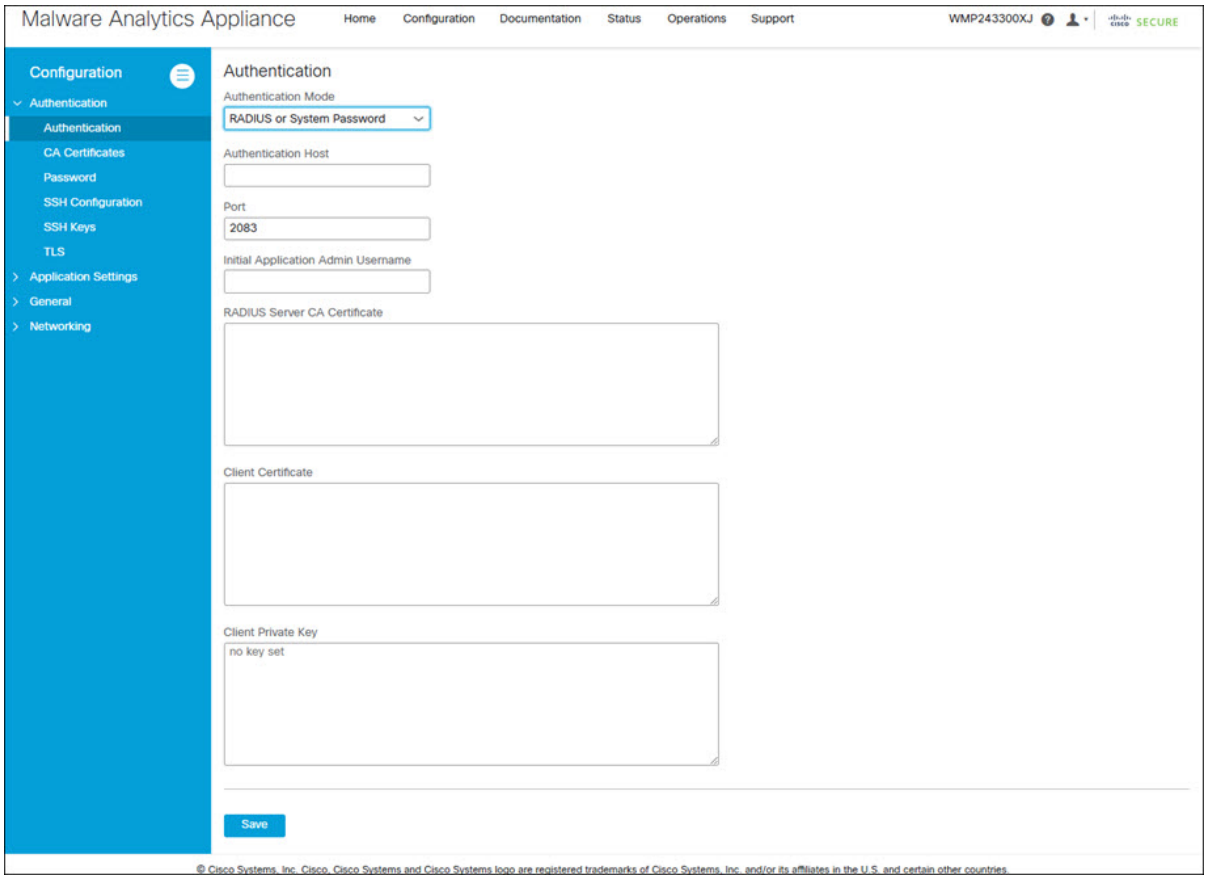
Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **Authentication**.

Step 3 From the **Authentication Mode** drop-down, choose **RADIUS or System Password** to open the RADIUS configuration page.

Note
The first time you configure RADIUS authentication, you must choose **RADIUS or System Password**, log out of the OpAdmin, and then log back in using your RADIUS credentials. You can then change the setting to **RADIUS**. Logging in a second time after RADIUS and system password is configured ensures that RADIUS configuration is validated before removing system password as a fallback login method.

Figure 4: RADIUS Authentication Configuration Page



Step 4 Complete the fields on the page as appropriate:

- **Hostname** - The host name to connect to via RADIUS.
- **Port** - The DTLS port number to connect to via RADIUS (default 2083). Unlike conventional RADIUS, DTLS uses a single port for both authentication and accounting. Only DTLS-based RADIUS authentication is supported.
- **Initial Face Admin** - The RADIUS user to whom the initial/default administration user in the primary Secure Malware Analytics UI shall be mapped. This account should be the party responsible for creating other user accounts in Secure Malware Analytics and configuring their permissions.
- **CA Certificate** - A PEM-format CA certificate to be used to authenticate the RADIUS server used for authentication. Will change to <VALID> when successfully saved. Clear this to empty the field.
- **Client Certificate** - A PEM-format client certificate to be used to authenticate this host to the RADIUS server used for authentication. This value will change to <VALID> when successfully saved; you can clear it to empty the field.

- **Client Private Key** - A PEM-format key to be used to authenticate this host to the RADIUS server used for authentication. The value must correspond with the client certificate given above. The value will change to <VALID> when successfully saved; you can clear it to empty the field. Private keys in PEM-encoded PKCS#8 format are supported by the OpAdmin.

Step 5 Click **Save**.

Note

`NAS-Identifier` is sent in the authentication requests from the Security Malware Analytics application UI and OpAdmin.

- `NAS-Identifier` sent in authentication requests from SMA portal is: `Threat Grid UI`.
- `NAS-Identifier` sent in authentication requests from OpAdmin is: `Threat Grid Admin`.

For more information on the specific values sent through the `NAS-identifier`, refer to https://www.rfc-editor.org/rfc/rfc2865.html#section-5.32.

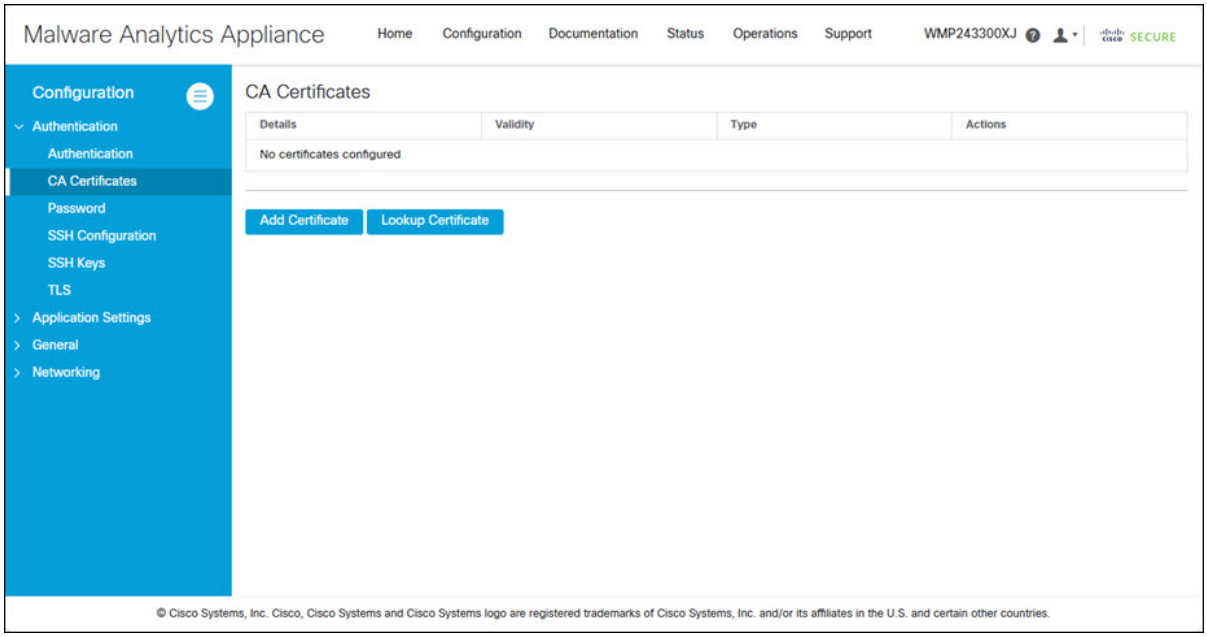
CA Certificates

The **CA Certificates** page in the OpAdmin is used to manage the Certificate Authority (CA) certificate trust store for outbound SSL connections so that the Secure Malware Analytics Appliance can trust the Cisco Secure Endpoint Private Cloud to notify it about analyzed samples that are considered malicious.

Procedure

Step 1 Navigate to **Configuration** > **Authentication** > **CA Certificates**

Figure 5: CA Certificates Page



Step 2 Create a **.pem** file that contains the outbound SSL connections (CA certificates) for the Secure Endpoint Private Cloud, copy the contents, and paste it into the **Certificate** field.

Step 3 Click **Add Certificate** and confirm. Changing a CA certificate does not require reconfiguration.

Password

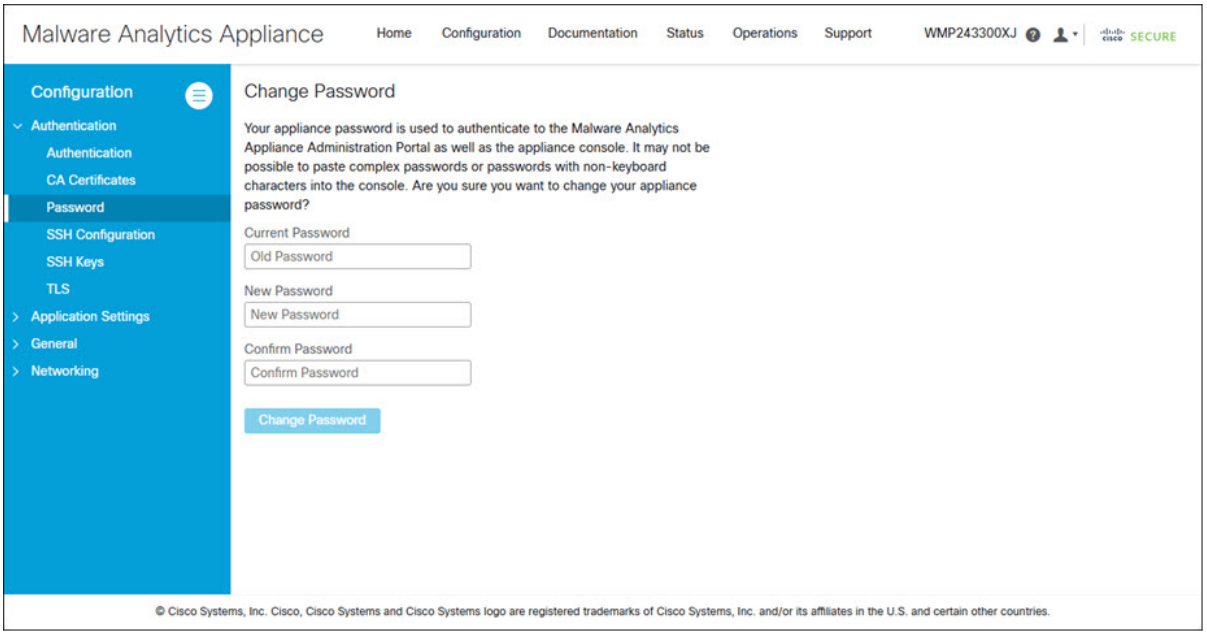
Your appliance password is used to authenticate to the Secure Malware Analytics Appliance OpAdmin as well as the appliance console. You can change your password from the OpAdmin using the **Password** page.

Note It may not be possible to paste complex passwords or passwords with non-keyboard characters into the console so be careful when you change your password.

Procedure

Step 1 Navigate to **Configuration** > **Authentication** > **Password**

Figure 6: Password



Step 2 Enter your **`Current Password`**, and then enter the **`New Password`** and **`Confirm Password`**.

Step 3 Click **Change Password** and confirm the change. Changing a password does not require reconfiguration.

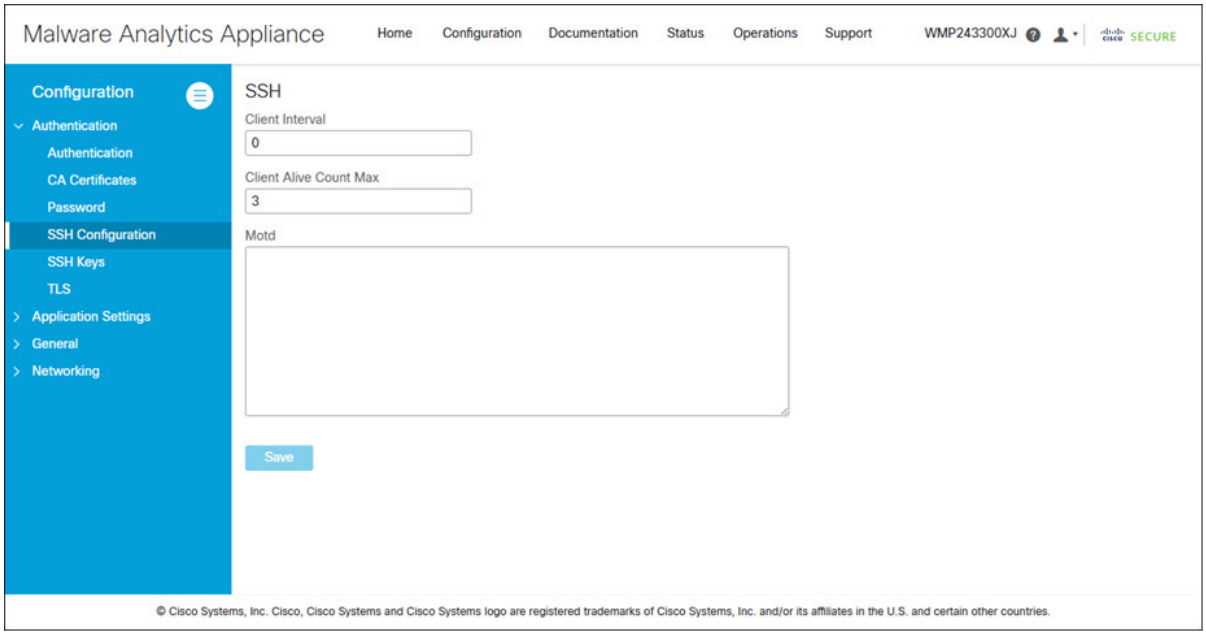
SSH Configuration

Setting up SSH Configuration provides the Secure Malware Analytics Appliance administrator with access to set the *ClientAliveInterval*, *ClientAliveCountMax*, and *motd* (Message of the Day) on your appliance using the **SSH Configuration** page in the OpAdmin.

Procedure

Step 1 Navigate to **Configuration** > **Authentication** > **SSH Configuration**

Figure 7: SSH Configuration



Step 2 Enter the **Client Interval**. *Client Interval* or *ClientAliveInterval* - Sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.

Step 3 Enter the **Client Alive Count Max**. *Client Alive Count Max* or *ClientAliveCountMax* - Sets the number of client alive messages which is sent without SSH receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session.

Step 4 Enter the **Motd** (Message of the Day). It is used to display a message when a remote user login to the Secure Malware Analytics appliance using SSH.

SSH Keys

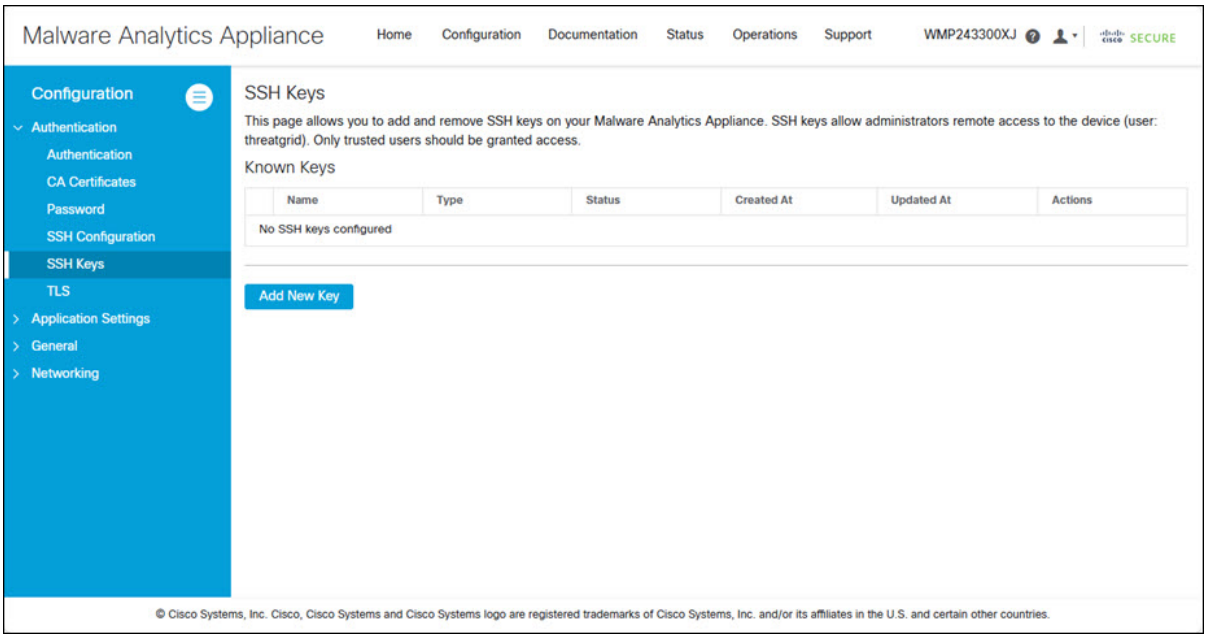
Setting up SSH keys provides the Secure Malware Analytics Appliance administrator with access to the Admin TUI via SSH (`threatgrid@<host>`); it does not provide root access or a command shell. You can add and remote SSH keys on your appliance using the **SSH Keys** page in the OpAdmin.

Note Configuring a SSH public key for access to the Secure Malware Analytics Appliances disables password-based authentication via SSH; this makes SSH authentication methods one or the other, not both. After a successful SSH connection using key-based authentication, the Admin TUI prompts for a password, such that both tokens are required.

Procedure

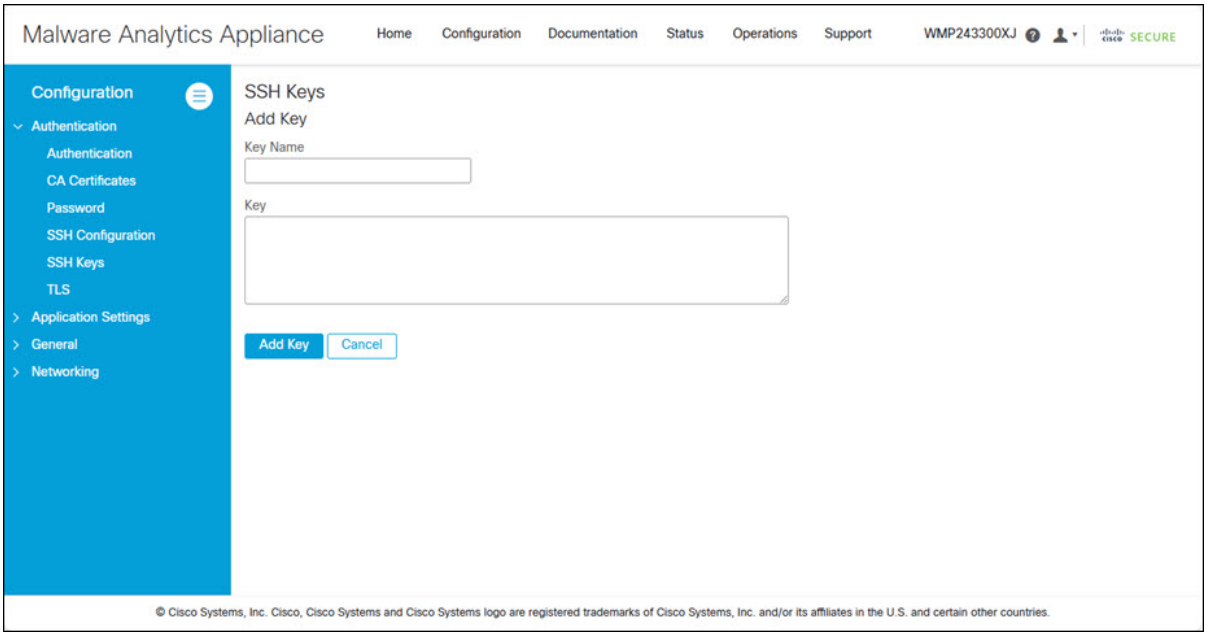
Step 1 Navigate to **Configuration** > **Authentication** > **SSH Keys**

Figure 8: SSH Keys



Step 2 Click **Add New Key**.

Figure 9: Add Key



Step 3 Enter the **Key Name** and paste the key into the **Key** field.

Step 4 Click **Add Key**.

TLS

All network traffic passing to and from the Secure Malware Analytics Appliance is encrypted using TLS. The following information is provided to assist you through the steps for setting up TLS certificates to support Secure Malware Analytics Appliance connections with Email Security Appliance (ESA), Web Security Appliance (WSA), Secure Endpoint Private Cloud, and other integrations.

Note A full description of how to administer TLS certificates is beyond the scope of this guide.

Interfaces Using TLS

There are two interfaces on the Secure Malware Analytics Appliance that use TLS:

- **Clean** interface for the Secure Malware Analytics Portal UI and API, and integrations (ESA, WSA, and Secure Endpoint Private Cloud Disposition Update Service).
- **Admin** interface for the OpAdmin.

Supported TLS Version

The following versions of TLS are supported on the Secure Malware Analytics Appliance:

- TLS v1.0 - Disabled in the Admin interface
- TLS v1.1 - Disabled in the Admin interface
- TLS v1.2

Note TLS v1.0 and TLS v1.1 are disabled in the Admin interface, and disabled by default for the main application. If one of these protocols is required for integration compatibility purposes, they can be re-enabled (for the main application only) from tgsh.

Supported Customer-Provided CA Certificates

Customer-provided CA certificates are supported to allow customers to import their own trusted certificates or CA certificates.

Self-Signed Default TLS Certificates

The Secure Malware Analytics Appliance is shipped with a set of self-signed TLS certificates and keys already installed. One set is for the Clean interface and the other is for the Admin interface. These TLS certificates can be replaced by an administrator.

The default Secure Malware Analytics Appliance TLS certificate hostname (Common Name) is the appliance serial number (with an additional subjectAltName field for the IP address), and is valid for 1 year. For releases prior to v2.11, the default TLS certificate hostname is **pandem**.

If a different hostname was assigned to the Secure Malware Analytics Appliance during configuration, the hostname and the Common Name in the certificate will no longer match.

The hostname in the certificate must also match the hostname expected by a connecting an ESA or WSA, or other integrating Cisco device or service, as many client applications require TLS certificates where the Common Name used in the certificate matches the hostname of the connecting appliance.

Configuring TLS Certificates

Cisco security products, such as ESA, WSA, and Secure Endpoint Private Clouds, can connect to a Secure Malware Analytics Appliance (inbound connection) and submit samples to it. To accomplish this, the connected appliance or other device must be able to trust the Secure Malware Analytics Appliance TLS certificate.

You must first validate that the hostname matches the Common Name; if it doesn't match, you must regenerate or replace it. You then must export the TLS certificate from the Secure Malware Analytics Appliance, and then import it into the connected appliance or device.

The certificates used for inbound TLS connections on the Secure Malware Analytics Appliance are configured on the **TLS Keys** page. The TLS certificates for the Clean and Admin interfaces can be configured independently.

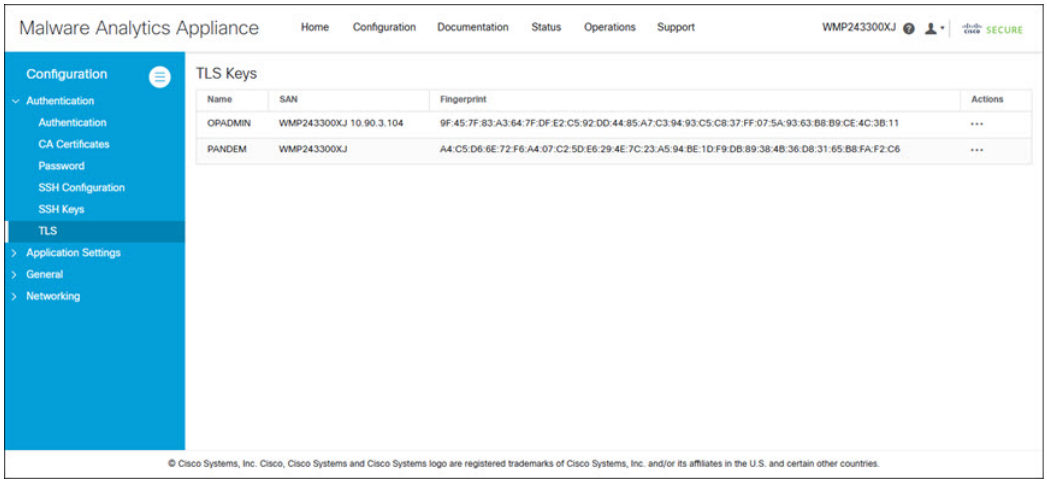
Note For information about outbound TLS connections so that the Secure Malware Analytics Appliance can trust the Cisco Secure Endpoint Private Cloud, see CA Certificates.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **TLS** to open the **TLS Keys** page.

Figure 10: TLS Keys Page



In this example, there are two TLS certificates: **OpAdmin** for the Admin interface, and **Pandem** for the Clean interface.

Step 3 Confirm that the hostname matches the SAN (Subject Alternative Name) used in the TLS. The hostname must match the SAN used in the TLS certificate on the Secure Malware Analytics Appliance. If they do not match, you can regenerate the TLS certificate. See Regenerating SSL Certificates.

Replacing TLS Certificates

TLS certificates usually need to be replaced at some point for various reasons, such as the certificate has expired, the hostname has changed, or to support integrations with other Cisco devices and services.

Cisco ESA, WSA, and other CSA Cisco integrating devices may require an TLS certificate in which the Common Name matches the Secure Malware Analytics appliance hostname. You must replace the default TLS certificate with a newly generated certificate that uses the same hostname to access the Secure Malware Analytics Appliance.

If integrating a Secure Malware Analytics Appliance with an Secure Endpoint Private Cloud to use its Disposition Update Service, you must install the Secure Endpoint Private Cloud TLS Certificate so the Secure Malware Analytics Appliance can trust the connection.

There are several ways to replace an TLS certificate on a Secure Malware Analytics Appliance:

- Regenerating TLS Certificates that uses the current hostname for the SAN.
- Downloading TLS Certificates
- Uploading TLS Certificates; this can be a commercial or enterprise TLS, or one you create using OpenSSL.
- Generating TLS Certificates Using OpenSSL

Regenerating TLS Certificates

You can regenerate a TLS certificate on the **TLS Keys** page if your hostname does not match the SAN in the certificate.

Procedure

Step 1 Navigate to **Configuration** > **Authentication** > **TLS**.

Step 2 In the **Actions** column, click the (**...**) menu and choose **Regenerate** for the interface that needs a new certificate.

A new self-signed TLS certificate is generated on the Secure Malware Analytics Appliance that uses the current hostname of the appliance in the SAN field of the certificate. The regenerated certificate (.cert file) can be downloaded and installed on the integrating appliance.

Downloading TLS Certificate

The Secure Malware Analytics generated TLS certificates, but not the keys, can be downloaded. A downloaded certificate can be used when setting up a cluster. It can also be installed on integrating devices so they can trust connections from the Secure Malware Analytics appliance. (You will only need to .cert file for this step.)

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **TLS** to open the **TLS Keys** page.

Step 3 From **Actions** (**...**) menu, choose **Download** for the appropriate interface. The TLS Certificate is downloaded.

Uploading TLS Certificates

If you already have a commercial or corporate TLS certificate in place for your organization, you can use that to generate a new TLS certificate for the Secure Malware Analytics Appliance and use the CA cert on the integrating device.

Procedure

Step 1 Navigate to **Configuration** > **Authentication** > **TLS**.

Step 2 In the **Actions** column, click the (**...**) menu and choose **Upload** for the appropriate interface. The **Upload TLS Certificate** page opens.

Step 3 Complete the **Certificate** and **Private Keys** fields and then click **Add Certificate**.

Generating TLS Certificates Using OpenSSL

OpenSSL is a standard open-source TLS tool for creating and managing OpenSSL certificates, keys, and other files. You can manually generate a TLS certificate using OpenSSL when there is no TLS certificate infrastructure already in place on your premises and upload it to the Secure Malware Analytics Appliance (as described in Uploading SSL Certificates). .

Note OpenSSL is not a Cisco product, therefore Cisco does not provide technical support for it. It is recommended that you search the Web for additional information on using OpenSSL. Cisco does offer a TLS library, *Cisco TLS*, for generating TLS certificates.

Procedure

Step 1 Run the following command to generate a new self-signed TLS certificate:

Note
The following example still uses the CN (Common Name) instead of the more contemporary SAN (Subject Alternative Name).

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout tgapp.key -nodes -out
tgapp.cert -subj "/C=US/ST=New York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

openssl - OpenSSL

req - Specifies to use X.509 certificate signing request (CSR) management. X.509 is a public key infrastructure standard that SSL and TLS use for key and certificate management. In this example, this parameter is used to create a new X.509 cert.

-x509 - This modifies the req parameter X.509 to make a self-signed certificate instead of generating a certificate signing request.

-days 3650 - This option sets the length of time for which the certificate will be considered valid. In this example, it is set for 10 years.

-newkey rsa:4096 - This specifies to generate a new certificate and a new key at the same time. Because the required key was not previously created, it must be created with the certificate. The **rsa:4096** parameter indicates to make an RSA key that is 4096 bits long.

-keyout - This parameter indicates where OpenSSl should save the generated private key file that is being created.

-nodes - This parameter indicates that OpenSSL should skip the option to secure the certificate with a passphrase. The appliance needs to be able to read the file, without user intervention, when the server starts up. A certificate that is secured with a passphrase requires that the user enter the passphrase every time the server is restarted.

-out - This parameter indicates where OpenSSL should save the certificate that is being created.

-subj: (Example):

- **C=US** - Country
- **ST=New York** - State
- **L=Brooklyn** - Location
- **O=Acme Co** - Owner's name
- **CN=tgapp.acmeco.com** - Enter the Secure Malware Analytics Appliance FQDN (Fully Qualified Domain Name). This includes the HOSTNAME of the Secure Malware Analytics Appliance (in this example, **tgapp**) and the associated domain name (in this example, **acmeco.com**).

  Important

You must at least change the Common Name to match the FQDN of the Secure Malware Analytics Appliance Clean interface.

Step 2 Once the new TLS certificate is generated, upload the certificate to the Secure Malware Analytics Appliance from the **TLS Keys** page (see Uploading SSL Certificates). You must also upload the certificate (**.cert** file only) to the Email Security Appliance or Web Security Appliance, if you are integrated with those devices.

Application Settings

The Secure Malware Analytics Appliance application settings are configured in this panel.

Integrations

Integrations with several third-party detection and enrichment services, including TitaniumCloud, Umbrella (OpenDNS), and VirusTotal, can be configured on the appliance using the **Integrations** page.

The Cloud Search Federation feature, provides users with an option in the Secure Malware Analytics portal UI to rerun a search query against the Secure Malware Analytics cloud instance, if a cloud endpoint is configured as described below.

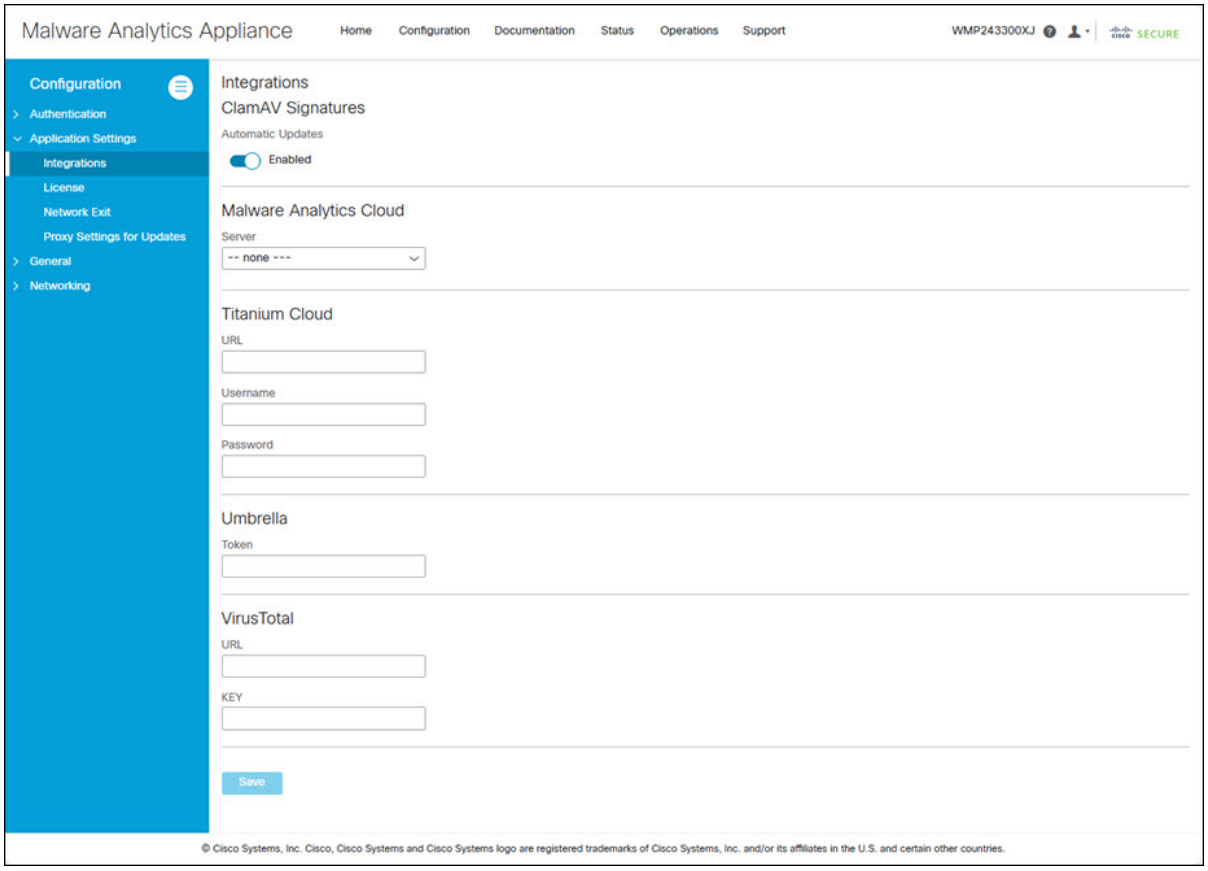


Note If Umbrella (OpenDNS) is not configured, the **whois** information on the Domains entity page in the analysis report (Cloud UI) will not be rendered.

Procedure

Step 1 Navigate to **Configuration** > **Application Settings** > **Integrations**.

Figure 11: Integrations Configuration Page



Integrations screen appears.

Step 2 Under Malware Analytics Cloud, select **US Cloud** or **EU Cloud**. Make sure you have an account on the selected cloud service (**US Cloud** or **EU Cloud**).

Note
By default, the Malware Analytics Cloud region is set to **None**. To enable cloud-based analysis, you must first perform an update check. For more information on performing an update check, see Update.

From Secure Malware Analytics (SMA) you have a provision to connect to the Secure Malware Analytics Cloud. Through the cloud connection, you can leverage **sample disposition lookup**. This functionality allows your SMA appliance to search a central database within the Secure Malware Analytics Cloud. This database stores information about previously analyzed files (samples) submitted by the entire SMA user community.

Figure 12: Samples dashboard - Secure Malware Analytics Cloud link

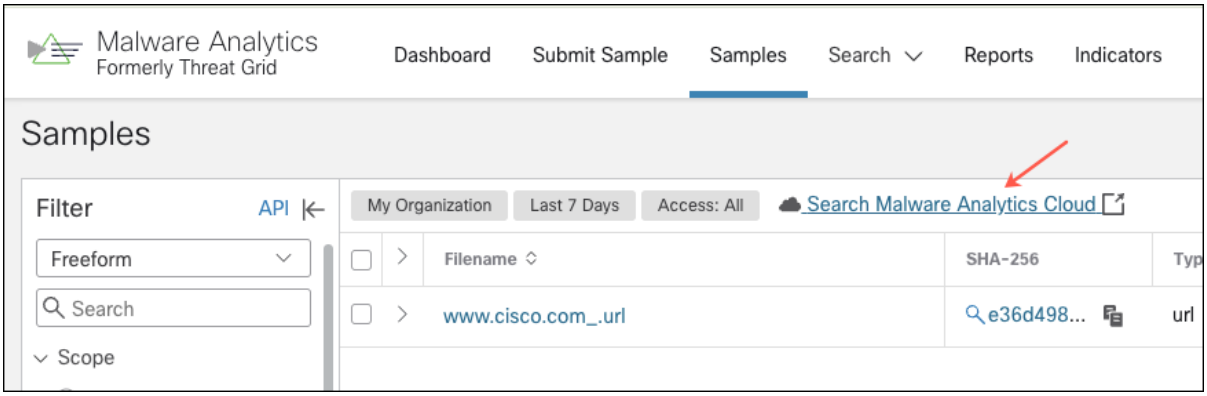
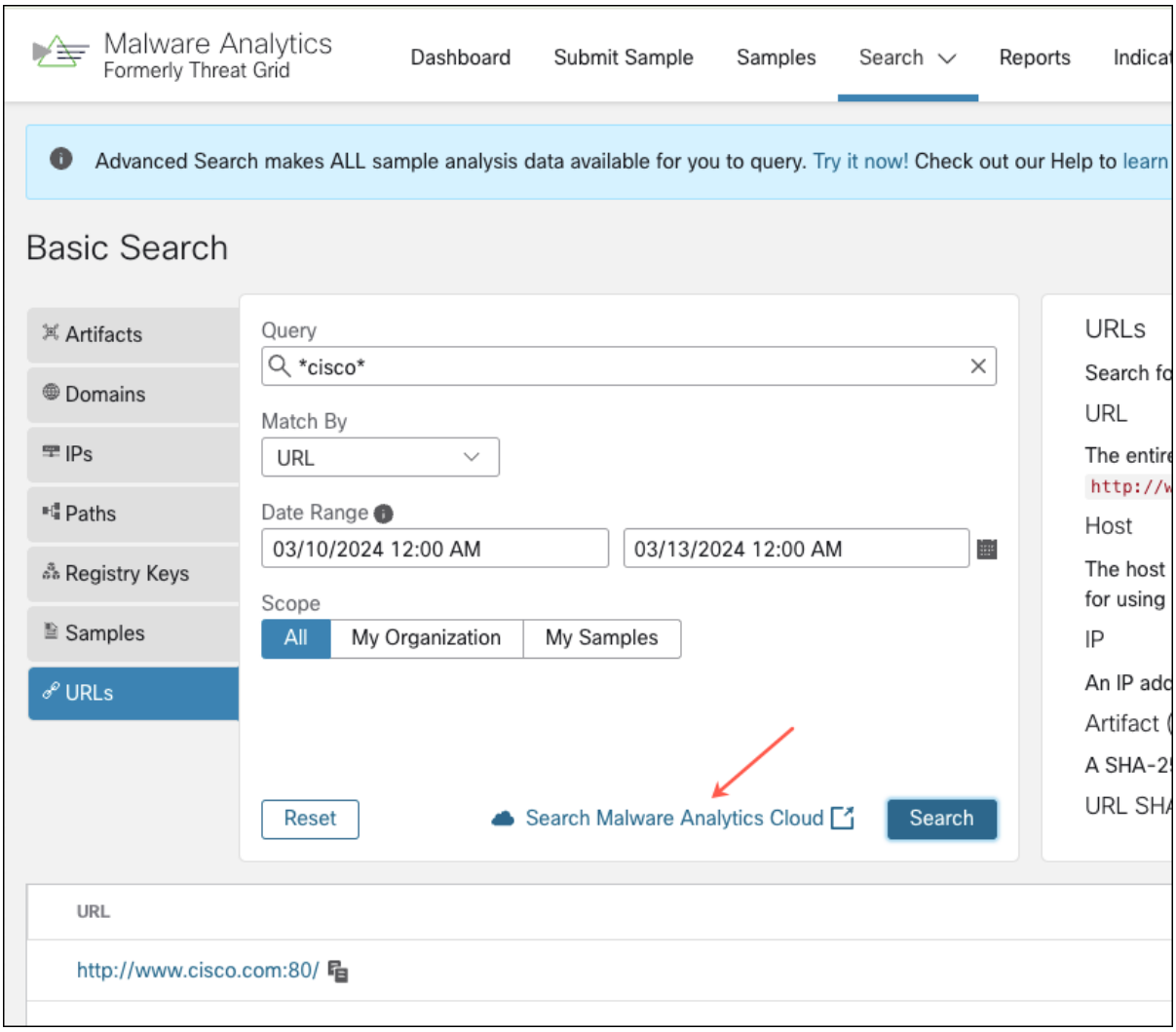


Figure 13: Basic Search - Secure Malware Analytics Cloud link



Note

The Secure Malware Analytics appliance prioritizes data security. When you perform a sample disposition lookup in the Malware Analytics Cloud, the actual sample file itself is **not** uploaded or transferred to the cloud.

This feature expands the capabilities of your appliance by enabling searches across two intelligence sources:

- **Local Intelligence Store:** This on-appliance database stores information about previously analyzed files.
- **Cloud Intelligence Store:** This centralized repository in the Secure Malware Analytics cloud aggregates threat data from the entire SMA user base.

Step 3 Enter the credentials required for each integration.

Note
ClamAV signatures can be automatically updated on a daily basis, and is enabled by default. Enabling ClamAV signatures in malware analysis allows you to detect known malware using ClamAV's database of virus signatures. You can disable the **Automatic Updates** setting in the **ClaimAV** section.

Titanium Cloud (ReversingLabs TitaniumCloud™)

Use the TitaniumCloud Integration Malware Analysis Platform to increase detection, analysis, and response efficiency by identifying files with its global goodware and malware database of over 6 billion files.

To configure an integration with TitaniumCloud, you will need :

a. **URL:** Titanium Cloud URL.

b. **Username:** Username of you TitaniumCloud account.

c. **Password:** Password of you TitaniumCloud account.

Umbrella (Cisco - previously named OpenDNS)

Integrating Umbrella with your existing security infrastructure can help improve malware detection by blocking malicious domains and IPs at the DNS layer, providing real-time threat intelligence, and integrating with other security tools. This can help prevent malware from even connecting to command and control servers or downloading malicious payloads, even if the user clicks on a malicious link or opens an infected attachment. To configure an integration with Umbrella, you can navigate to Admin in the Umbrella portal to get the **Token**.

Note
You need Tier2 or Tier3 Investigate license for the Umbrella integration.

VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and detects viruses, worms, trojans, and all kinds of malware. It integrates easily with Security Operations. Integrating VirusTotal into your security infrastructure can improve malware detection by providing access to a large and comprehensive malware database, the ability to detect new and emerging malware, and the ability to analyze suspicious URLs and files in a sandbox. Before you can use the VirusTotal integration, you must activate the plugin, provide the URL of the activated instance along with the appropriate API key.

Step 4 Click **Save**.

License

When a new appliance is purchased, a license is generated and the **Retrieve License From Server** button on the **Configuration** > **License** page is enabled. However, if that doesn't work or if there's a special case (such as a license being a custom one-off), then you will be given the license directly, as an encrypted file with a password.

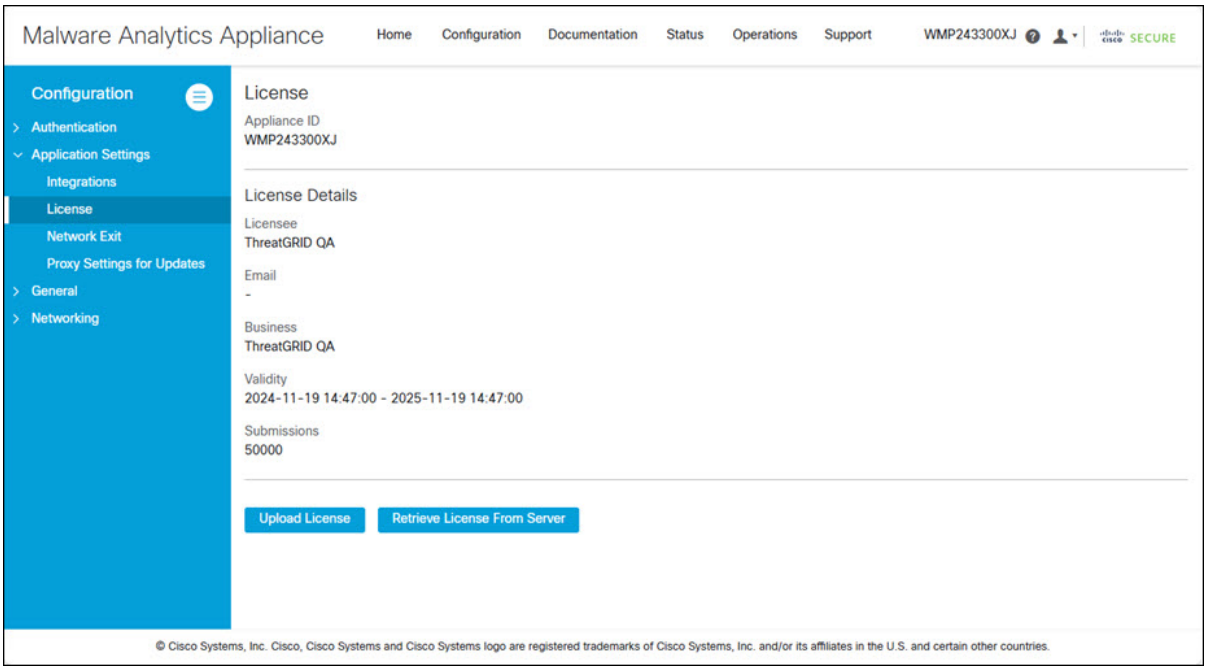
You can view or update your license information using the **License** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Application Settings** in the side navigation and choose **License** to open the **License** page.

Figure 14: License Page

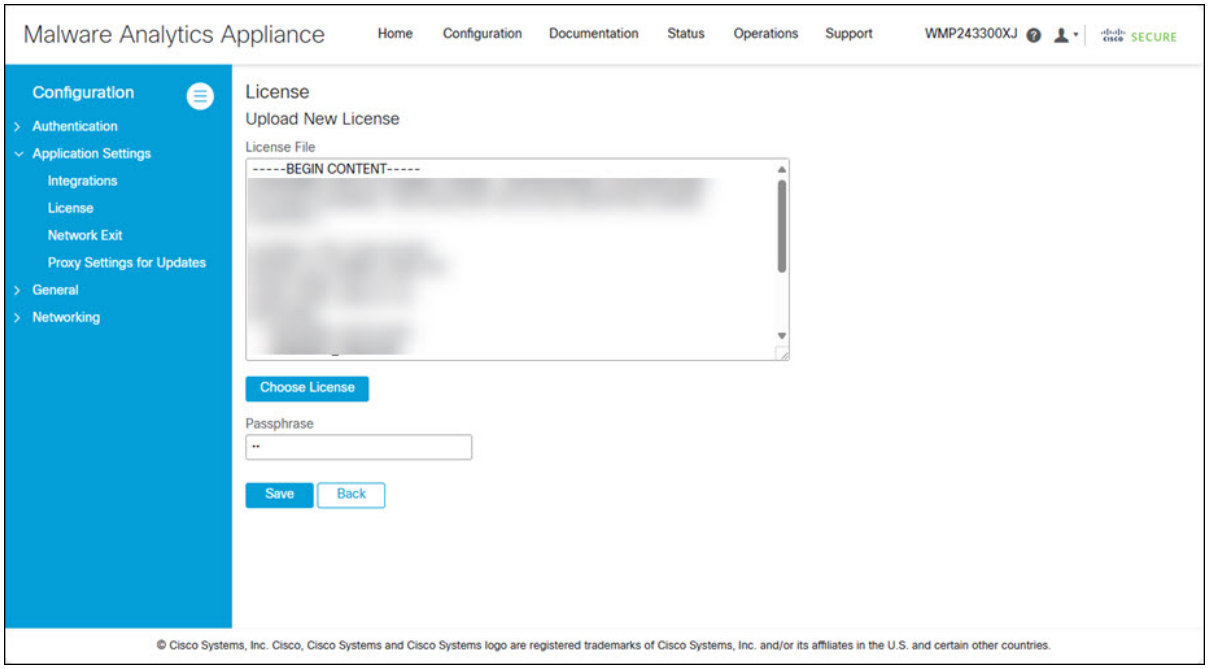


Step 3 Upload the license or retrieve it from the server. Typically, you must upload the license for air-gapped appliances.

To Upload License:

a) Click **Upload License** to open the **Upload New License** page.

Figure 15: Upload License



b) Click **Choose License** to open the **File Manager**, choose the license file you received from Secure Malware Analytics (the file has .lic extension), and click **Open**.

The contents of the license are added to the **License File** field.

c) Enter the password that Secure Malware Analytics provided (with the .lic file) in the **Passphrase** field and click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

To Retrieve License from Server:

a) Click **Retrieve License From Server** to retrieve and add the license.
b) Click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

Network Exit

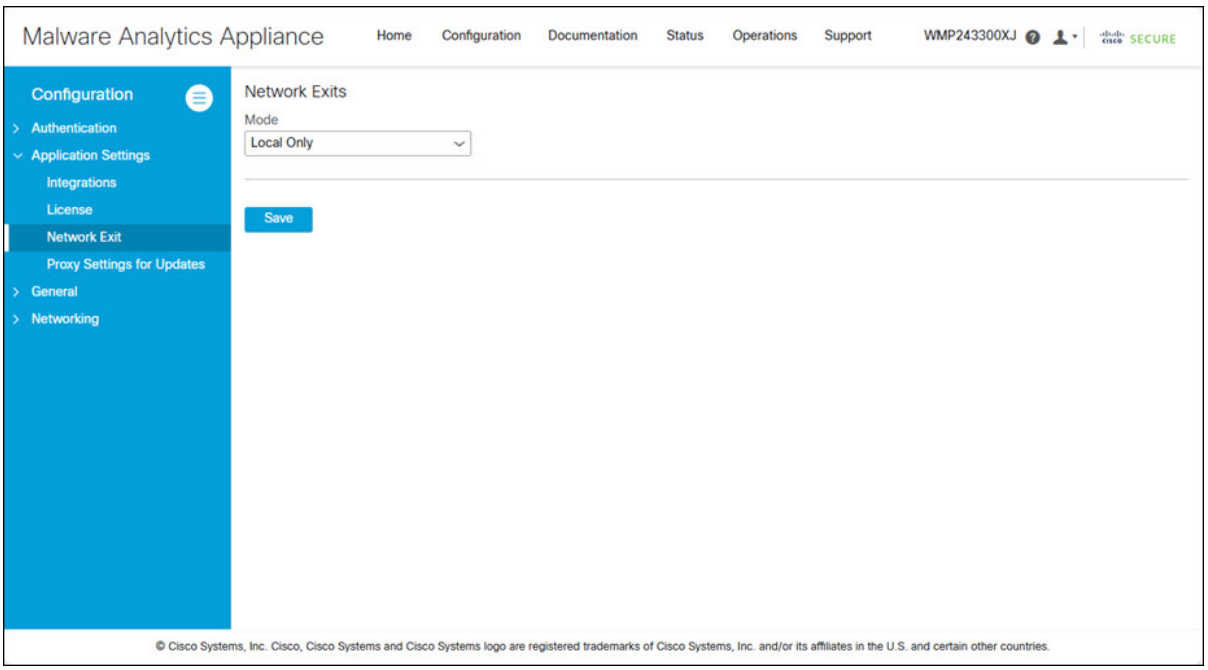
Geographic location is often an important issue for malware analysis. Some types of malware behave differently depending on geographic location, while other types may target a specific area. Similar in concept to VPN, the **Network Exits** mode makes any outgoing network that is generated during sample analysis appear to exit from that location. Configuration files are automatically distributed and there is no need for support staff to manually install or update them.

Procedure

Step 1 Navigate to **Configuration** > **Application Settings** > **Network Exit**

The setting on this page determines the **Network Exit** options that will be available in the Secure Malware Analytics portal when submitting samples for analysis.

Figure 16: Network Exits Configuration



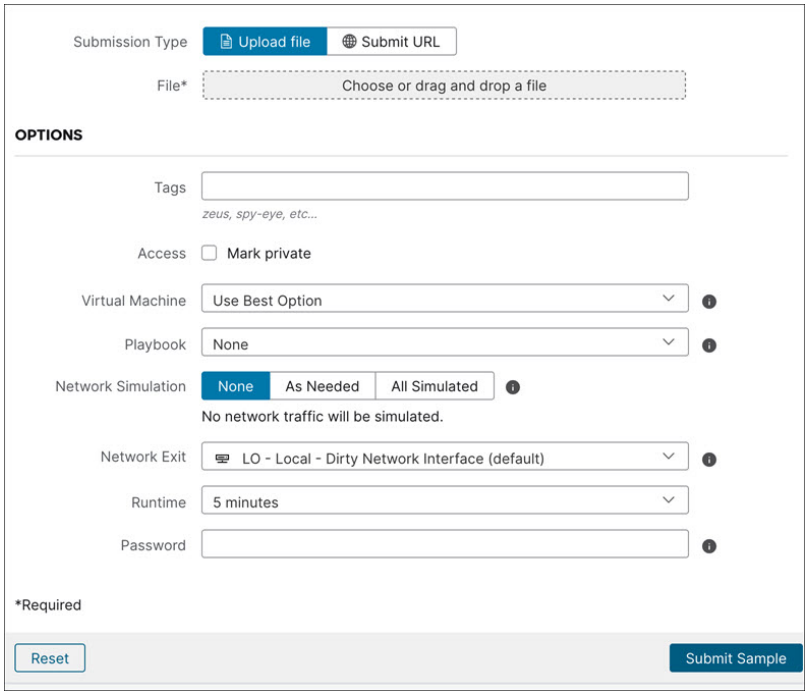
Step 2 From the Mode drop-down list, choose **Local Only**, **Remote Only**, **Both Local and Remote**, or **Simulation Only**.

If you choose **Local Only** or **Remote Only**, the application makes only those options available to users; if you choose **Both Local and Remote**, both options will be available to users.

If you choose **Simulation Only**, the API and UI users cannot choose any option to send network traffic from virtual machines to destinations outside of the local Secure Malware Analytics Appliance.

Accessing private networks, even for DNS lookup, is not allowed even for Network Exit. All malware traffic comes out of the Dirty interface, using the Dirty DNS server configured.

Figure 17: Submit Sample



Note
Sometimes it may be necessary to simulate network connections during analysis. Network simulation provides analysts with a way to present network resources to malware samples that may otherwise be unavailable, and for other reasons. For example, you may want to choose a network simulation option to simulate network connections when the upstream servers are not accessible; when they have been taken down; when their DNS records are gone; or if other restrictions on outbound connectivity apply in order to improve sample execution and convictions.

In addition, network simulation can provide at least some connectivity to air-gapped appliances and improve sample execution on them.

The **Network Simulation** option for sample analysis is available on Secure Malware Analytics Appliances. For additional information, refer to the Secure Malware Analytics portal UI online help topic.

Updates Proxy

SOCK5 is an Internet protocol that exchanges network packets between a client and server through a proxy server. If the appliance's dirty interface cannot reach update servers. SOCKS5 proxy is configured to download the updates.

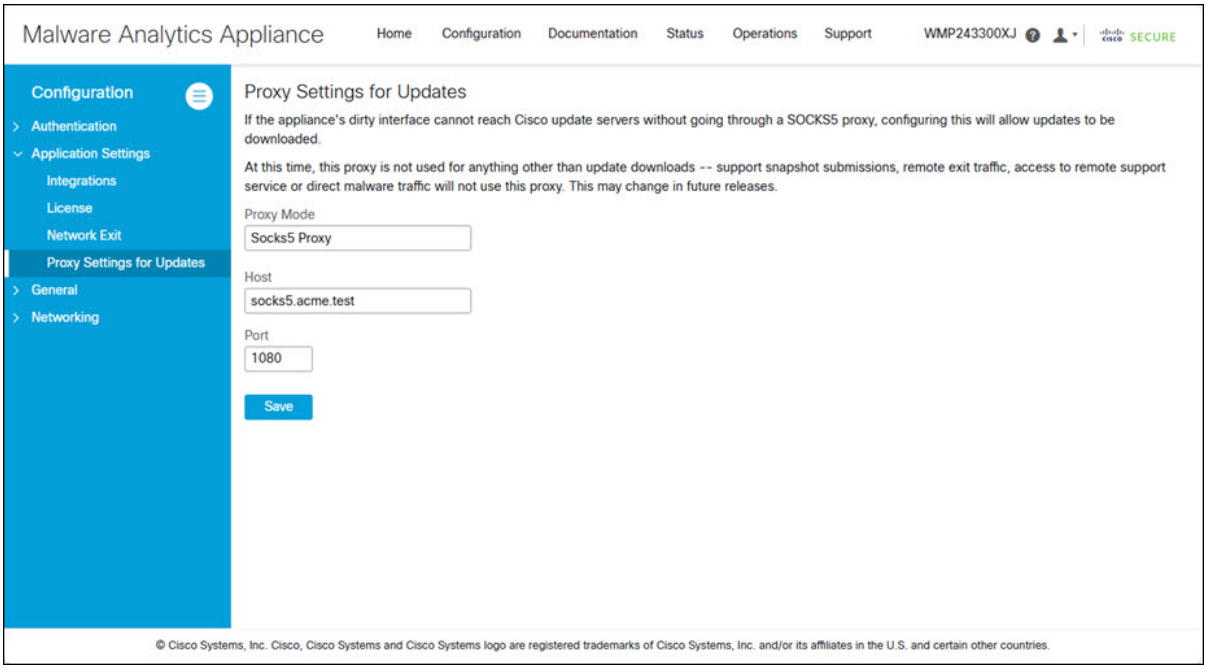
Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Application Settings** in the side navigation and choose **Proxy via Dirty** to open the **Authentication** configuration page.

The setting on this page determines the **Updates proxy** options that will be used to download the updates.

Figure 18: Updates Proxy Configuration



Step 3 From the **Proxy Mode** drop-down list, choose **Socks5 Proxy**.

Step 4 Enter the host in the **Host** field.

Step 5 Enter the port in the **Port** field.

General

The Secure Malware Analytics Appliance general configuration settings are under the General side navigation.

Content Update

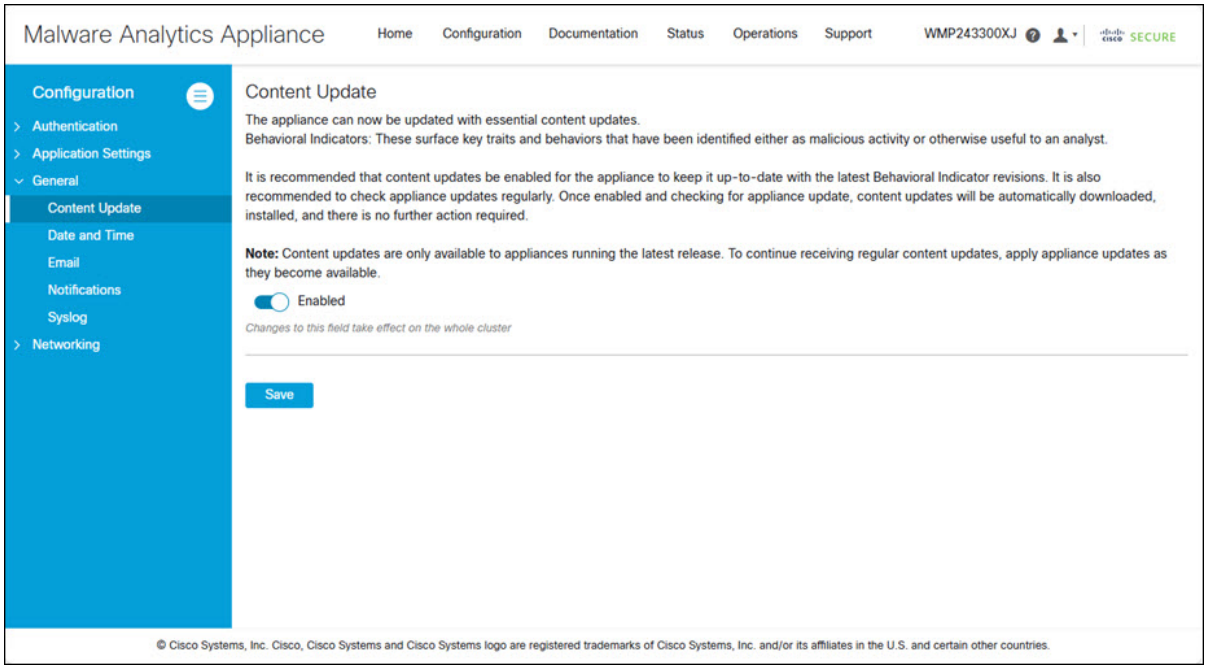
Content Update allows your appliance to receive the latest behavioral indicators automatically while updating the appliances. In order to receive the BIs automatically, you need to toggle the Content Update switch in the **Enabled** position. To enable Content Update, do the following:

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and and choose **Content Update** to open the **Content Update** page.

Figure 19: Content Update



Note
When you enable the Content Update, it updates all the appliances in the cluster.

Step 3 Toggle the switch from **Disabled** to **Enabled** position.

Note
When enabled, Content Updates are downloaded and applied during the nightly appliance update check.

Step 4 Click **Save**.

Date and Time

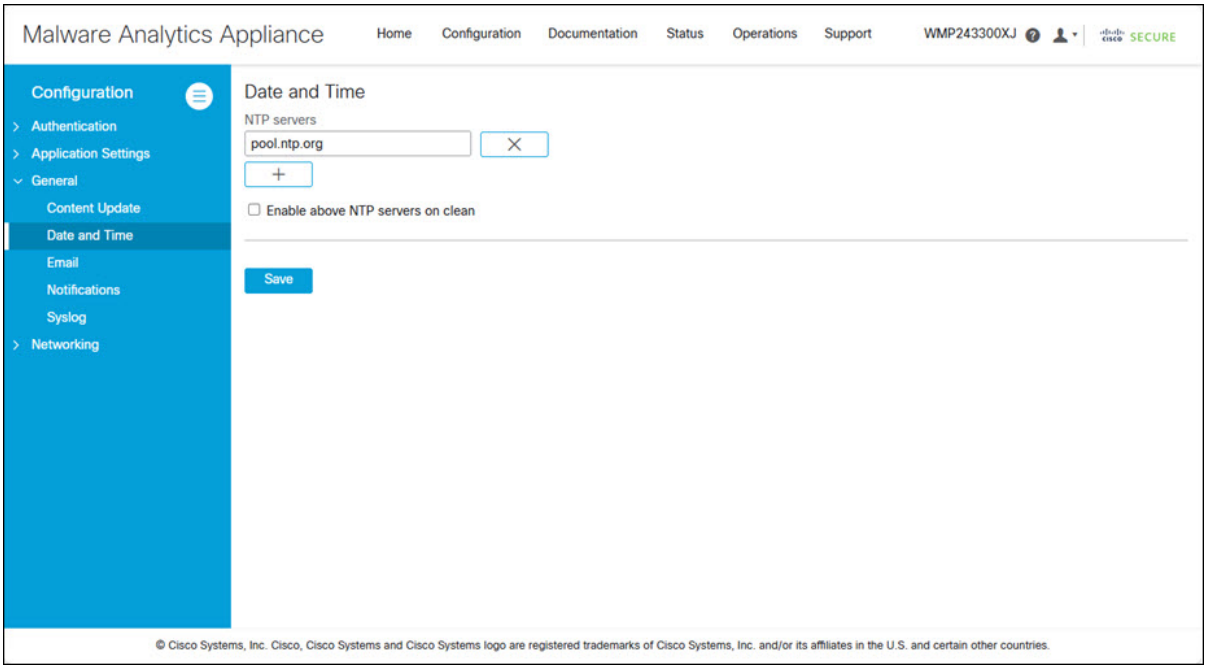
When you initially set up the Secure Malware Analytics Appliance, you specify the Network Time Protocol (NTP) servers to configure the date and time. You can add or delete NTP servers using the **Date and Time** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and and choose **Date and Time** to open the **Date and Time** page.

Figure 20: Date and Time



Step 3 Add or remove NTP Server(s):

- Click the + icon to add another field and enter the NTP server name or IP address; repeat as needed.
- Click the **x** icon to remove a server.

Step 4 Click **Save**.

Email

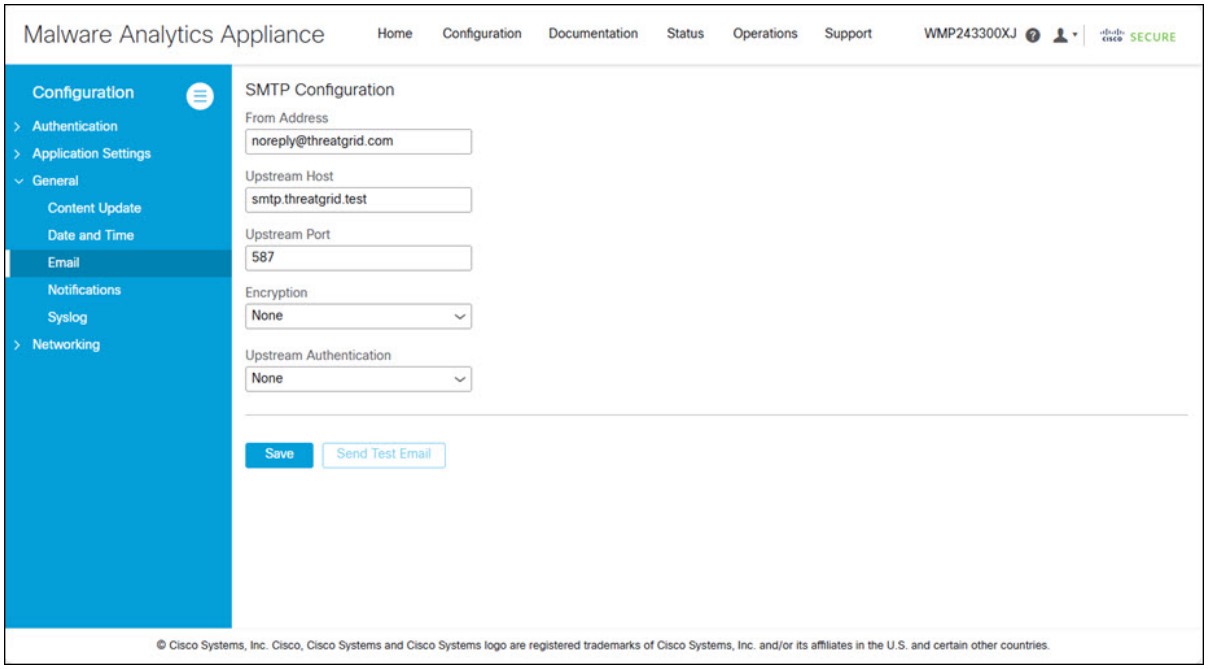
When you initially set up the Secure Malware Analytics Appliance, you configure your email settings. You can modify these settings on the **Email** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and choose **Email** to open the **SMTP Configuration** page.

Figure 21: SMTP Configuration



Step 3 Make your modifications and click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

Step 4 Click **Send Test Email** to test the SMTP configurations.

Notifications

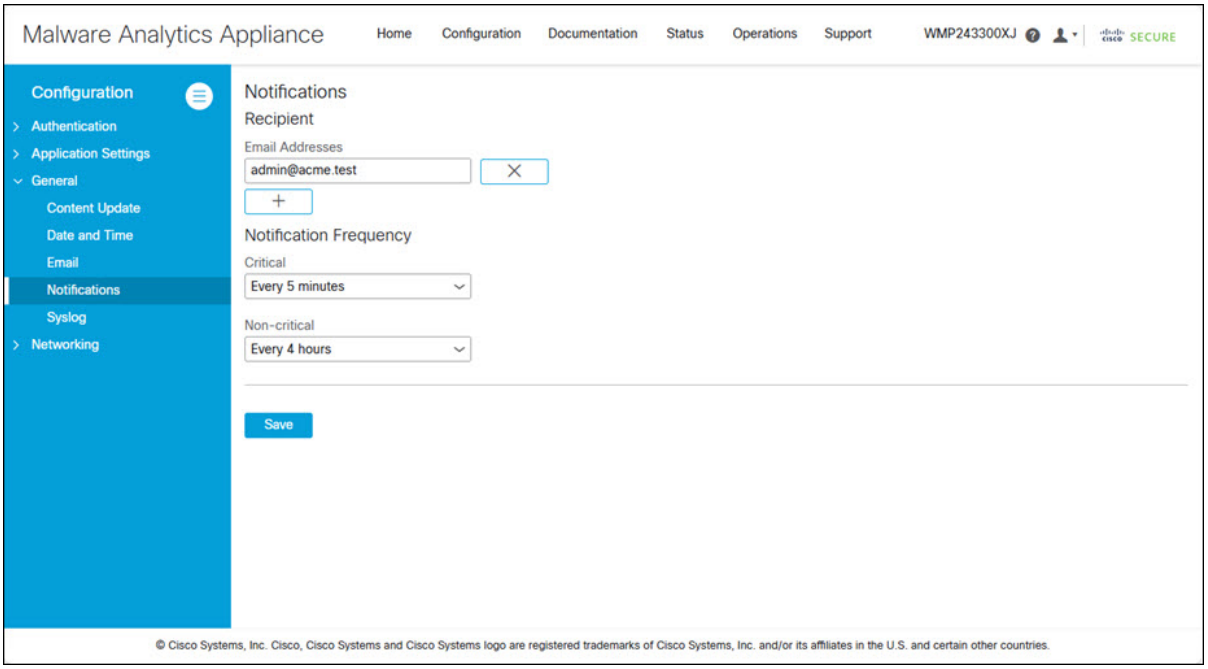
When you initially set up the Secure Malware Analytics Appliance, you configure the notifications to be received via email. You can add or delete recipients, and change the notification frequency using the **Notifications** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and choose **Notifications** to open the **Notifications** page.

Figure 22: Notifications



Step 3 Under **Recipients**, enter the **Email Address** for at least one notifications recipient. If you need to add multiple email addresses, click the + icon to add another field; repeat as needed.

Step 4 Under **Notification Frequency**, choose the settings for **Critical** and **Non-critical** from the drop-down lists.

Step 5 Click **Save**.

Syslog

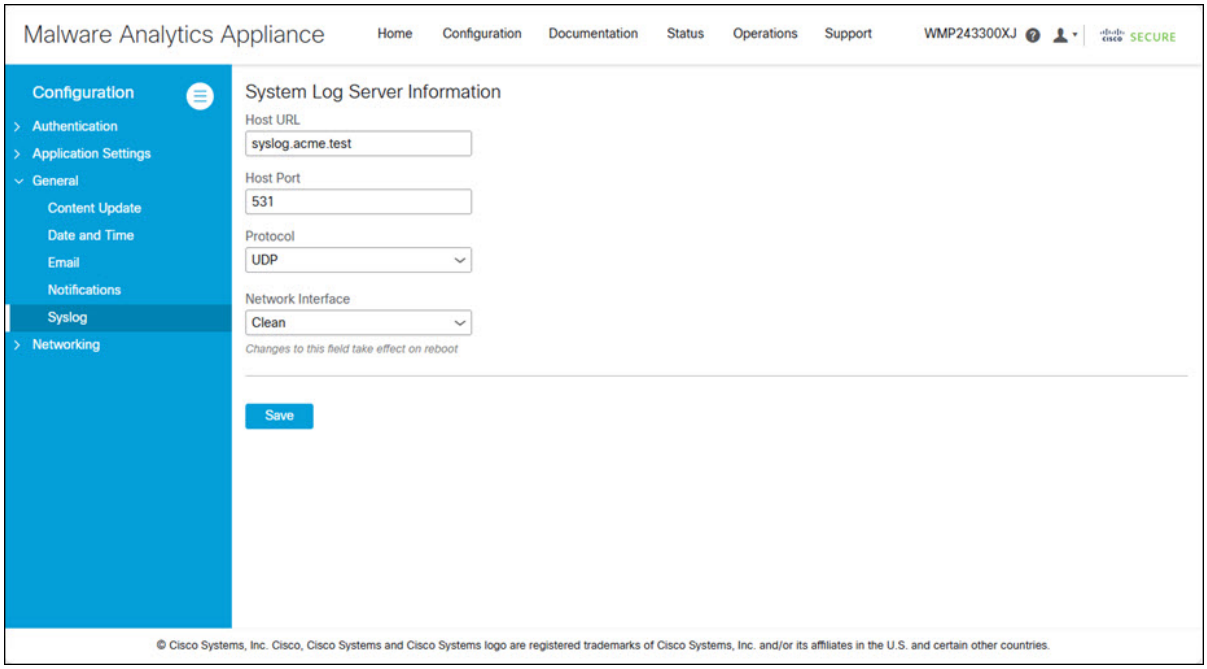
The **System Log Server Information** page is used to configure a system log server to receive syslog messages and Thread Grid notifications.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and choose **Syslog** to open the the **System Log Server Information** page.

Figure 23: System Log Server Information



Step 3 Complete the fields on the page:

- **Host URL** - Enter the host name or URL for the system log server.
- **Host Port** - Enter the port number for the server.
- **Protocol** - Choose **TCP** or **UDP** from the drop-down list.

Step 4 Click **Save**.

Networking

The Secure Malware Analytics Appliance network configuration settings are under the Networking side navigation.

Network

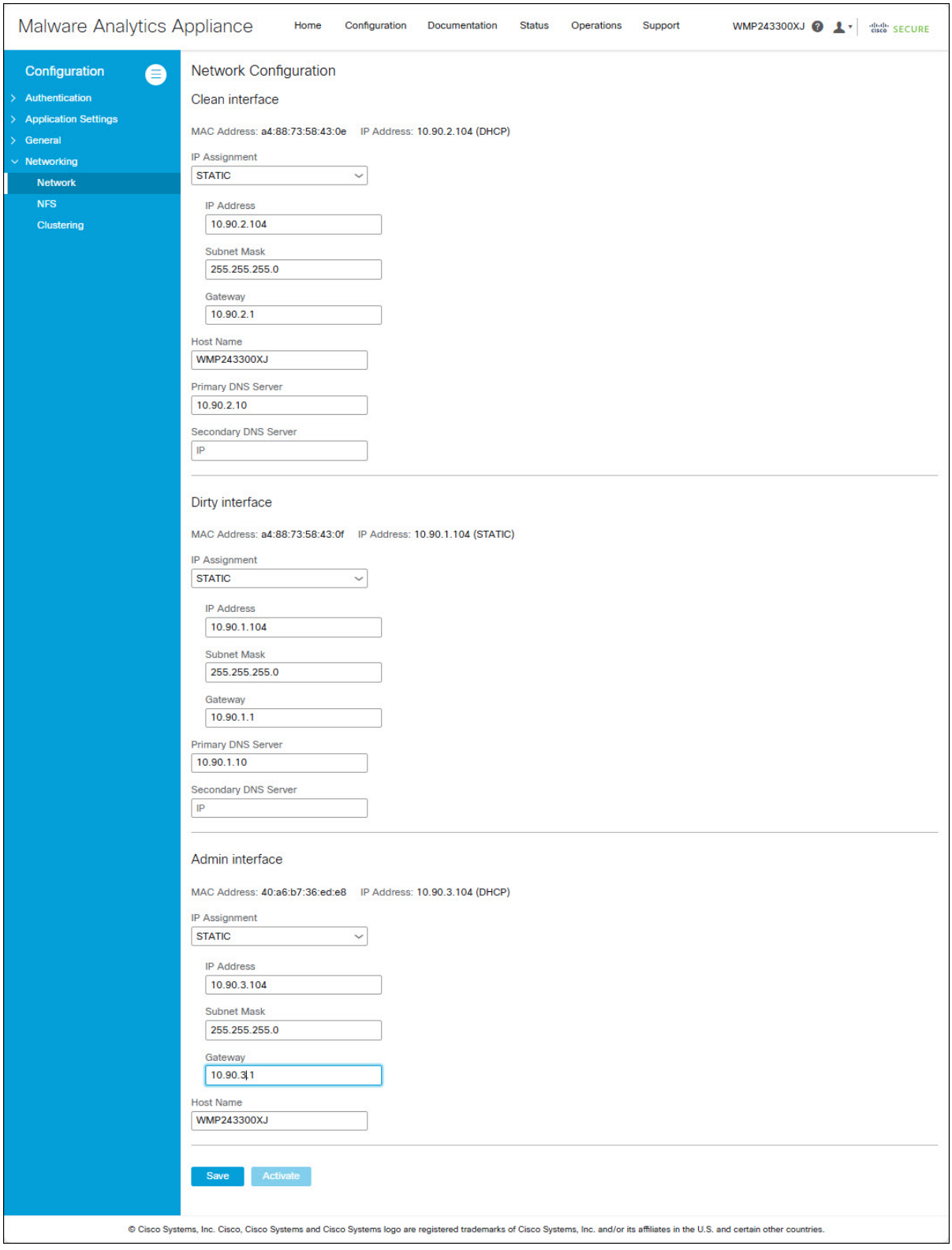
If you used DHCP for the initial configuration, and you need to adjust the IP assignment from DHCP to your permanent static IP addresses for all three networks, perform the following steps.

Note The OpAdmin does not validate the gateway entries. If you enter the wrong gateway and save it, the OpAdmin will not be accessible. You will need to use the console to fix the networking configuration if that was done on the admin interface. If Admin is still valid, you can fix it in the OpAdmin and reboot.

Procedure

Step 1 Navigate to **Configuration** > **Networking** > **Network**

Figure 24: Network Configuration



Step 2 Complete the following fields:

Note
The Admin network settings were configured using the Admin TUI during the initial Secure Malware Analytics Appliance setup and configuration.

- **IP Assignment** - Choose **Static** from the drop-down lists for all three interfaces (Clean, Dirty, and Admin).
- **IP Address** - Enter a static IP address for the Clean or Dirty network interface.
- **Subnet Mask and Gateway** - Complete as appropriate for the type of network interface.
- **Host Name** - Enter the host name for server.
- **Primary DNS Server** - Enter the primary DNS server address.
- **Secondary DNS Server** - Enter the secondary DNS server information.

Note
ADMIN Interface: Select **DISABLED** for **IP Assignment** to reroute the traffic from *Admin* to go through *CLEAN*.

Step 3 Click **Save** to save your network configuration settings, and then click **Activate**.

A message is displayed indicating that reconfiguration is required (see Applying Configuration Changes).

Configuring DNS

By default, DNS uses the Dirty interface. If the hostname of an integrating appliance or service, such as Secure Endpoint Private Cloud, cannot be resolved over the Dirty interface because the Clean interface is used for the integration, a separate DNS server that uses the Clean interface can be configured in the OpAdmin.

Procedure

Step 1 Navigate to **Configuration** > **Networking** > **Network**

Step 2 Complete the **DNS** fields for the Dirty and Clean networks.

Step 3 Click **Save**.

NFS

The Secure Malware Analytics Appliance supports encrypted backups to NFS-backed storage, initialization of data from such storage, and reset to an empty-database state into which such a backup can be loaded.

Note Reset is different from the Wipe Appliance process; it is used to allow an appliance to be shipped off customer premises without information leakage, and is for backup preparation. The wipe process appropriate for that purpose already exists in the recovery bootloader, but is not suitable for preparing a system to restore a backup.

Content is encrypted with gocryptfs, a third-party open source product.



Note Filename encryption is disabled for performance reasons. Samples and other content in Secure Malware Analytics are not stored with their original names under any circumstances so this does not leak customer-owned data.

We strongly encourage consulting the documentation prior to use. Extended documentation regarding the backup functionality is available, and we strongly encourage consulting it prior to use. For additional technical information and instructions see the *Secure Malware Analytics Appliance Backup Notes and FAQ*.

NFS Requirements

The following NFS requirements must be met for encrypted backups to NFS-backed storage:

- Must be running the NFSv4 protocol over TCP, accessible from the Secure Malware Analytics Appliance admin interface.
- Only root user (UID 0) is allowed to mount. Make sure that UID 0 is allowed while mounting. Windows NFS admins should have users with UID 0 that will be able to write to that location.



Note For Linux servers, it does not matter as *root_squash* is available by default. But in strict environments *no_root_squash* can be added.

- Configured directory must be writable by **nfsnobody** (UID 65534).
  - Exposing files for write by **nfsnobody** is secure. The only processes on the Secure Malware Analytics Appliance running as **nfsnobody** or with write to **nfsnobody**, are those responsible for encryption of data. Plain text data is exposed under distinct user accounts for different subtrees according to principal of least privilege; the PostgreSQL service on the appliance cannot access Elasticsearch data or the freezer; the Elasticsearch service cannot access PostgreSQL or freezer data.
  - Using the **nfsnobody** account simplifies configuration, preventing the need to build an **idmap.conf** for each customer site, mapping local and remote account names together.
- The NFSv4 server must be accessible via the Admin 10-Gb interface.
- Sufficient storage must be available (see Backup Storage Requirements).
- The system will use these parameters: `rw`, `sync`, `nfsvers=4`, `nofail`



Note Do not enter conflicting parameters. Manually entering any parameters that conflict with the above parameters is explicitly unsupported and may result in undefined behavior.

- Invalid NFS configuration (or configuration pointing the service to an incorrectly configured NFS server) will generally cause the process of applying configuration to fail. Correcting this configuration in the OpAdmin and reapplying should result in success.

Backup Storage Requirements

It is recommended to provid at least 6 TB of NFS backup storage per node involved in the backup configuration. While implementation-specific factors may necessitate more backup storage, this figure is sufficient for standard deployments using average sample files less than 1 MB. A backup store consists of the following components:

- **Object Store** - This component typically constitutes the bulk of the storage used. Data retention for the bulk component of a backup store follows the same policies and limits documented for Secure Malware Analytics. For more information, refer to Secure Malware Analytics Appliance Data Retention Notes.
- **PostgreSQL database store** - This component contains ten full backups of the PostgreSQL database and a chain of WAL logs sufficient to allow replay from the oldest of the retained full backups.
- **Elasticsearch snapshot store**

Backup Expectations

The following backup expectations should be considered:

- **Included in Backup** - The initial release of the Secure Malware Analytics Appliance backup process includes the following customer-owned bulk data:
  - Samples
  - Analysis results, artifacts, flagging
  - Application-layer (not OpAdmin) organization and user account data.
  - Databases (including users and organizations)
  - Configuration done within the Secure Malware Analytics portal UI
- **Not Included in Backup** - The following is not included in the initial release of the Secure Malware Analytics Appliance backup process:
  - System logs
  - Previously downloaded and installed updates
  - Configuration inside the appliance OpAdmin, including SSL keys and CA certificates
- **Other Expectations** - Other considerations about the backup process include:
  - **PostgreSQL base backup** takes place on a 48-hour cycle. Database backup cannot be restored, and a warning will be displayed, until this has successfully completed at least once.
  - **Elasticsearch backup** takes place incrementally, once every 5 minutes.
  - **Freezer backup** takes place on an ongoing basis, with a job following behind every 24 hours to handle any objects which were missed from the ongoing backup.
  - **Generating a new key** creates a new, independent backup store. Like the original, this new store is not valid until a base backup has taken place on a 48-hour cycle.

Backup Data Retention

During a backup, data is retained as follows:

- **PostgreSQL** - The last ten successful backups and all WAL segments since those backups are retained.
- **Elasticsearch** - The last two 5-minute snapshots are retained.
- **Bulk Storage** - The same retention policy followed and documented for a single Secure Malware Analytics Appliance is used for the shared store.

If you want to retain historical data for longer periods, it is strongly recommended that you use an NFS server with filesystem- or block-layer snapshot support.

Database base backups are only retained until a new base backup has been successfully created.



Note Backup copies of the virtual machine images are created on the RAID-1 storage array, to be used in the event of a reset following a bulk-storage failure. Early Cisco Secure Malware Analytics Appliance models (based on the UCS C220-M3 platform) have less storage than later models, and are more likely than other units to have less than 25 percent of disk space remaining available on the RAID-1 file system after installing Secure Malware Analytics Appliance v2.9, which will trigger a service notice.

For later model hardware, being at less than 25 percent of remaining storage on the RAID-1 array after installing the v2.9 release is not normal and should be raised to customer support.

Strictly Enforce Retention Period Limits

The **strict_retention** option in **tgsh** allows you to strictly enforce the retention period limit by not storing artifacts from analysis for more than fifteen (15) days. When this option is enabled, files are deleted during the first nightly pruning on which they are more than 15 days old.



Note The time period of 15 days cannot be configured or changed.

Artifacts refers to the samples themselves and other things generated from them. Artifacts do not include the analysis report HTML, which is subject to its original limits as otherwise documented. Artifacts also do not include database entries and search indexes.

The **strict_retention** option is disabled (false) by default. To enable the hard-pruning of artifacts after 15 days, set the option to true in **tgsh**:

configure set strict_retention true

Backup Frequency

The backup frequency of data is as follows:

- For bulk storage of samples, artifacts and reports, content is continuously backed up. Additionally, a pass is performed to look for and transfer missing content on a 24-hour cycle.
- For the PostgreSQL database, a base backup is created on a 24-hour cycle, and incremental content is continually added thereafter, either as soon as a 16-MB threshold of newly-written database content is reached, or not less than once every 5 minutes.

- For the Elasticsearch database, content is incrementally added to the backup store on a 5-minute cycle.

Backup frequency cannot be controlled or tuned because doing so would make estimates regarding storage usage, restore-process time, and performance overhead invalid.

Backup Related Service Notices

The following service notices may be displayed during the backup process:

- **Network storage not mounted** - Check that the network file system being used as a backend is fully operational, and then try reapplying configuration through the OpAdmin or rebooting your appliance.
- **Network storage not working** - Check that the network file system being used as a backend is fully operational; if the system does not recover within 15 minutes of correcting any problems with the NFS server, try rebooting your appliance.
- **Backup file system access failure** - Contact customer support.
- **No PostgreSQL backup found** - This is a normal condition between the point in time when a backup store has been configured and the point in time when the first base backup (run automatically on a 24-hour cycle) takes place. Note that until this is complete, a backup is not considered complete and cannot be restored. If and only if this message persists for more than 48 hours, contact customer support.
- **Newest PostgreSQL base backup more than two days old** - This indicates that the system has not been successful in generating a new base backup for PostgreSQL. If not remediated, it can result in unbounded usage on the backup store (to retain a full chain of writes necessary to restore from an increasingly old backup point), and unacceptably long processing time needed for a restore to take place. Contact Support.
- **Backup Creation Messages** - These reflect errors detected when starting or triggering a backup.
- **ES Backup (Creation) Inactive** - Indicates that when Elasticsearch was started, the backup store was unavailable. This can be remediated by rebooting the appliance, or (if NFS and the encryption service are now functional) by logging into **tgsh** and running the command service `restart elasticsearch.service`.
- **Backup Maintenance Messages** - These reflect errors detected when checking status of previously created backups.
- **ES Backup (Maintenance) snapshot (...) status FAILED** - This indicates that in the most recent attempt to update the backup of the Elasticsearch database, no indices could be successfully written. Check that the NFS server is functional and has free space; if no issue can be identified and the issue persists, contact customer support.
- **ES Backup (Maintenance) snapshot (...) status INCOMPATIBLE** - Should only occur immediately after an appliance upgrade installing a new version of Elasticsearch; will be displayed until the backup store has been upgraded to be compatible with this new release. Restoring from an incompatible backup may require customer service assistance, should a failure occur while in this state.
- **ES Backup (Maintenance) snapshot (...) status PARTIAL** - Contains one of two messages in the body: No prior successful backups seen, so retaining. (if we're keeping a partial backup as better than none at all); or Prior successful backups exist, so removing. (if we're discarding that partial backup with the intent to retry later).
- **ES Backup (Maintenance) - Backup required (...) ms** - Occurs if a backup requires more than 60 seconds. This is not necessarily an error: Elasticsearch performs periodic maintenance which can cause

significant write load even on idle systems. However, if it takes place consistently when under periods of low load, investigate storage performance or contact customer service for assistance.

- **ES Backup (Maintenance)** - Unable to query Elasticsearch snapshot status - Elasticsearch could not be contacted; and this failure took place after a backup creation was successfully started. Generally, this will occur in conjunction with other appliance failures, and remediation should focus on those issues. If this error is seen when the appliance is otherwise fully functional and does not go away of its own accord, contact customer support.

Appliance Backup

Perform the following steps to perform a backup of the Secure Malware Analytics Appliance:

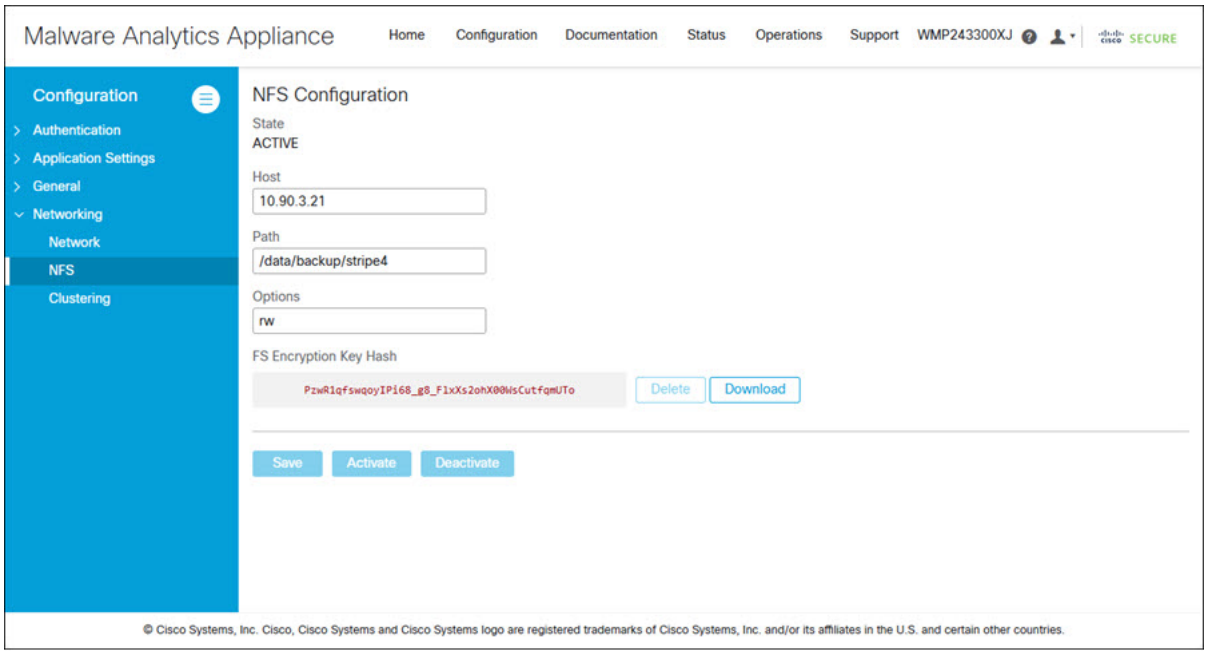
Procedure

Step 1 Create the backup target directory according to the NFS Requirements.

Step 2 Navigate to **Configuration** > **Networking** > **NFS**

Note
If you completed the NFS configuration during the initial appliance setup and you have the encryption key, you can skip step 3 through step 5. Otherwise, you must obtain an encryption key to restore the backup data.

Figure 25: NFS Configuration



Step 3 Enter the following information:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server under which files will be stored.

- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4. The default is **rw**.
- **FS Encryption Key Hash** - Click **Generate Key** to generate a new encryption key. You will need this key to restore backups later. (At that time, click **Upload** and upload the key required for the backup.)

Step 4 Click **Save**. The page refreshes and a **FS Encryption Password Key ID** is displayed.

The first time you configure this page, options to **Delete** or **Download** the encryption key become visible. The **Upload** option is available if you have NFS enabled but do not have a key created. Once you create a key, the **Upload** button changes to **Download**. (If you delete the key, the **Download** button becomes **Upload** again.)

Note
If the key correctly matches the one used to create a backup, the **Key ID** displayed in OpAdmin after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key.

Step 5 Click **Activate** to activate the key.

Important
The user is responsible for backing up the encryption key and securely storing it; Secure Malware Analytics does not retain a copy. Backup cannot be completed without this key.

Step 6 Reset the backup restore target as described in Reset Appliance as Backup Restore Target.

Step 7 Restore the backup data as described in Restore Backup Content, on page 43.

Reset Appliance as Backup Restore Target

Before an appliance can be used as a restore target, it must be in a preconfigured state. Appliances ship in this state. However, getting one back to the preconfigured state once it has been configured requires explicit administrative action.



Caution Performing this process will destroy customer-owned data. Read all of the documentation before performing any tasks, and be very careful before proceeding. .



Note Reset is not the same as the secure wipe that is available in recovery mode; only the recovery-mode secure wipe is appropriate to completely remove customer-owned data from an appliance before shipping it to a DLP reimaging center. However, the secure wipe in recovery mode is not a replacement for this reset: secure wipe renders an appliance unusable until reimaged, while this reset prepares an appliance to restore a backup.

Data Reset

The data reset process was updated in Secure Malware Analytics Appliance and is now more comprehensive. While the Wipe process (in the recovery bootloader menu) is still required for a firm guarantee of the destruction of all customer-related data, the reset process now clears operating system logs and other state which was previously left in place.

A successfully reset Secure Malware Analytics Appliance now has a new randomly-generated password displayed on its console (identical to behavior in newly-installed state). This improved process now reboots multiple times, and can be invoked from recovery mode (as opposed to the prior process, which could only be successfully invoked when booted into regular operation).

The Secure Malware Analytics Appliance uses XFS as the primary file system. If a Secure Malware Analytics Appliance has its data reset, the datastore will be changed to a XFS file system. This improves forward compatibility and provides OS-level support for I/O usage monitoring on a per-service basis.

The data reset process now also requires sufficient storage to contain all content necessary for a fresh install on the system SSDs. Any pre-existing data is only deleted after the presence and validity of this content has been ensured. It is possible that systems that have been in use for an extended period (particularly first-generation hardware), may not have sufficient space immediately available. If this is the case, customer support can assist, if needed.

Returning a Target Appliance to Preconfigured State

If you are not restoring to a system fresh from manufacturing, the restore target appliance must be returned to the preconfigured state by clearing pre-existing data and NFS-related configuration from the system.

Procedure

Step 1 Access the Admin TUI via the Secure Malware Analytics Appliance TTY, or SSH.

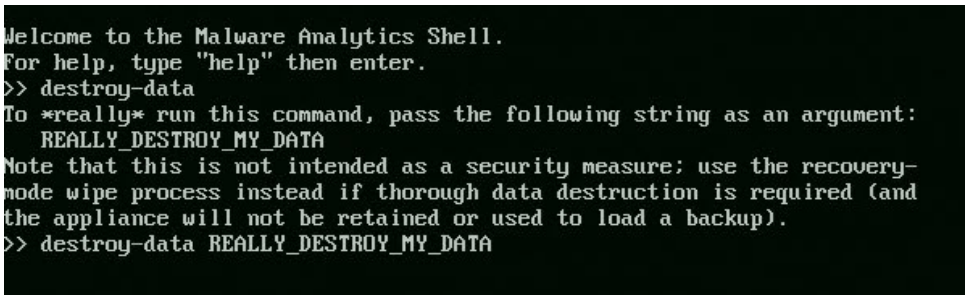
Step 2 Choose the **Console** option to enter **tgsh**.

Note
Entering **tgsh** via Recovery Mode is not suitable for this use case.

Step 3 At the **tgsh** prompt, enter the command `destroy-data`. Carefully read and follow the instructions provided with the prompt.

Caution
There is no Undo from this command. All data will be destroyed.

Figure 26: The destroy-data REALLY_DESTROY_MY_DATA Command and Argument



The following data is destroyed:

- Samples
- Analysis results, artifacts, flagging
- Application-layer (not the OpAdmin) organization and user account data

- Databases (including users and organizations)
- All types of configuration including the network information
- Configuration done within the Secure Malware Analytics portal UI
- NFS configuration and credentials
- The local copy of the encryption key used for NFS

Returning Non-Target Appliance to Preconfigured State

If another system or Secure Malware Analytics Appliance is actively writing to the backup that is being restored, for example, a test restore of content being written by a second master Secure Malware Analytics Appliance actively used in production, return that Secure Malware Analytics Appliance to the preconfigured state.

Procedure

Step 1 Generate a consistent, writable copy of the datastore.

Step 2 Point the Secure Malware Analytics Appliance that is doing the test restore to the writable copy instead of to the store which is being continuously written.

Once the Secure Malware Analytics Appliance is in a preconfigured state, it can function as the target for the backup store as described in Restore Backup Content.

Restore Backup Content



Important

- The system is unavailable for sample submission during the restore process.
- Only one server can be running with data from a given backup store active at a time.
- Backups can only be restored from the OpAdmin.
- Set up the same NFS store and encryption key, as previously used, with a process identical to the original process. Setting up a Secure Malware Analytics Appliance with a prior NFS store and encryption key will trigger a restore.
- To test the restore process on a different Secure Malware Analytics Appliance while the primary Secure Malware Analytics Appliance is still operational, make a copy of a consistent snapshot of the backup store and point the new Secure Malware Analytics Appliance (with the encryption key uploaded) to it.

Perform the following steps to restore the backup content:

Procedure

Step 1 Click the **Configuration** tab and choose **NFS** to open the **NFS Configuration** page.

Step 2 Click **Upload** to retrieve the backup key previously generated when configuring the server on which the backup was created.

If the key correctly matches the one used to create a backup, the **Key ID** displayed in the OpAdminshould match the name of a directory in the configured path. The install wizard checks for a directory matching the backup key, and if it finds one, begins restoring the data to that location.

Note
There is no progress bar. The amount of time required to restore data depends on the size of the backup and other factors. In testing, a 1.2-GB restore is quick, while a 1.2-TB restore required over 16 hours. For large restores it may appear that the install has hung so be patient. The OpAdmin will report that the restore has succeeded, and the appliance will start up.

Step 3 Confirm that the restored data looks the same as the original data.

Clustering

Clustering increases the capacity of a single system by joining several Secure Malware Analytics Appliances together into a cluster (consisting of 3 to 7 nodes). It helps recovery from failure of one or more appliances in the cluster, depending on the cluster size. Each Secure Malware Analytics Appliance in a cluster saves data in the shared file system, and has the same data as the other nodes in the cluster.



Important If you have questions about installing or reconfiguring clusters, contact Cisco Support for assistance to avoid possible destruction of data.

Features

Clustering Secure Malware Analytics Appliances offers the following features:

- **Shared Data** - Every Secure Malware Analytics Appliance in a cluster can be used as if it a standalone; each one is accessing and presenting the same data.
- **Sample Submissions Processing** - Submitted samples are processed on any one of the cluster members, with any other member able to see the analysis results.
- **Rate Limits** - The submission rate limits of each member are added up to become the cluster's limit.
- **Cluster Size** - The preferred cluster sizes are 3, 5, or 7 members; 4- and 6-node clusters are supported, but with availability characteristics similar to a degraded cluster (a cluster in which one or more nodes are not operational) of the next size up.
- **Tiebreaker** - When a cluster is configured to contain an even number of nodes, the one designated as the tiebreaker gets a second vote in the event of an election to decide which node has the primary database.

Each node in a cluster contains a database, but only the database on the primary node is actually used; the others just have to be able to take over if and when the primary node goes down. Having a tiebreaker can prevent the cluster from being down when exactly half the nodes have failed, but only when the tiebreaker is not among the failed nodes.

Odd-numbered clusters will not have a tied vote. In an odd-numbered cluster, the tiebreaker role only becomes relevant if a node (not the tiebreaker) is dropped from the cluster; it then becomes even-numbered.

Limitations

Clustering Secure Malware Analytics Appliances has the following limitations:

- When building a cluster of existing standalone Secure Malware Analytics Appliances, only the first node (the initial node) can retain its data. The other nodes must be manually reset because merging existing data into a cluster is not allowed.

  Remove existing data with the destroy-data command, as documented in Reset Appliance as Backup Restore Target



Important Do not use the Wipe Appliance feature, as it will render the appliance inoperable until the Field Installer procedure is executed.

- Adding or removing nodes can result in brief outages, depending on cluster size and the role of the member nodes.
- Clustering on the M3 server is not supported. Contact Threat Grid Support if you have any questions.
- Starting with 2.20 SMA Appliance release, two-node clusters are not supported. Two nodes are not enough to keep quorum if a node goes down unexpectedly, and gives no availability guarantees, even with previous support for a tiebreaker node.

Requirements



Important **Clustering in Airgapped Deployments Strongly Discouraged** - Due to the increased complexity of debugging, appliance clustering is **strongly discouraged** in airgapped deployments or other scenarios where a customer is unable or unwilling to provide L3 support access to debug.

The following requirements must be met when clustering Secure Malware Analytics Appliances:

- **Version** - All Secure Malware Analytics Appliances must be running the same version to set up a cluster in a supported configuration; it should always be the latest available version.
- **Clust Interface** - Each Secure Malware Analytics Appliance requires a direct interconnect to the other Secure Malware Analytics Appliances in the cluster; a SFP+ must be installed in the Clust interface slot on each Secure Malware Analytics Appliance in the cluster (not relevant in a standalone configuration).

  Direct interconnect means that all Secure Malware Analytics Appliances must be on the same layer-two network segment, with no routing required to reach other nodes and no significant latency or jitter. Network topologies where the nodes are not on a single physical network segment are not supported.

- **Data** - A Secure Malware Analytics Appliance can only be joined to a cluster when it does not contain data (only the initial node can contain data). Moving an existing Secure Malware Analytics Appliance into a data-free state requires the use of the database reset process (available in v2.2.4 or later).



Important Do not use the destructive Wipe Appliance process, which removes all data and renders the application inoperable until the Field installer procedure is executed..

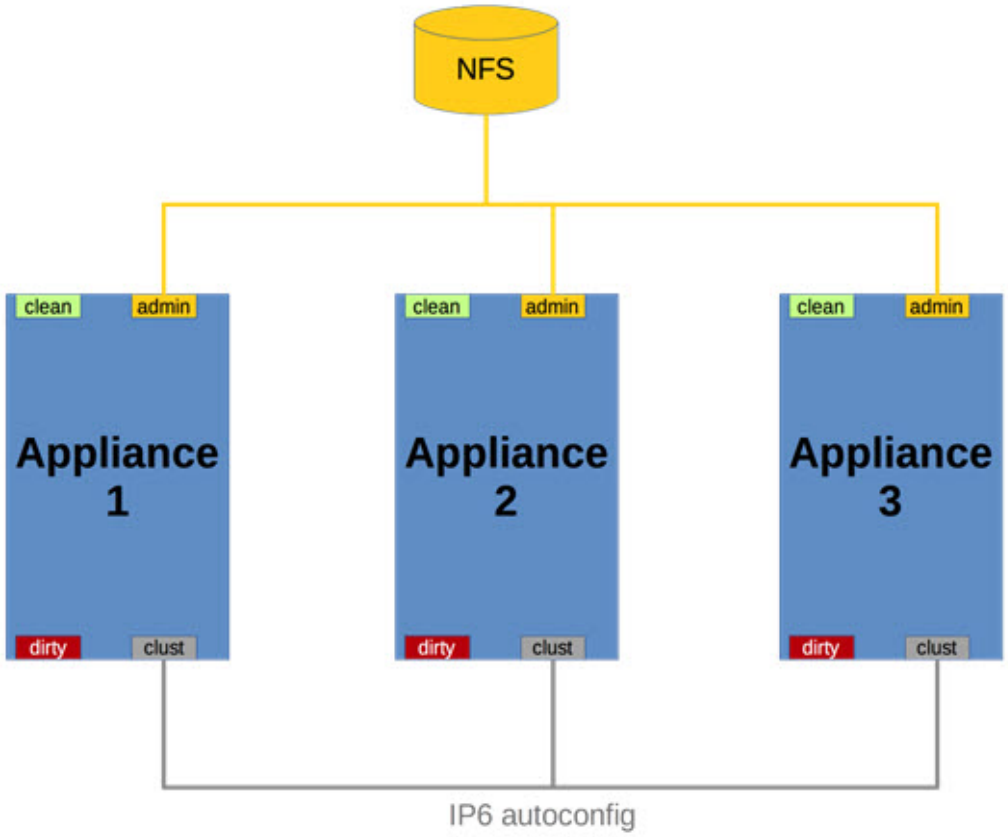
- **SSL Certificates** - If you are installing SSL certificates signed by a custom CA on one cluster node, then the certificates for all of the other nodes should be signed by the same CA.

Networking and NFS Storage

Clustering Secure Malware Analytics Appliances requires the following networking and NFS storage considerations:

- Secure Malware Analytics Appliance clusters require a NFS store to be enabled and configured. It must be available via the Admin interface and accessible from all cluster nodes.
- Each cluster must be backed by a single NFS store with a single key. While that NFS store may be initialized with data from a pre-existing Secure Malware Analytics Appliance, it must not be accessed by any system that is not a member of the cluster while the cluster is in operation.
- The NFS store is a single point of failure, and the use of redundant, highly reliable equipment for that role is essential.
- The NFS store used for clustering must keep its latency consistently low.

Figure 27: Clustering Network Diagram



Disaster Recovery in Cluster Mode

In cluster deployments, traditional appliance backup processes do not run because all data is stored on shared NFS storage.

Important You are responsible for backing up the NFS storage system. Consult your NFS server documentation for backup and snapshot capabilities to ensure data redundancy.

Building a Secure Malware Analytics Appliance Cluster

Building a Secure Malware Analytics Appliance cluster in a supported manner requires that all members be on the same version, which should always be the latest available version. This may mean that all of the members have to be built standalone first to get fully updated.

If the Secure Malware Analytics Appliance has been in use as a standalone appliance prior to clustering, only the data of the first member can be preserved. The others need to be reset as part of the build.

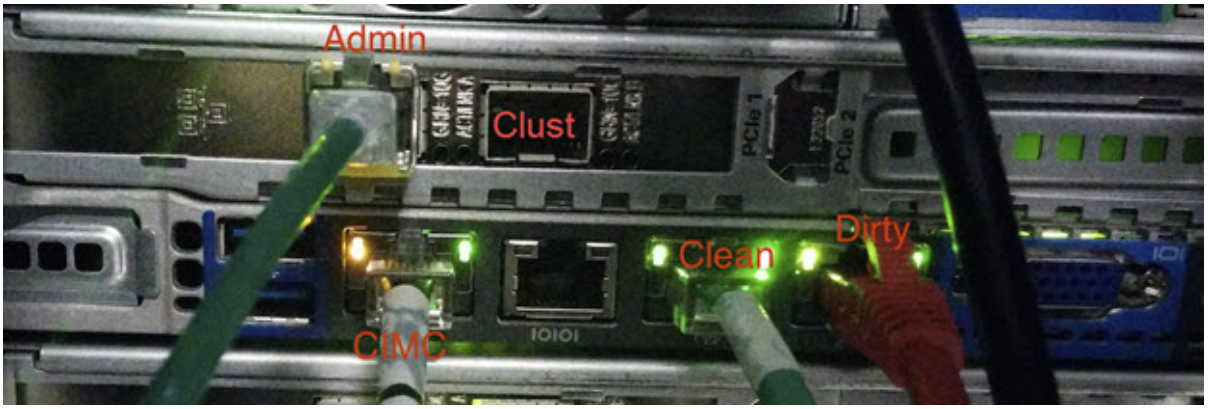
Start a new cluster with an initial node, and then join other Secure Malware Analytics Appliances to it. There are two distinct paths that are available for building a new cluster:

- Using an existing standalone Secure Malware Analytics Appliance
- Using a new Secure Malware Analytics Appliance

Clust Interface Setup

Each appliance in the cluster requires an additional SFP+ for the Clust interface. Install a SFP+ module in the fourth (non-Admin) SFP port. On the M5, this is the second SPF interface from the left (see the Cisco Threat Grid M5 Hardware Installation Guide for more information).

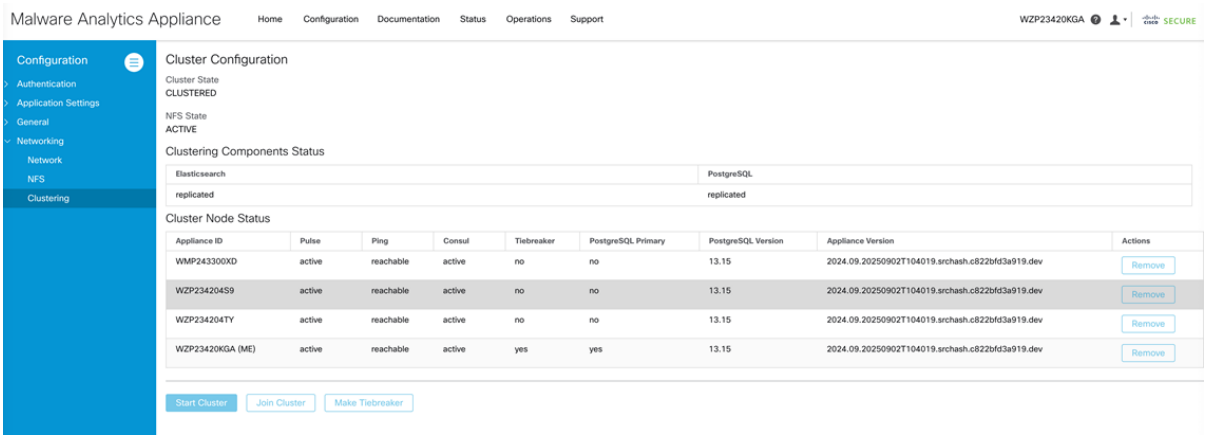
Figure 28: Clust Interface Setup for Cisco UCS M4 C220



Cluster Configuration

Clusters are configured and managed in the OpAdmin on the **Cluster Configuration** page (**Configuration** > **Networking** > **Clustering**). This section describes the fields on this page to gain an understanding of an active and healthy cluster (the screenshot shows a cluster with three nodes).

Figure 29: Cluster Configuration for Active Cluster



Cluster Prerequisites

- The appliance must be fully set up and configured.

- The NFS State must be **Active**.

Cluster State

- **Unconfigured** - Not yet configured as explicitly part of a cluster or as a standalone Secure Malware Analytics Appliance; you make this choice in the initial setup wizard if the prerequisites for clustering have been met.
- **Pending_NFS_Enable** - Cluster is pending NFS enablement.
- **Pending_NFS_Key** - Cluster is pending NFS key.
- **Standalone** - Appliance is configured as a standalone node; cannot be configured as part of a cluster without a reset.
- **Clustered** - Is clustered with one or more other Secure Malware Analytics Appliances.
- **Unknown** - Status cannot be determined.

Clustering Components Status

- **Elasticsearch**- The service used for queries that require search functionality.
- **PostgreSQL** - The service used for queries that require up-to-date, definitive data (such as account lookups).

Both services are described with one of the following status values:

- **Replicated** - Everything is working properly. Additionally, everything required to take over on failure is also in place. The appliance is able to tolerate failure and continue working. Being in a replicated state does not mean that a failure will have zero downtime. Rather, a failure should entail zero data loss and constrained downtime (less than a minute in normal circumstances, with the exception of any active analysis on the specific cluster node that fails).

  Maintenance operations that bring down nodes should only be performed when the cluster is in the replicated state.

  For a fully replicated cluster, recovery should be automatic and require less than a minute to complete in any normal scenario.
- **Available** - Everything is working properly and the referenced service is available for use (that is, it can service API and user requests), but it is not replicated.
- **Unavailable** - The service is known to be non-functional.

For more information, see the *Secure Malware Analytics Appliance Clustering FAQ* on Cisco.com.

Cluster Nodes Status

- **Pulse** - Indicates whether the node is actively connected to and using the NFS store (not during initial setup, but while running services).
- **Ping** - Describes whether the cluster node can be seen over the Clust interface.
- **Consul** - Indicates whether the node is participating in the consensus store. This requires both a network connection over Clust and a compatible encryption key.

- **Postgres Primary** - Indicates whether the node is the PostgreSQL primary node.

Start Building Cluster from Existing Standalone Appliance

When you start building a cluster of Secure Malware Analytics Appliances, you must start the cluster with the first node being either an existing standalone Secure Malware Analytics Appliance or a new appliance. This section describes how to build a cluster from an existing standalone Secure Malware Analytics Appliance, which allows you to preserve existing data from one appliance and use it to start a new cluster.



Note

- An existing backup must be available on NFS from which the cluster is started.
- All other nodes to be joined to the cluster must have data removed before joining; the data from additional nodes cannot be merged into the cluster.

Perform the following steps to start building the first node in a cluster from an existing standalone appliance:

Procedure

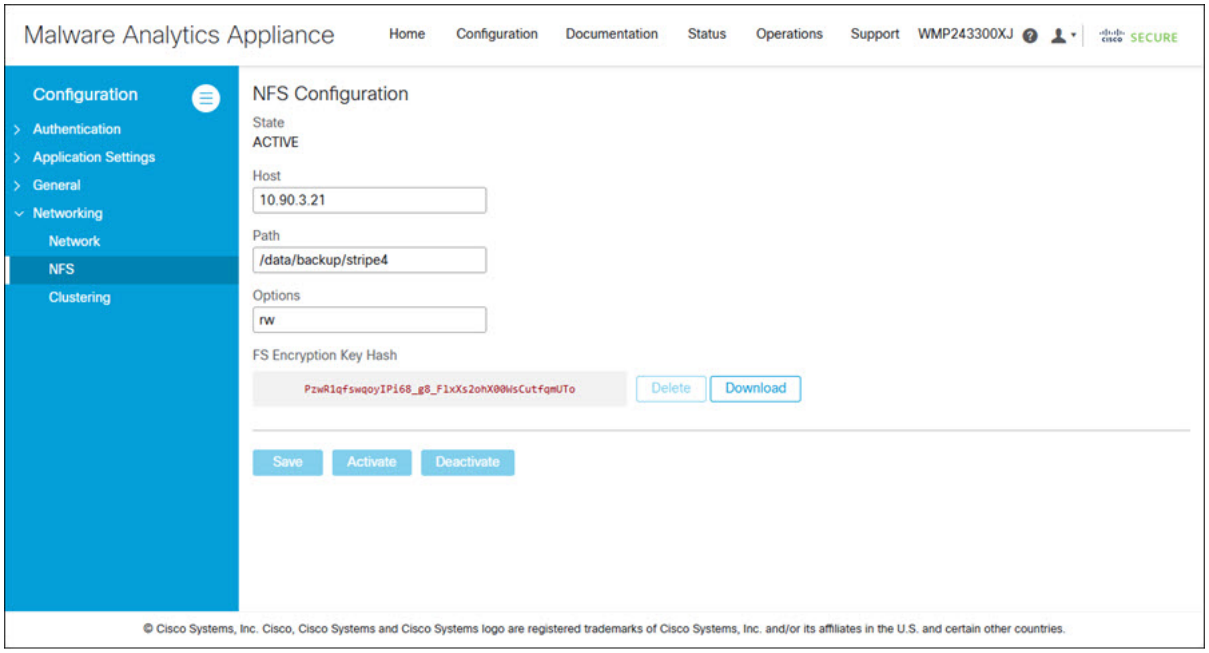
Step 1 Fully update the Secure Malware Analytics Appliance to the latest version. Depending on which version is currently running, this may require more than one update cycle to reach the latest version.

Step 2 If not already completed, configure NFS for backup of the appliance:

Note
This step describes the default Linux NFS server implementation; it may be different for your server setup.

a) Navigate to **Configuration** > **Networking** > **NFS**

Figure 30: NFS Configuration



b) Complete the following fields:

- **`Host`** - The NFSv4 host server. We recommend using the IP address.
- **`Path`** - The absolute path to the location on the NFS host server where files will be stored. This does not include the Key ID suffix, which will be added automatically.
- **`Options`** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

c) Click **Save**.

The page refreshes and the **Generate Key** button becomes available.

The first time you configure this page, the **Remove** and **Download** buttons are available for removing and downloading the encryption key.

The **Upload** button is available if you have NFS enabled but no key created. Once you create a key, the **Upload** button changes to **Download**. If you delete the key, the **Download** button becomes **Upload** again.

Note
If the key correctly matches the one used to create a backup, the **KeyID** displayed in the OpAdmin after upload should match the name of a directory in the configured path. Backups cannot be restored without the encryption key. The configuration process includes the process of mounting the NFS store, mounting the encrypted data, and initializing the appliance's local datastores from the NFS store's contents.

d) Click **Generate Key** to generate a new NFS encryption key.

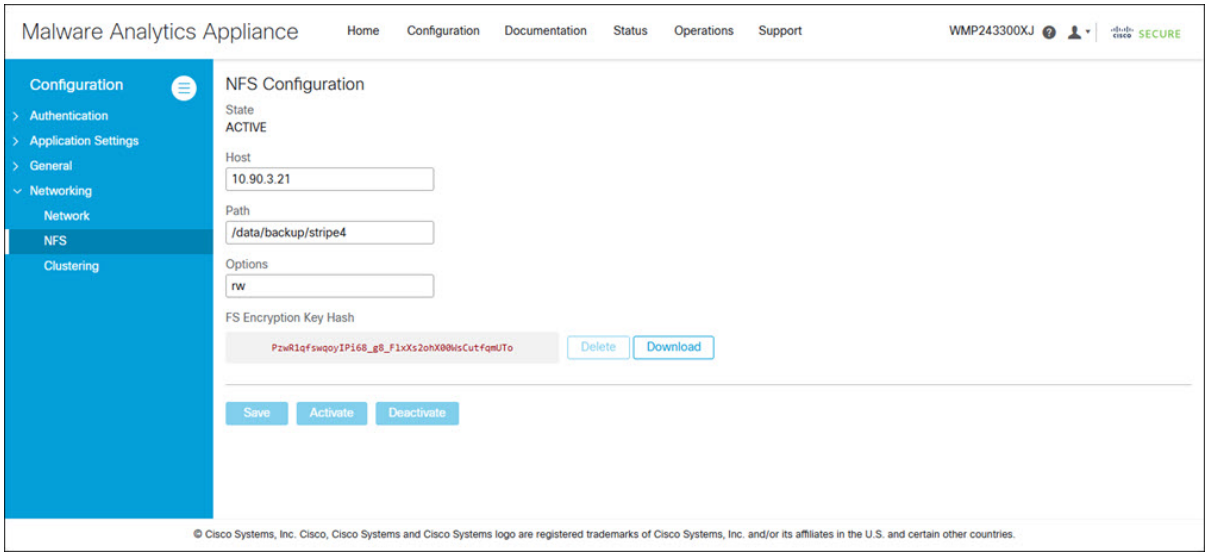
e) Click **Save**.

The page refreshes and the **Key ID** is displayed; the **Activate** and **Download** buttons become available.

f) Click **Activate**.

After a few seconds, the **State** becomes **Active**.

Figure 31: NFS Active



g) Click **Download** to download the backup encryption key. Save the generated file in a secure location. You will need the key for joining additional nodes to the cluster.

Important
If this step is missed, all data will be lost in the following steps.

Step 3 Complete the configuration, as needed, and reboot the Secure Malware Analytics Appliance to apply the NFS backup configuration.

Step 4 Perform a backup.

Note
If you do the backup at least 48 hours in advance, as recommended, and there are no service notices indicating problems with the backup, then the following manual steps are unnecessary.

Backup and other service notices are available in the Secure Malware Analytics portal UI from the icon in the upper-right corner. If a service notice **There is no PostgreSQL backup yet** is displayed, DO NOT PROCEED.

If you want your backup to be useable without waiting for 48 hours then manually initiate a backup of all data to NFS to ensure it's complete. Performing the manual backup is only necessary if you are setting up backup immediately before rebuilding the standalone appliance in a cluster.

a) Open **tgsh** and enter the following commands:

```
service start tg-database-backup.service
service start freezer-backup-bulk.service
service start elasticsearch-backup.service
```

Figure 32: Initiating a Backup of All Data to NFS



b) Wait about 5 minutes after the last command returns.

Step 5 In the Secure Malware Analytics portal UI, check for service notices. If any notices indicate a backup process failure, such as a warning that there is no PostgreSQL backup yet, then DO NOT PROCEED.

Important
Do not continue unless these processes have completed successfully.

Step 6 Navigate to **Configuration** > **Networking** > **Clustering**

Step 7 Click **Start Cluster**.

Step 8 On the confirmation dialog, click **OK**.

The **Clustering Status** changes to **Clustered**.

Step 9 Finish the installation. This initiates a restore of the data in cluster mode.

What to do next

Now you can begin joining other Secure Malware Analytics Appliances to the new cluster, as described in Joining Appliances to a Cluster.

Start Building Cluster with New Appliance

When you start building a cluster of Secure Malware Analytics Appliances, you can start the cluster with the first node being new Secure Malware Analytics Appliance. This method of building a cluster can be used for new appliances that are shipped with cluster-capable versions of the software, or for existing appliances that have had their data reset.

Note Remove existing data with the `destroy-data` command, as documented in Reset Secure Malware Analytics Appliance as Backup Restore Target. Do not use the Wipe Appliance feature.

Procedure

Step 1 Set up and begin the OpAdmin configuration as normal.

Step 2 Configure the Network and License.

Step 3 Navigate to **Configuration** > **Networking** > **NFS**

Note
For more information, refer to the images in Start Building a Cluster from Existing Standalone Appliance.

Step 4 Complete the following fields:

- **`Host`** - The NFSv4 host server. We recommend using the IP address.
- **`Path`** - The absolute path to the location on the NFS host server where the files will be stored. This does not include the Key ID suffix, which will be added automatically.
- **`Options`** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

Step 5 Click **Save**.

The page refreshes, and the **Generate Key** and **Activate** buttons become available.

Step 6 Click **Generate Key** to generate a new NFS encryption key.

Step 7 Click **Activate**.

The **State** changes to **Active**.

Step 8 Click **Download** to download a copy of the encryption key for safekeeping. You will need the key for joining additional nodes to the cluster.

Step 9 On the **Cluster Configuration** page, click **Start Cluster**, and then click **OK** on the confirmation dialog.

The **Clustering State** changes to **Clustered**.

Step 10 Complete the remaining steps in the wizard and click **Start Installation**. This initiates a restore of the data in cluster mode.

Step 11 Open the **Cluster Configuration** page and check the health of the new cluster.

What to do next

Proceed to Join Secure Malware Analytics Appliances to Cluster.

Joining Secure Malware Analytics Appliances to a Cluster

This section describes how to join new and existing Secure Malware Analytics Appliances to a cluster.

Note A Secure Malware Analytics Appliance can be joined to an existing cluster only when it contains no data; unlike the initial appliance, which may contain data.

Also, it is critically important that the Secure Malware Analytics Appliance that is joining a cluster has the latest software version installed (all nodes in a cluster must be running the same version). This may require setting up the Secure Malware Analytics Appliance and update it, then reset the data, and join it to the cluster.

Add one node at a time, and wait for Elasticsearch and PostgreSQL to reach the state of **Replicated** before adding the next node. The **Replicated** status is expected in clusters of two or more nodes.

Note The wait for the state change for Elasticsearch and PostgreSQL to reach **Replicated** does not apply to the single-node case. If you are initializing a single-node cluster from a backup, you should wait for the restore to be completed and the application to be visible in the UI before adding the second node.

When joining a Secure Malware Analytics Appliance to a cluster, the NFS and clustering must be configured during the initial setup.

Joining Existing Appliances to a Cluster

Perform the following steps to join an existing Secure Malware Analytics Appliance to a cluster:

Procedure

Step 1 Update the Secure Malware Analytics Appliance to the latest version. This may require several update cycles depending on the current version that is installed. All nodes in a cluster must be the same version.

Step 2 Run the `destroy-data` command in **tgsh** to remove all data; when joining an existing Secure Malware Analytics Appliance to a cluster, all data must be removed prior to being merged into the cluster. See Reset Secure Malware Analytics Appliance As Backup Restore Target.

After running the `destroy-data` command on an existing Secure Malware Analytics Appliance, it basically becomes a new node, and joining it to a cluster follows the same steps as Joining New Appliances to a Cluster.

Joining New Appliances to a Cluster

Perform the following steps to join a new Secure Malware Analytics Appliance to a cluster:

Procedure

Step 1 Begin the new OpAdmin configuration as described in the Cisco Secure Malware Analytics Appliance Getting Started Guide.

Step 2 In the **NFS Configuration** page, specify the **Host** and **Path** to match the configurations you entered in first node in the cluster.

Step 3 Click **Upload** for **FS Encryption Key Hash** and choose the NFS encryption key you downloaded from the first node when you started the new cluster.

Step 4 Click **Save**.

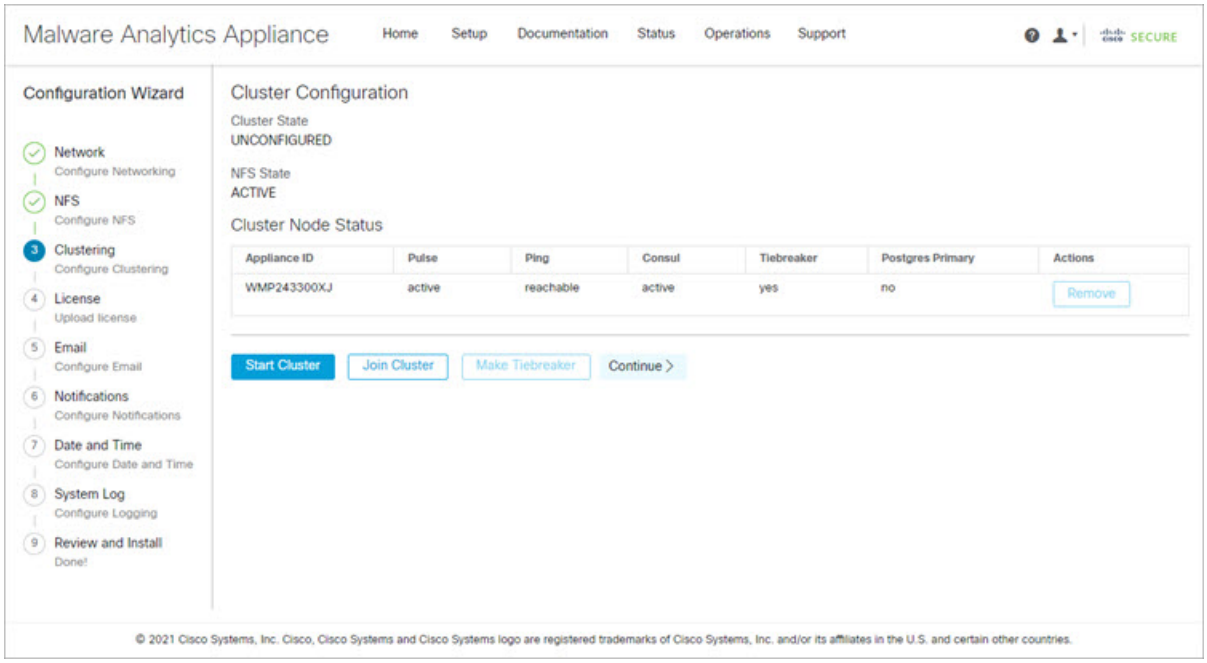
The page refreshes; the **Key ID** is displayed and the **Activate** button is enabled.

Step 5 Click **Continue**.

Cluster Configuration screen appears with the first node.

Step 6 Click **Join Cluster** and then click **OK** on the confirmation dialog.

Figure 33: Cluster Configuration



The **Cluster State** changes to **Clustered**.

Step 7 Repeat the Step 1 through Step 10 for each node you want to join to the cluster.

Removing a Cluster Node

To remove a node from a cluster, navigate to the **Cluster Configuration** page (**Configuration > Clustering**) and click **Remove** in the **Action** column for the node to be removed.

- Removing a node from the cluster indicates that it should no longer be considered part of the cluster, rather than a node that is temporarily down. You should remove a Secure Malware Analytics Appliance when it is being decommissioned; either being replaced with different hardware or will be rejoined to a cluster only after its data has been reset.
- Removing a node indicates to the system that you are not going to re-add a node, or if you do re-add it, it has been reset.
- A node is not marked as having been permanently removed from a cluster if it has pulse (is actively writing to NFS), or is active on consul (part of the consensus store).

To replace a still-live node (in a cluster with less than seven nodes), add the new node, wait for the cluster to go green, then remove the old one offline using the **Remove** button. This alerts the system that it's not coming back.

When you first take the node offline, the cluster status changes to yellow. After you click **Remove**, the status reverts back to green (since the cluster will resize such that it no longer expects the now-removed node to be present).



Tip A node that is missing (failed or powered down) will eventually time out and be available to remove.

Resizing a Cluster

When a node is removed from a cluster using the **Remove** button, the cluster resizes; this may affect the number of failures it is expected to tolerate. If a cluster is resized in such a way as to change the number of expected failure tolerances (as defined in Failure Tolerances), it will force an Elasticsearch restart, which will cause a brief service interruption.

Exception: This does not include a system other than the PostgreSQL master being rebooted or having a transient failure. Disruption should be minimal in that case except for clients actively using that node, or if samples are running on it.

If you add a Secure Malware Analytics Appliance that was not already part of the cluster, or if you click **Remove**, and this changes the cluster size such that the number of tolerated failures is changed, then there will be a brief interruption as the rest of the cluster reconfigures.

Failure Tolerances

In the event of a failure, clustered Secure Malware Analytics Appliances will not lose any data, with the exception of any analysis being actively run by the failed node, and will recover service with a minimal (less than one minute) service disruption period and no user involvement.

Most failures will recover in less than a minute if the number of available nodes is not smaller than the number shown in the **Nodes Required** column in the **Failure Tolerances** table; or will recover after the number of available nodes increases to meet that count. This is true if the cluster was in a healthy state prior to failures (as indicated by services listed as **Replicated** on the **Clustering** page).

The number of failures a cluster of a given size is expected to tolerate is shown in the following table.

Table 1: Failure Tolerances

Cluster Size	Failures Tolerated	Nodes Required
1	0	1
3	1	2
4	1	3
5	2	3
6	2	4
7	3	4

These figures represent best-case scenarios. If the cluster is not showing green across the board when all nodes are up, then it may not be able to tolerate the full failure count indicated.

For example, if you have a 5-node cluster size with 2 failures tolerated, 3 nodes required, and all 5 appliances are actively processing data, the cluster will be able to reconfigure itself and continue operation without human administrative action if up to 2 failures take place.

Another consideration, in a 5-, 6-, or 7-node cluster, the +1 in the number of failures tolerated means that the percentage of nodes that can fail is higher, which is particularly important because the number of nodes acts as a multiplier to the failure rate. (If you have two nodes, and each has a hardware fault once every 10 years, then you just change your hardware fault rate to once every 5 years.)

Failure Recovery

Most failures recover automatically. If not, you should contact Cisco Support, or restore the data from backups. See Restore Backup Content for more information.

API/Usage Characteristics

Status of samples submitted to any node in a cluster may be queried from any other node in the cluster; there is no need to track to which individual node a submission took place.

Processing of sample submissions made to one node will be split across all nodes in the cluster; there is no need to actively load-balance from the client side.

Operational/Administrative Characteristics

Service may be temporarily disrupted during a failover event; samples which were actively running during a failover will not be automatically rerun.

In the context of clustering, capacity refers to throughput, not storage. A cluster with three nodes prunes data to the same maximum storage levels as a single Secure Malware Analytics Appliance. Consequently, a cluster of three 5000-sample appliances, with a total 15,000-samples/day rate limit, will (when used at full capacity), have retention minimums of 33 percent shorter than the 10,000-sample/day estimates provided in the *Threat Grid Appliance Data Retention Notes* on Cisco.com.

Sample Deletion

Support for deleting samples is available on Secure Malware Analytics Appliance:

- The **Delete** option is available in the **Actions** menu in the samples list.

- The **Delete** button is available in the upper-right corner of the sample analysis report.

Note It may take up to 24 hours for backup copies of deleted samples to be removed from all nodes.

Deleted samples are removed from the shared NFS store immediately; removed from the node processing the deletion request immediately, but the other nodes will lag until the nightly cron job is run. In clustered mode, the NFS store is considered the primary source for samples, so even if the sample is not physically removed from other nodes, it should no longer be retrievable from any of them.

In Secure Malware Analytics Appliance, sample deletion is extended to include artifacts, which matches the behavior of the cloud product.

Cluster restoration

The cluser restoration process wipes all clustering information during the restore process. This action effectively brings the appliance to a state similar to a standalone installation, allowing it to start from a clean slate and restores a clustered database from a backup.

Key limitations and important considerations

It is vital to be aware of the following limitations before attempting a cluster restore:

- **Standalone vs. Cluster compatibility**: You cannot restore a standalone database inside a cluster, nor can you restore a cluster inside a standalone. Consequently, a cluster backup must be restored on a cluster, and a standalone backup must be restored on a standalone.
- **Converting standalone to cluster**: If you want to make a standalone system a cluster after it has been reinstalled, you can follow the normal procedure to do so.
- **What is restored**: The restoration process includes sample files, sample reports, analysis results, and the database that holds this information together. The restore involves the database, Elasticsearch indexes, and files located in the freezer. For large restores, the files in the freezer can take a considerable amount of time to restore.
- **What is not restored**: The restoration process does not include the firmware or system configuration. For these reasons, a full reinstall is often necessary before a restore, as the process only brings back data, not the underlying system or its configuration.
- **New cluster state**: The target appliance for the new cluster must be in an initial state.

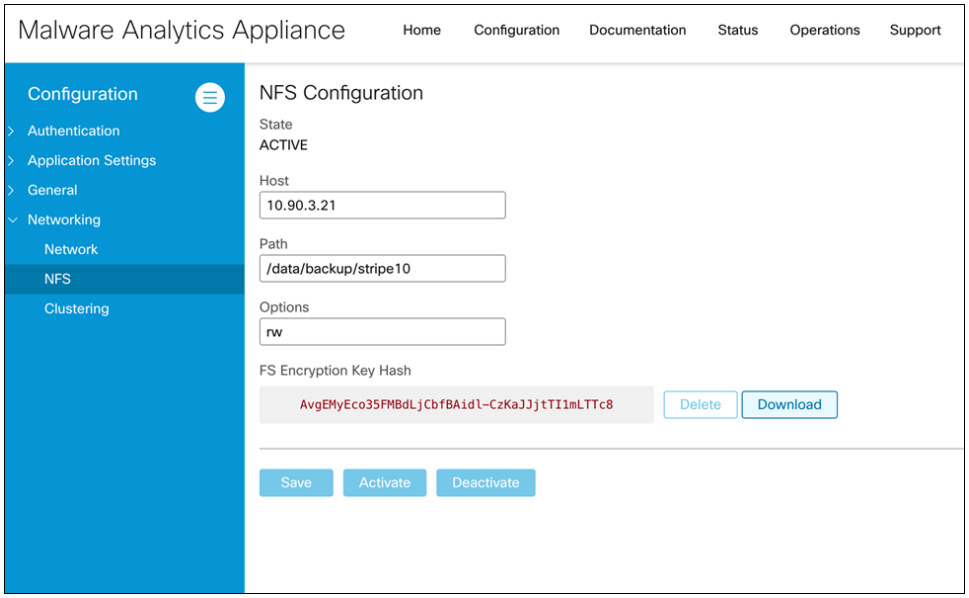
Cluster Restoration process

Perform the following steps to restore your Secure Malware Analytics Appliance cluster:

Before you begin

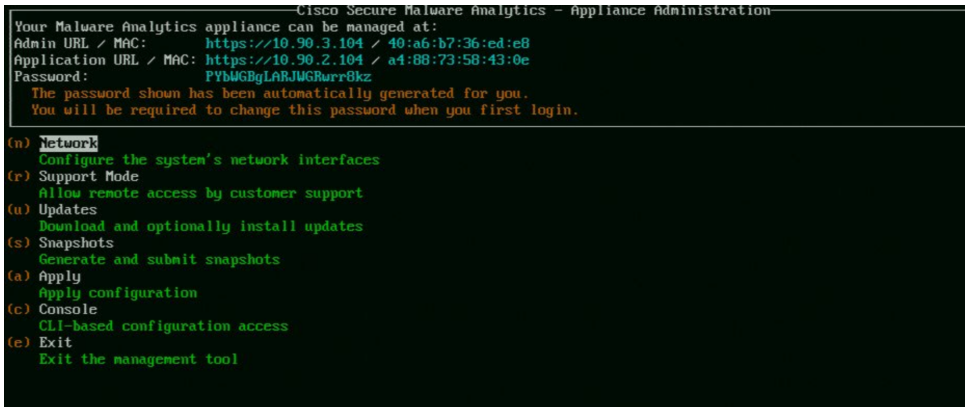
- **NFS key:** You must have the NFS encryption key for the specific backup you want to restore. This key can be downloaded from the original appliance. To download NFS key - in OpAdmin, navigate to **Networking** > **NFS** and click **Download**.

Figure 34: Download - NFS Key



- **New Appliance in Initial State:** The target appliance for the new cluster must be in an initial state with default passwords and an unconfigured network. If it is not, you must wipe its data.

Figure 35: Cluster node in intial state



Procedure

Step 1 **Prepare the target appliance**: The appliance you are restoring to must be a newly received one or have its data destroyed to be in an initial state.

a) Access the admin TUI, then select **Console** → **Tgsh**

b) Execute destroy-data command. This command (`destroy-data REALLY_DESTROY_MY_DATA`) will wipe all the data.

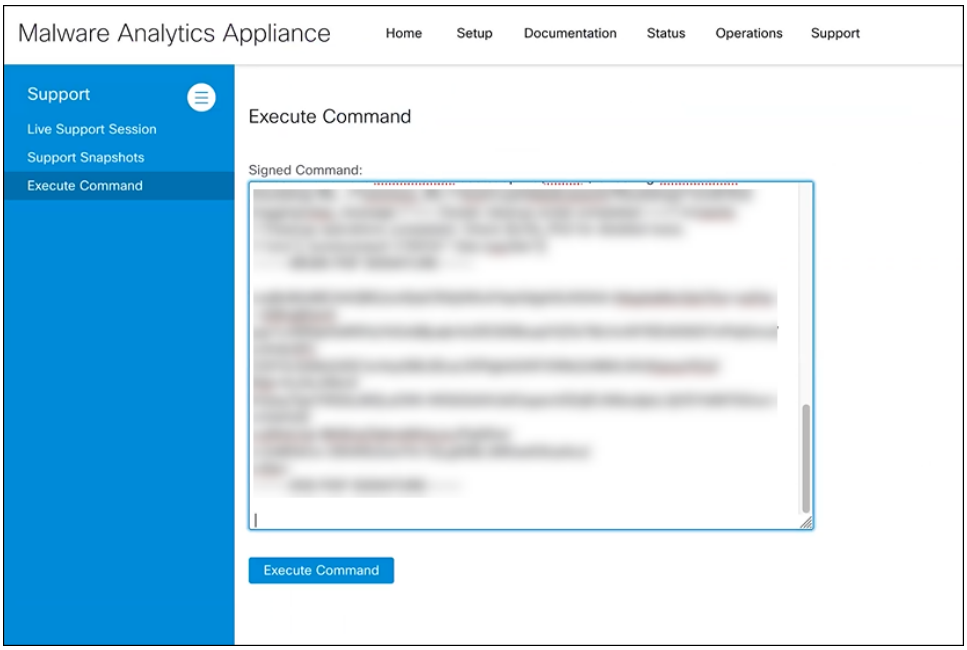
Warning
This is irreversible. It erases all data, configuration, NFS credentials, and the local encryption key. After completion, the appliance will reboot (possibly multiple times) and display a new system-generated password.

Step 2 **Configure Network**: In the OpAdmin, configure the network settings to ensure proper connectivity. The initial setup, installation, and configuration wizard is described in the Cisco Secure Malware Analytics Appliance Getting Started Guide.

Step 3 **Configure NFS Key**: You must possess the **NFS encryption key** for the specific backup you wish to restore. Upload this key to the new appliance's NFS configuration page.

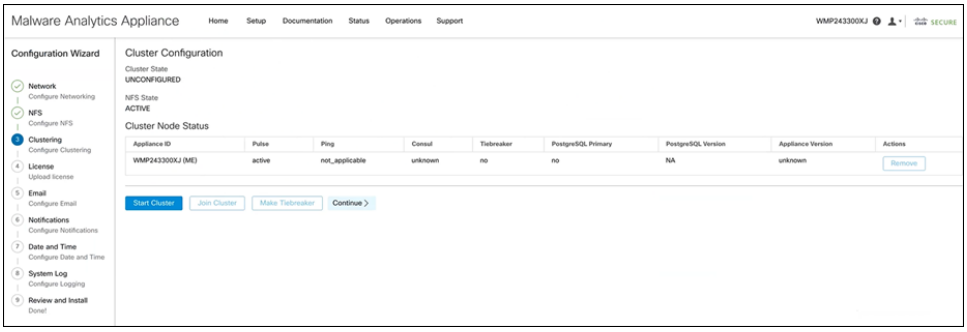
Step 4 **Execute the Signed Command**: Navigate to **Support** > **Execute Command**. You will need to request a specific signed command from support that clears the old cluster information. This command wipes all clusters and is highly sensitive, customized for your appliance, and has a limited validity period. Paste it in the **Signed Command** field and click **Execute Command**.

Figure 36: Cluster node in intial state



Step 5 **Start the Cluster**: Go back to the clustering page in the wizard and click **Start cluster**.

Figure 37: Cluster node in intial state



Step 6 **Continue Installation**: Proceed with the standard installation steps.

Step 7 **Monitor the Restore Process**: You will now enter a period where the system indicates that a **restore is occurring**. This state can last for a considerable amount of time.

The restoration involves three main components:

- Database restore
- Elastic search restore
- Freezer file restore

The restore of files in the freezer can be extremely lengthy, especially with large datasets. For example, restoring 167,000 submissions with approximately 700GB of samples and reports takes close to 3 hours and 30 minutes.

Note
There is no progress bar during the restore process. For large restores, it appears as if the install has hung. The OpAdmin will report that the restore has succeeded, and the appliance will start up.

Standalone restoration procedure

Perform the following steps to restore your Secure Malware Analytics standalone appliance cluster:

Procedure

Step 1 **Prepare the Target Appliance**: The appliance you're restoring to must be a newly received one or have its data destroyed to be in an initial state. This can be done by using the destroy-data command .

Step 2 **Configure Network**: Configure the network settings.

Step 3 **Configure NFS Key**: You must possess the **NFS encryption key** for the specific backup you wish to restore. Upload this key to the new appliance's NFS configuration page.

Step 4 **Access Clustering Page**: Access the clustering page.

Step 5 **Remove Node**: If the appliance was previously part of a cluster, remove the node from the cluster table using the remove button.

Step 6 **Do Not Start Cluster**: Do not start the cluster as you are in a standalone configuration. If you intend to convert it into a cluster, wait until the initial restoration is performed.

Step 7 **Continue Installation**: Proceed with the standard installation steps.

What to do next

Post-Restore Verification

Once the restoration process is complete, validate that expected data are present and the appliance behaves properly.

PostgreSQL Cluster Database upgrade

Why the Upgrade is Necessary

SMA version 2.20.0 includes a critical upgrade for the underlying database. Previously, appliance were running PostgreSQL version 9.6, an old and unsupported version.

This mandatory upgrade to **PostgreSQL version 13.5** is vital for two key reasons:

1. **Security :PostgreSQL 9.6 is unsupported**, making the upgrade necessary to maintain a secure operating environment and ensure compliance.
2. **Functionality:** The upgrade is required to support advanced database functions used by the cloud component. This ensures your appliance can stay current with features available in the cloud version.

Upgrade scenarios

The method of database upgrade depends on the appliance configuration

Configuration	Upgrade Behavior	Administrator Action
Standalone Appliance	Automatic/Seamless	None required; upgrade happens automatically during the software upgrade (e.g., 2.19.6 to 2.20.0).
Cluster (One Node)	Automatic/Seamless	None required; upgrade happens automatically during the software upgrade to 2.20.0.
Cluster (More than One Node)	Manual Trigger	The administrator must manually trigger the upgrade to ensure proper synchronization and replication across all nodes.

PostgreSQL Upgrade in a Multi-Node SMA Cluster

This manual process is required to ensure data integrity and synchronization across all nodes when moving from PostgreSQL 9.6 to 13.15. **You must be logged into the primary node** and ensure all prerequisites are met before beginning.

Before you begin

The following conditions must be met before you can manually trigger the database upgrade. If any of these conditions are not met, the **Upgrade PostgreSQL** button will be grayed out.

- **Uniform Appliance Version:** All nodes in the cluster must be upgraded to same SMA software version.
- **PostgreSQL Primary:** You must be logged into the node that is currently the PostgreSQL Primary.
- **Replicated State:** The cluster must be fully operational and in a **Replicated** state to confirm all nodes are synchronized.
- **Maintenance Window (Recommended):** It is advised to perform this task when the cluster is not actively processing samples (i.e., during a scheduled maintenance window).

Procedure

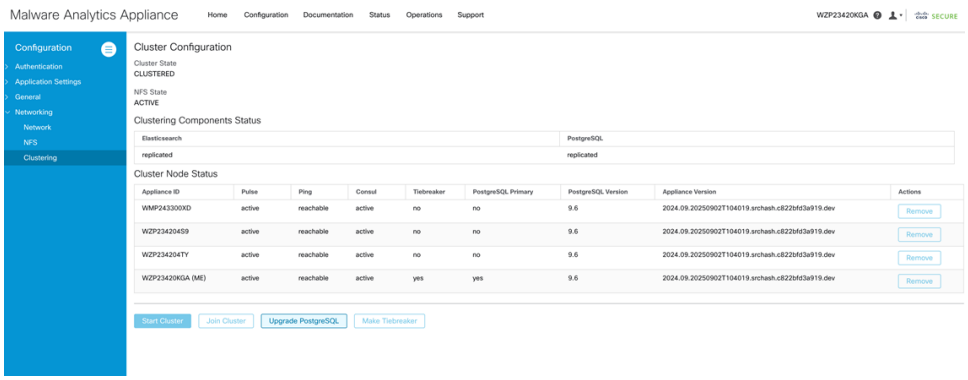
Step 1 Navigate to **Configuration** > **Networking** > **Clustering**.

Step 2 In the **Cluster Node Status** table, verify the following: .

- **PostgreSQL Primary:** Confirm the node you are logged into shows `yes` under the **PostgreSQL Primary** column (e.g., WZP2342WNDA (ME) in the image below).

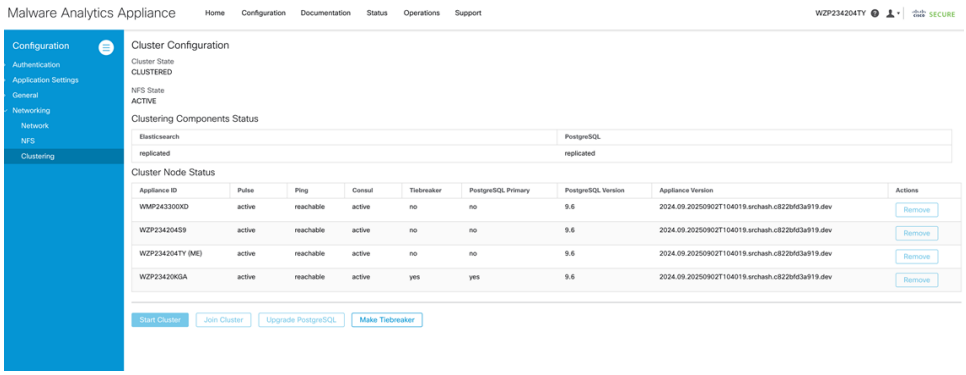
- **PostgreSQL Version:** Ensure all nodes are still on version **9.6** and the **Appliance Version** is uniform (meaning all nodes have been successfully upgraded to 2.20.0).

Figure 38: Clustering window - the Upgrade PostgreSQL is active if the node is primary



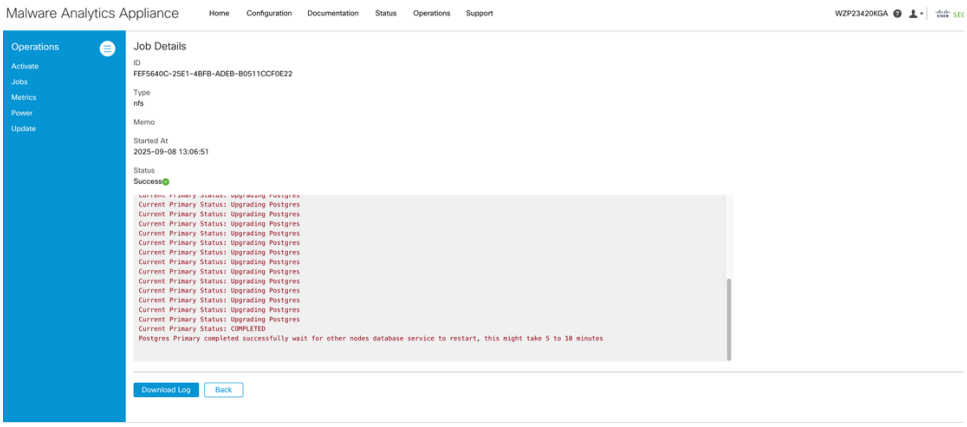
Example:

Figure 39: Clustering window - the Upgrade PostgreSQL is not active if the node is not primary



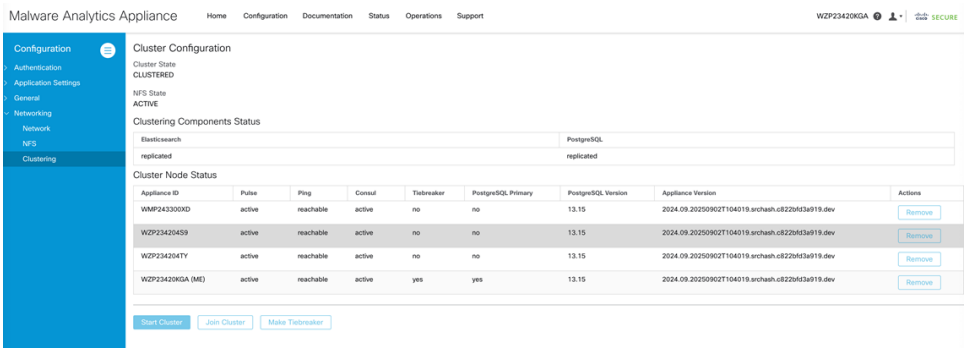
Step 3 Click the **Upgrade PostgreSQL** .
The **Upgrading PostgreSQL** window appears, you can click on the **Full Output** to view the progress and the status will change to **Success** after primary node installation is complete. Once the primary node is complete, all the other nodes are restarted and upgraded to PostgreSQL 13.15.

Figure 40: Upgrading PostgreSQL - Success message after the upgrade



Step 4 Navigate back to **Configuration** > **Networking** > **Clustering** to verify the final status of all the nodes.

Figure 41: Upgrading PostgreSQL - All nodes upgraded



All nodes in the cluster will be running **PostgreSQL version 13.5**.

The **Upgrade PostgreSQL** button will disappear from the clustering window, as the task is complete.