cohesive networks

VNS3:ms 2.0.0+ Configuration Guide

Table of Contents

Introduction

Monitor all virtual networks from a single network console

A single dashboard to manage and monitor VNS3 networks plus all underlying cloud VLAN network components (CIDR, subnets, route tables, ACLs, security groups, etc.).

VNS3:ms Hierarchical Taxonomy for Network Objects

- **Virtual Network** — Made up of one or more connected VNS3 Topologies and Cloud VLANs
  - **VNS3 Topology** — Made up of one VNS3 Controller or a Mesh of VNS3 Controllers creating an Overlay Network
    - **VNS3 Controllers** — Single VNS3 Controller instance
      - **Overlay Client Servers**
      - **Unencrypted VLAN Client Servers**
  - **Cloud VLAN** — A Cloud Provided VLAN made up of one or multiple VPCs
    - **VLAN Components** — VPC made up of Addresses, Routes and Rules

VNS3:ms Monitors VNS3 Controllers and Cloud VLANs

This document assumes you have either a VNS3 deployment or Cloud VLAN you would like to manage and monitor via VNS3:ms.

See the specific instructions for your cloud setup and instance launch on our Product Resources page.

Please review the VNS3 Support Plans and Contacts before sending support inquiries. If you need specific help with project planning, POCs, or audits, contact our professional services team via sales@cohesive.net for details.

Requirements

- You have a cloud account that Cohesive can use for enabling your access to the VNS3:ms images.
- Ability to open the required hypervisor firewall rules to allow your VNS3:ms instance to access your VNS3 Controller instances
- Ability to create and add cloud API credentials to allow your VNS3:ms instance to access your cloud account.

- VNS3:ms currently only support the “underlay” (cloud network) view in AWS at this time. Support for Azure and Google is underway.

VNS3:ms System Requirements

- Minimum of 2GB memory
- Persistent Storage (EBS-backed at AWS or similar in other cloud environments)
- Minimum of 30GB storage
- VNS3 Controller version 3.5 or later for devices that will be monitored and managed by VNS3:ms (3.0 and earlier are usable but not fully supported)

Firewall Considerations

VNS3:ms instances use the following TCP ports:

- **VNS3:TCP port 80 or 443**
  Inbound HTTP/HTTPS access on the VNS3:ms instance is required for the admin UI and/or API. TCP port 80 or 443 must be accessible from the hosts where you want to want to manage and monitor your virtual networks.

- **TCP port 8000**
  Port used to access the individual VNS3 Controller instance via the VNS3 API. Each VNS3 Controller that will be added to the VNS3:ms system must have inbound TCP port 8000 access open from the VNS3:ms instance's public IP.

- **TCP port 22**
  Only needed in support situations where you have requested Cohesive support staff to access your VNS3:ms instance to diagnose/troubleshoot an issue.

Remote Support

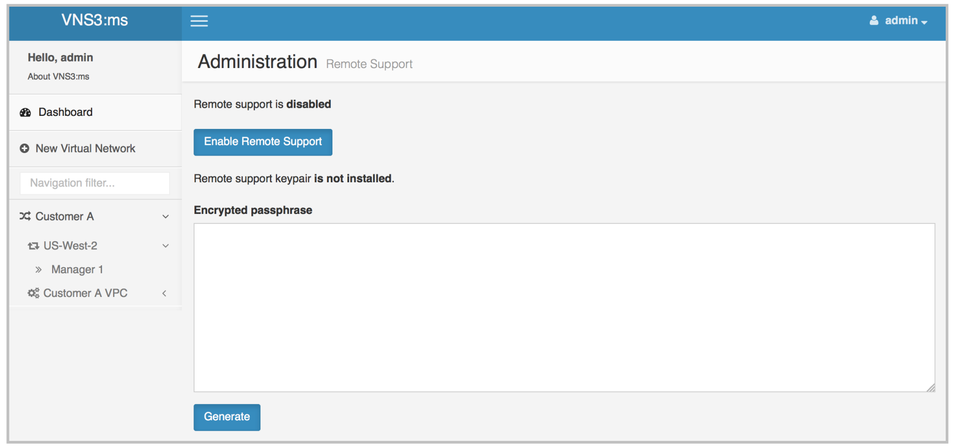
Note that TCP 22 (ssh) is not required for normal operations.

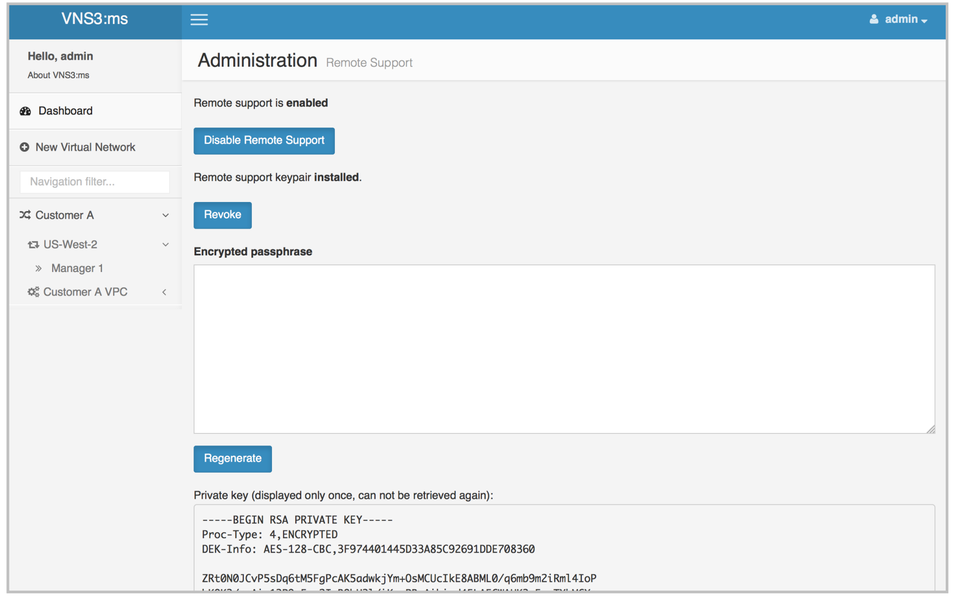
VNS3:ms has that same multi-party/multi-factor authentication system for Remote Support that all VNS3 products utilize.

Each VNS3:ms instance is running a restricted SSH daemon, with access limited only to Cohesive Networks for debugging purposes controlled by the user via the Remote Support toggle and key exchange generation.

In the event Cohesive Networks needs to observe runtime state of a VNS3:ms instance in response to a tech support request, we will ask you to open Security Group access to SSH from our support IP range and Enable Remote Support via the Web UI.

Cohesive Networks will send you an encrypted passphrase to generate a private key used by Cohesive Networks Support staff to access your Controller. Access to the restricted SSH daemon is completely controlled by the user. Once the support ticket has been closed you can disable remote support access and invalidate the access key.

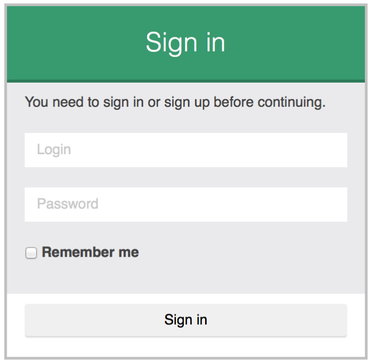




Startup and Initialization

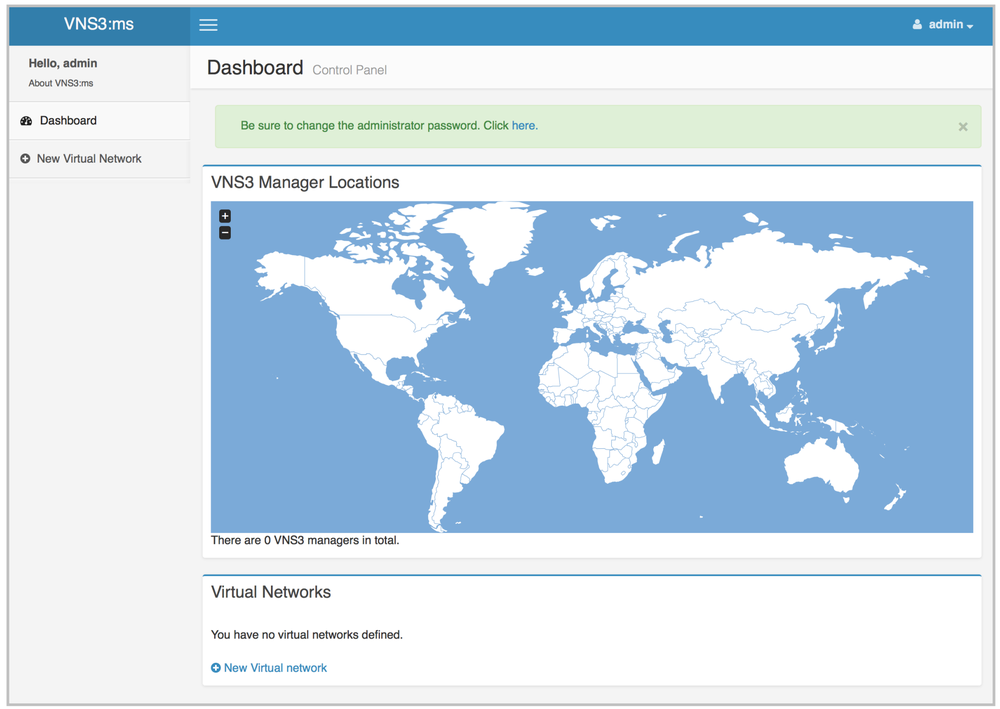
VNS3:ms Log in

When launching a VNS3:ms instance or VM, it is recommended a static public IP (e.g. Elastic IP) is associated and used. The use of the static IP allows remapping during instance version upgrades or DR failover scenarios.



Login to the VNS3:ms Web UI - https://<VNS3msIP>

Default username: *admin*
Default password: <*instance-id*> in AWS or *changeme* in other environments



Change VNS3:ms password and API key

VNS3:ms now includes safety features that restrict some functionality until the password and API key are changed from their default settings. As VNS3:ms can control your VNS3 deployments (and potentially your Cloud VLAN), it is important to select strong passwords and regenerate the API key to ensure the system is secure.

Cohesive Networks also recommends using two factor authentication for UI access. 2FA is covered on the following page.

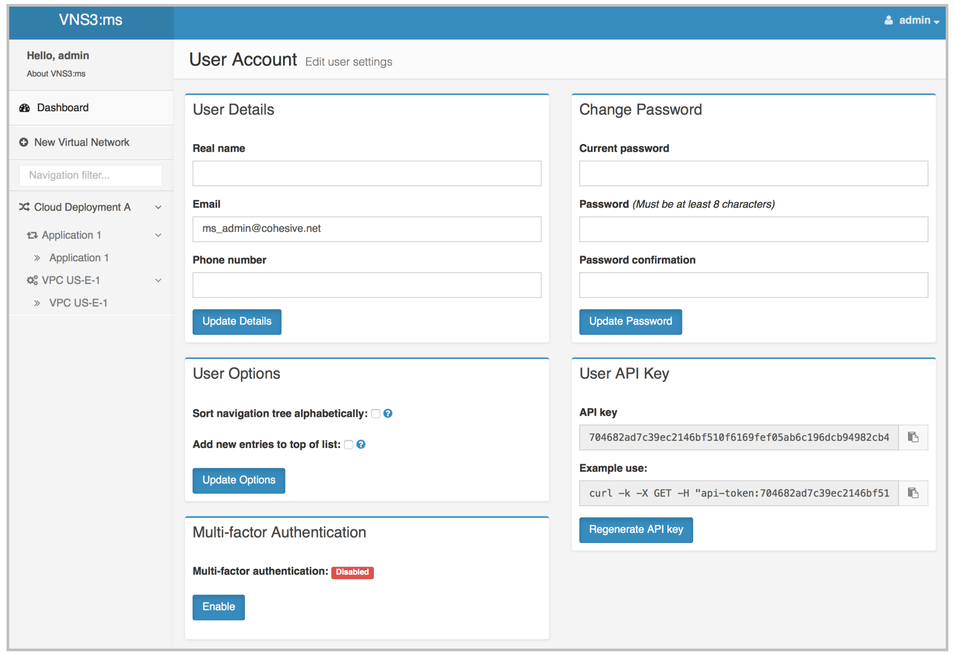
To reset the UI password and API key click the **admin** menu in the top right corner of the VNS3:ms UI.

Select **Change password**.

Change the VNS3:ms UI password and click **Update Password**.

Click **Regenerate Key**.

NOTE: Cohesive Networks does not have any key access or remote access to your VNS3 Controllers unless provided by you. If you forget these passwords we cannot recover them for you.



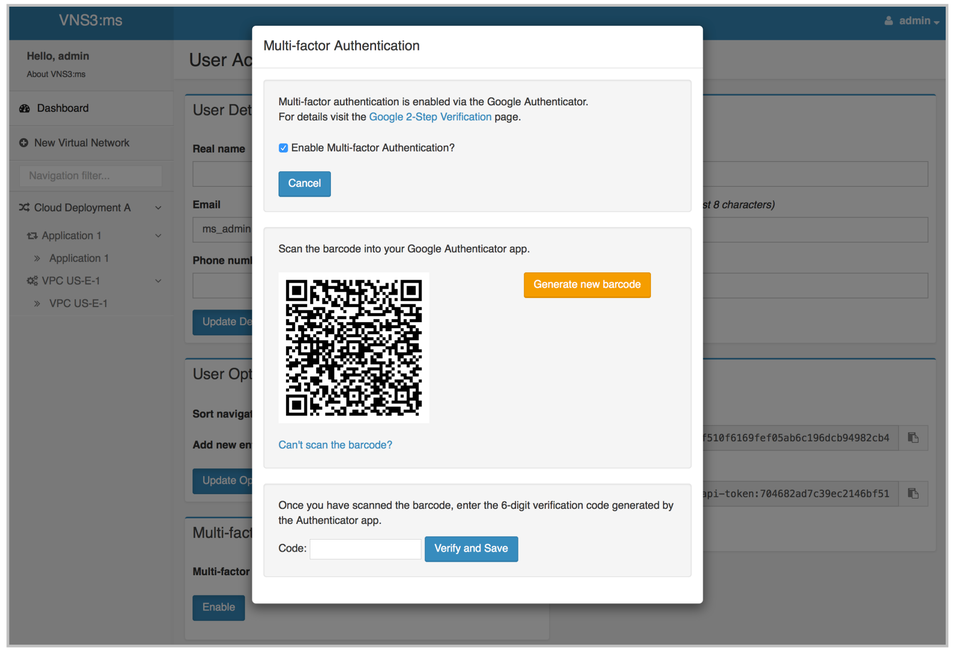
Use Multi-factor Authentication for UI access

To enable Multi-factor Authentication, click **Enable** in the Multi-factor Authentication section.

On the resulting pop-up window click the **Enable Multi-factor Authentication?** check box to display the QR code and verification section.

If the QR code is not correctly read by your authentication app, you can click **Can't scan the barcode?** for the secret key.

Once your authentication app has configured, sync the devices by entering a valid code and click **Verify and Save**.



Setup: How to Monitor VNS3 Controllers

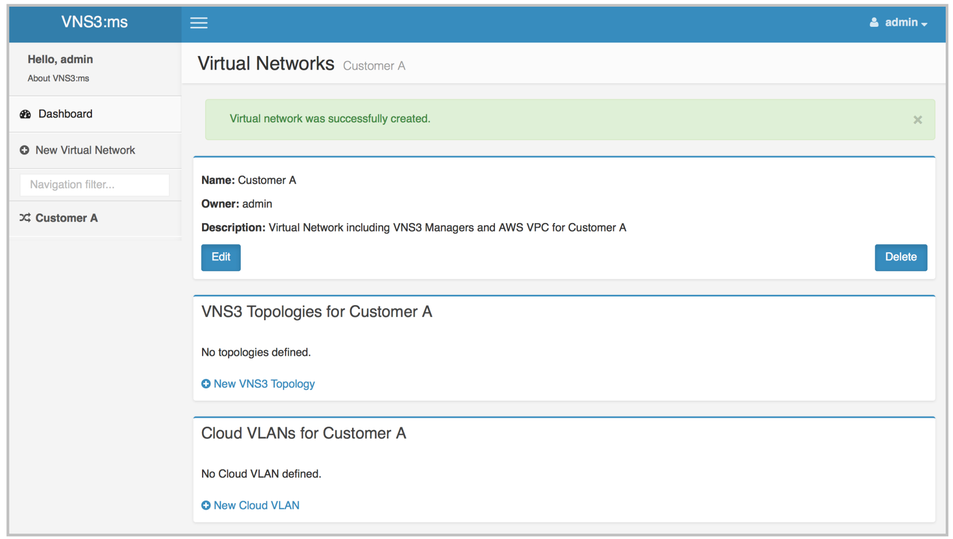
Create a Virtual Network

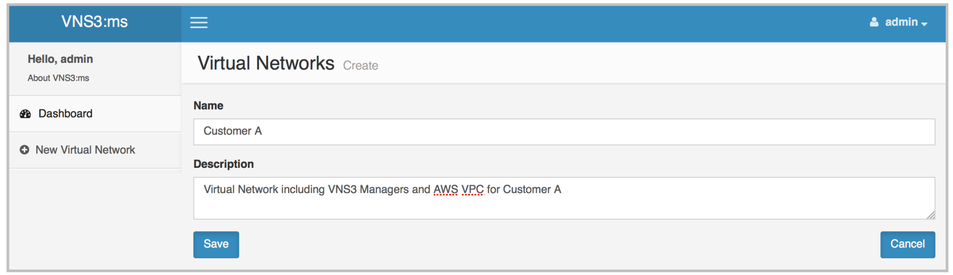
Virtual Networks is the primary taxon or classification unit in the VNS3:ms taxonomy. Virtual Networks are comprised of VNS3 Topologies and Cloud VLANs.

To create a Virtual Network, click on **New Virtual Network** from the left column menu.

On the resulting page give a name and description for your Virtual Network and click Save.

The Virtual Network object will be created and listed in the left column menu.





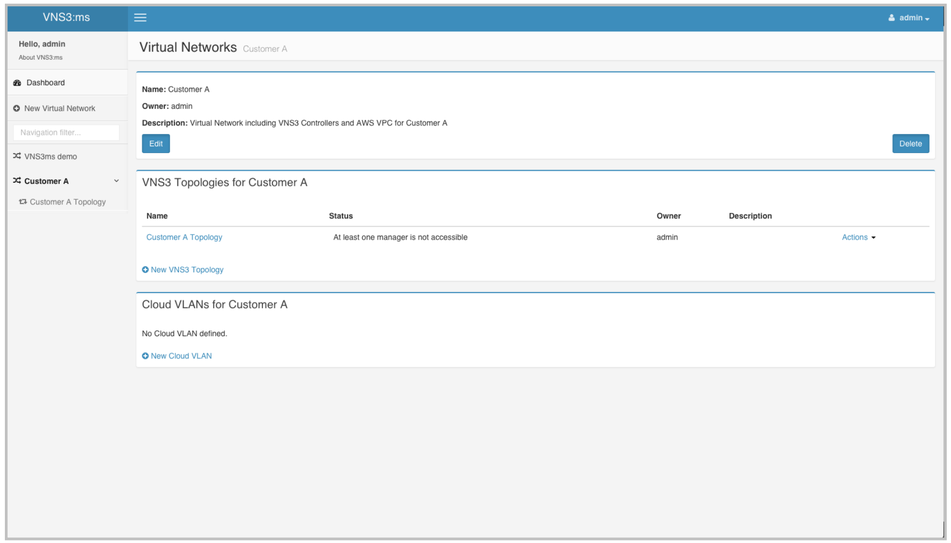
Create a VNS3 Topology

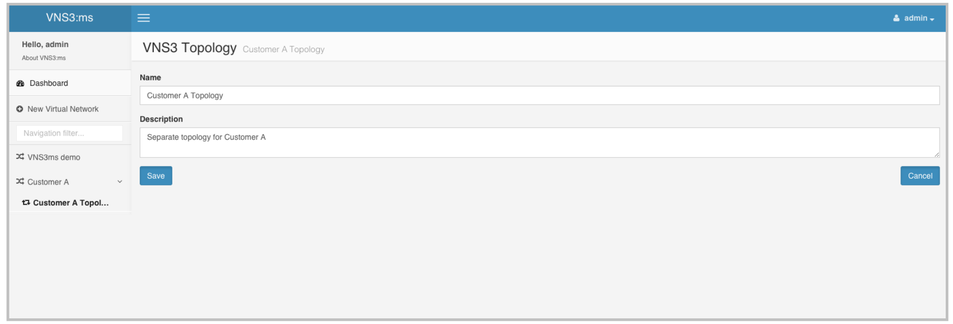
Once the Virtual Network Object is created, add a VNS3 Topology. VNS3 Topologies are made up of one or multiple Peered VNS3 Controller instances.

On the Virtual Network page click on **New VNS3 Topology**.

On the resulting page give a name and description for the VNS3 Topology and click Save.

The VNS3 Topology object will be created and listed in the left column menu.





Add VNS3 Controller(s)

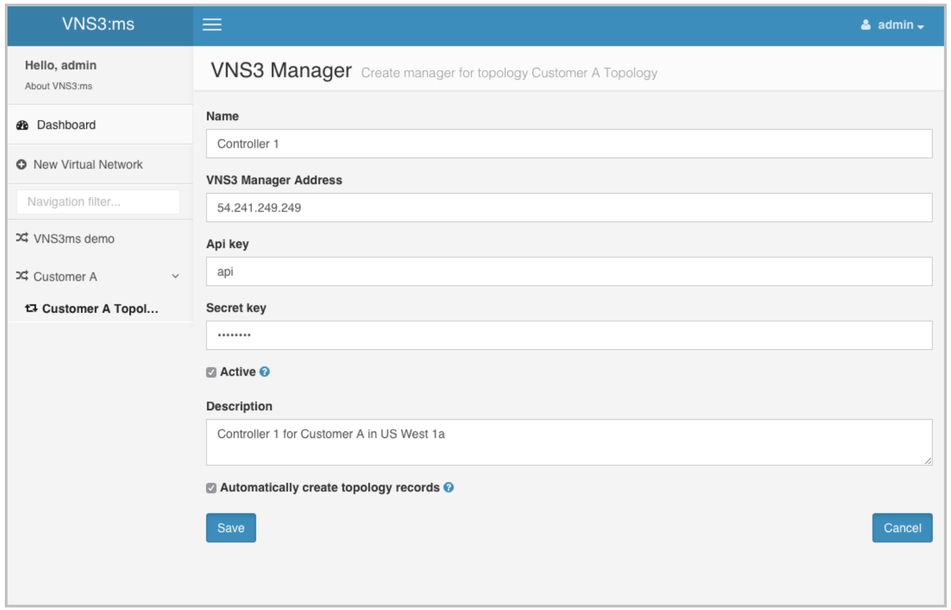
Once the VNS3 Topology object is created, add VNS3 Controllers to the Topology.

On the VNS3 Topology page click on **New VNS3 Controller**.

On the resulting page enter the following information:

- Name
- VNS3 Controller Address - public IP of the VNS3 Controller instance
- API Key - API username on the VNS3 Controller instance (default is *api*)
- Secret Key - API Password
- Active - Active toggle will attempt to connect to the VNS3 Controller instance on a regular basis. Uncheck this if the VNS3 Controller instance is stopped or terminated.
- Description
- Automatically create topology records - for use in VNS3 Peered topologies. VNS3:ms will attempt to add all the Peered Controllers that are connected using the API key and secret key specified. This can speed the configuration and addition of large VNS3 deployments to a VNS3:ms device.

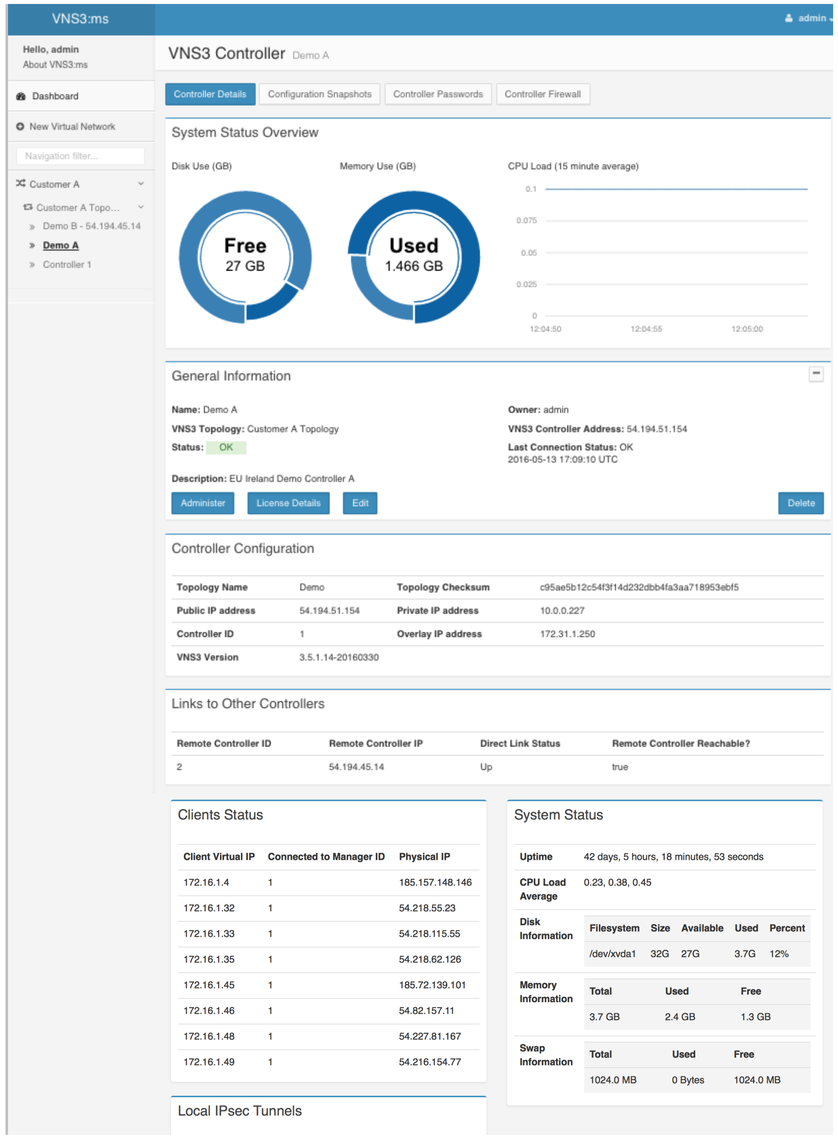
Click **Save**.



VNS3 Controller Instance Status Page

Once a Controller has been added to a VNS3 Topology that is part of a Virtual Network, all the following status information will be available:

- System Status Overview - graphs displaying system status information like disk, memory and CPU utilization.
- General Information - relations to the other network objects (e.g. Virtual Networks and VNS3 Topologies) as well as name and description information.
- Controller Configuration - Information from the VNS3 Controller instance like Topology Name, Controller ID, IP addresses and VNS3 Version.
- Links to Other Controller - Peering information, if any.
- Clients Status - Connected clients table including connected client overlay network IP, connected Controller and physical IP.
- Local IPsec Tunnels
- System Status - more detailed system status information.



Setup: How to Monitor Cloud VLAN

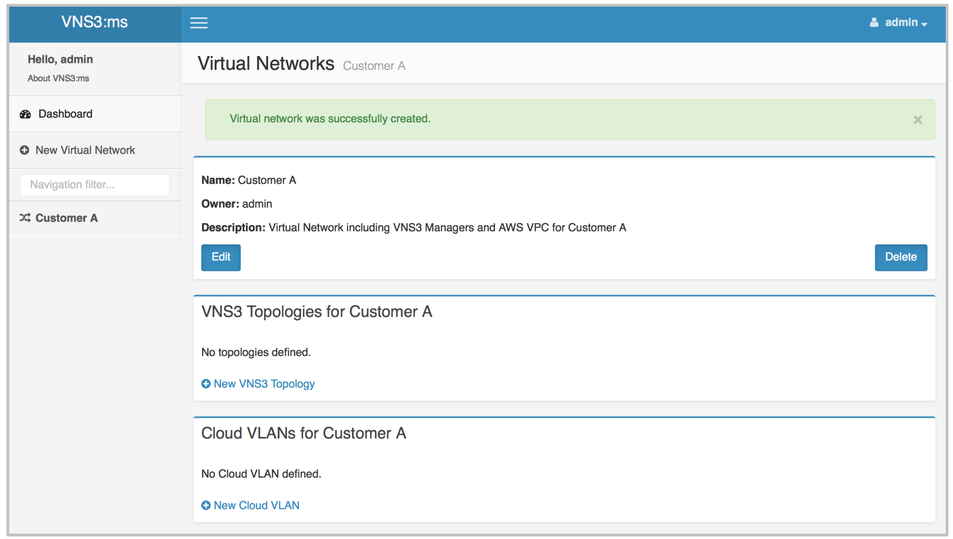
Create a Virtual Network

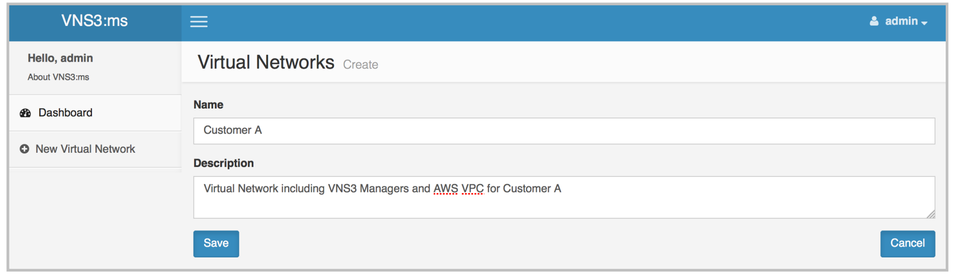
Virtual Networks is the primary taxon or classification unit in the VNS3:ms taxonomy. Virtual Networks are comprised of VNS3 Topologies and Cloud VLANs.

To create a Virtual Network, click on **New Virtual Network** from the left column menu.

On the resulting page give a name and description for your Virtual Network and click Save.

The Virtual Network object will be created and listed in the left column menu.





Add Cloud Credentials

In order to add a Cloud VLAN to to the VNS3:ms monitor and management system, cloud credentials must be added to the VNS3:ms instance in order to collect the relevant VLAN information from the cloud provider.

Recommended best practices are to use an AWS IAM Role attached to the VNS3:ms instance for temporary/dynamic AWS API keys (NOTE: IAM roles do support cross account access).

In situations where the IAM Role aren't an option, long term/static API credentials can be used but it is recommended that a specific IAM programatic access account is created for the VNS3:ms system. This can be done using AWS IAM or similar.

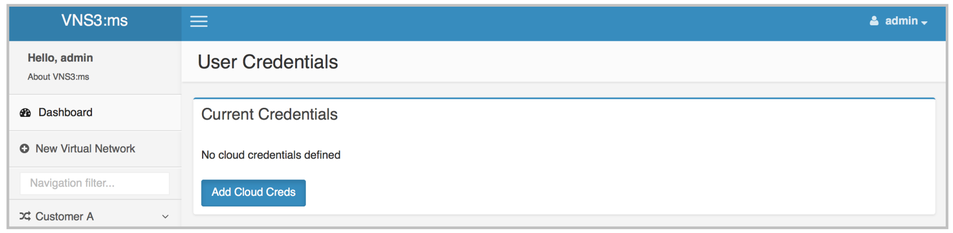
Start with EC2 read-only access. NOTE: If you plan on using VNS3:ha, you will need to provide some edit/full access capabilities to the VNS3:ms instance. See the VNS3:ha section for information.

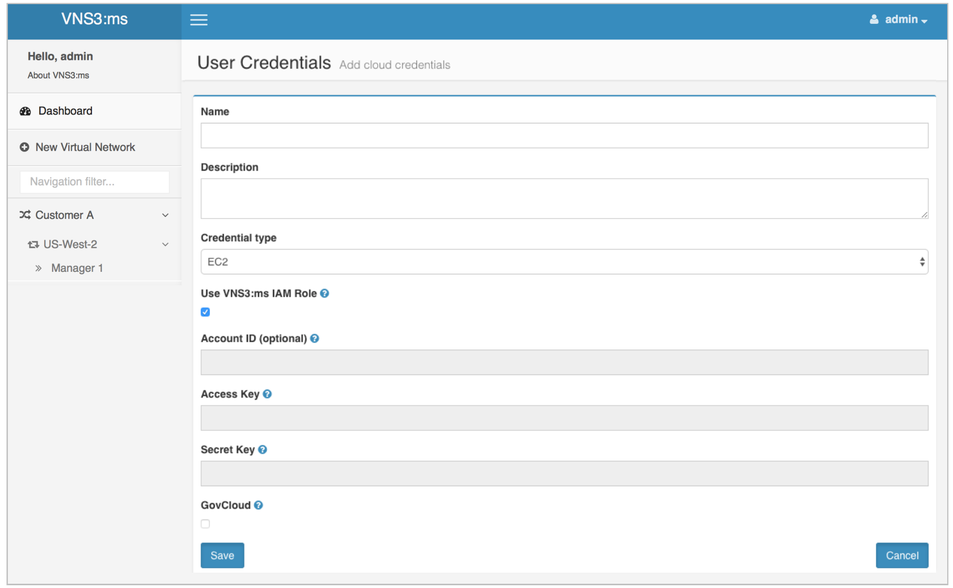
To add cloud credentials click on the **admin** top right corner drop down menu, then click on **Cloud Credentials**.

Click **Add Cloud Creds** then enter the following information:

- Name
- Description
- Credentials type - cloud provider that the credentials are associated. Initially AWS is supported with more clouds coming soon.
- Use VNS3:ms IAM Role - check this box if using IAM Role for API access as recommended above.
- Account ID
- Access Key
- Secret Key
- GovCloud - is this a Gov Cloud account or generic AWS

Click **Save**.





Add Cloud Credentials: IAMs Policy

In order to add a Cloud VLAN to to the VNS3:ms monitor and management system, cloud credentials must be added to the VNS3:ms instance in order to collect the relevant VLAN information from the cloud provider.

Recommended best practices are to use an AWS IAM Role attached to the VNS3:ms instance for temporary/dynamic AWS API keys (NOTE: IAM roles do support cross account access).

In situations where the IAM Role aren't an option, long term/static API credentials can be used but it is recommended that a specific IAM programatic access account is created for the VNS3:ms system. This can be done using AWS IAM or similar.

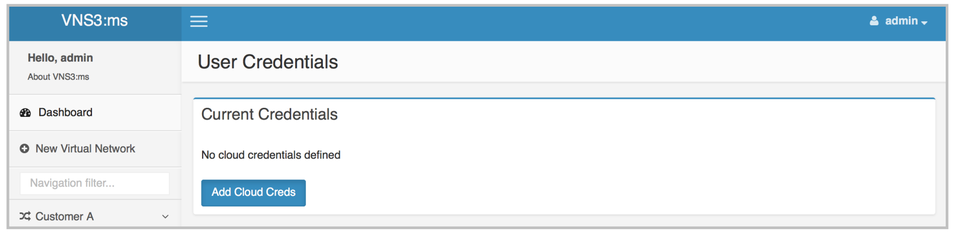
Start with EC2 read-only access. NOTE: If you plan on using VNS3:ha, you will need to provide some edit/full access capabilities to the VNS3:ms instance. See the VNS3:ha section for information.

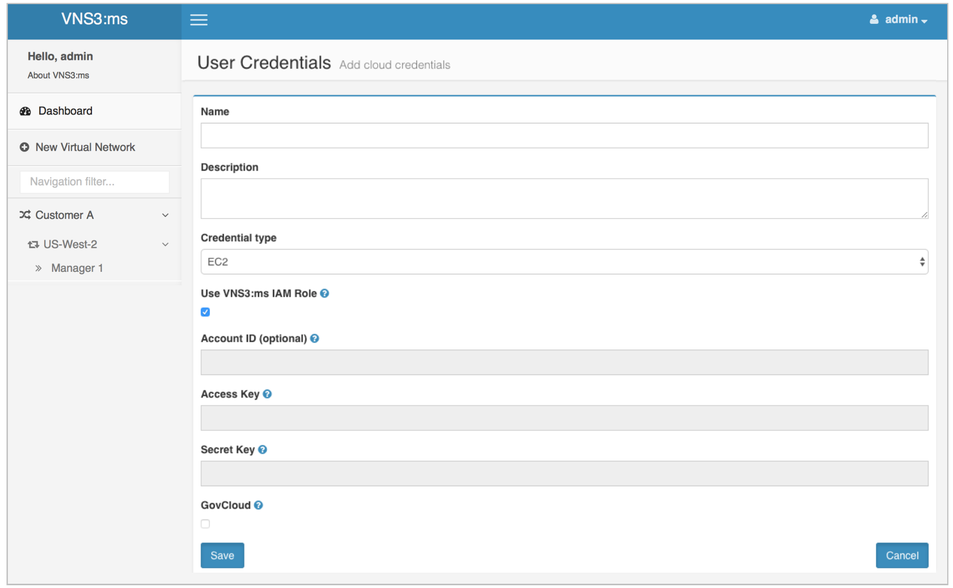
To add cloud credentials click on the **admin** top right corner drop down menu, then click on **Cloud Credentials**.

Click **Add Cloud Creds** then enter the following information:

- Name
- Description
- Credentials type - cloud provider that the credentials are associated. Initially AWS is supported with more clouds coming soon.
- Use VNS3:ms IAM Role - check this box if using IAM Role for API access as recommended above.
- Account ID
- Access Key
- Secret Key
- GovCloud - is this a Gov Cloud account or generic AWS

Click **Save**.

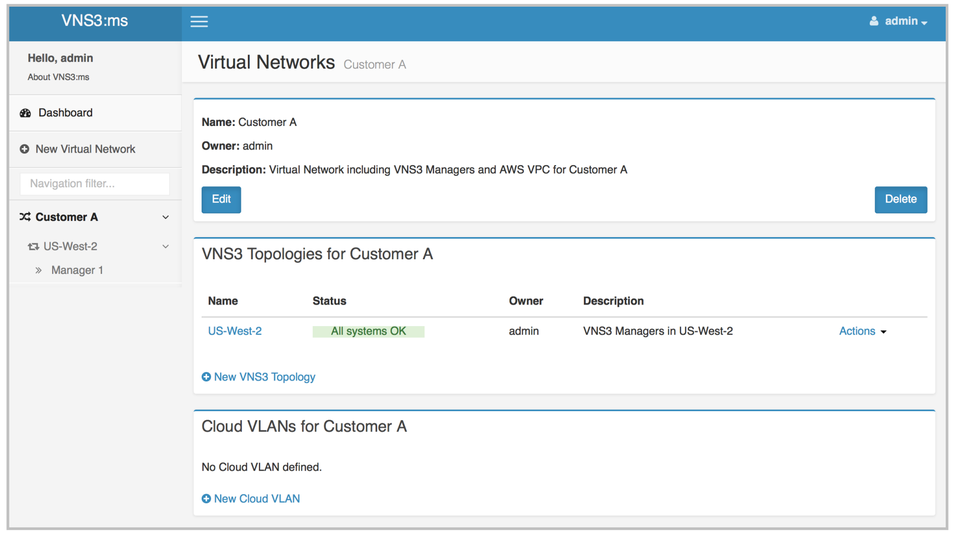


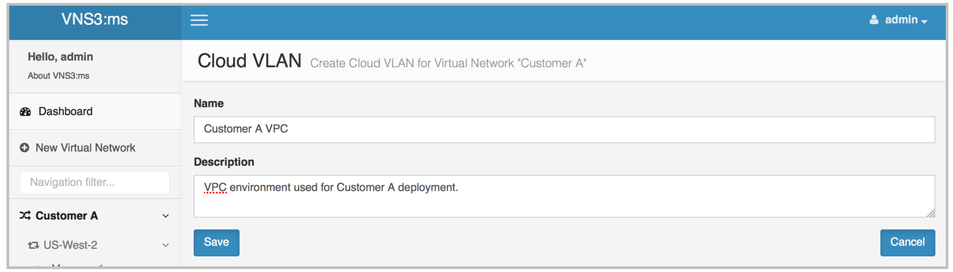


Create a Cloud VLAN

Return to the Virtual Network Page and click **New Cloud VLAN**.

Enter a Name and Description of the Cloud VLAN and click **Save**.





Specify a Cloud VLAN Component to Monitor

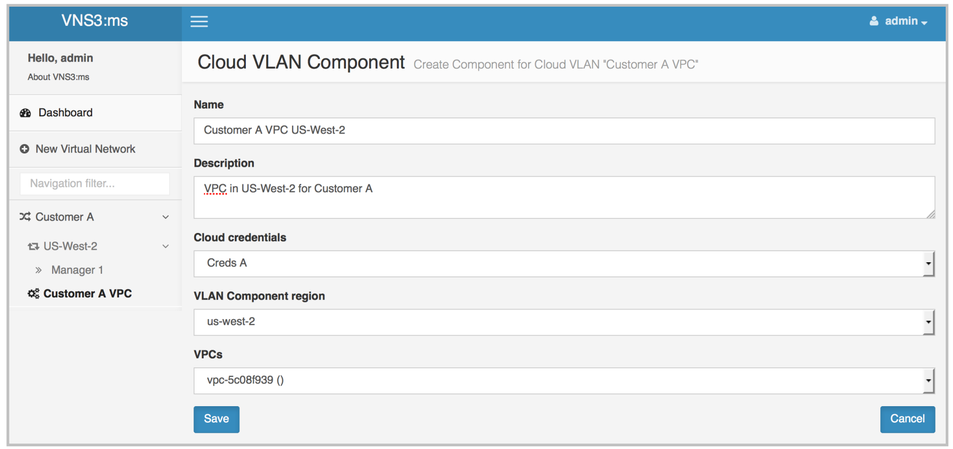
From the resulting Cloud VLAN page, click **Add New VLAN Component**.

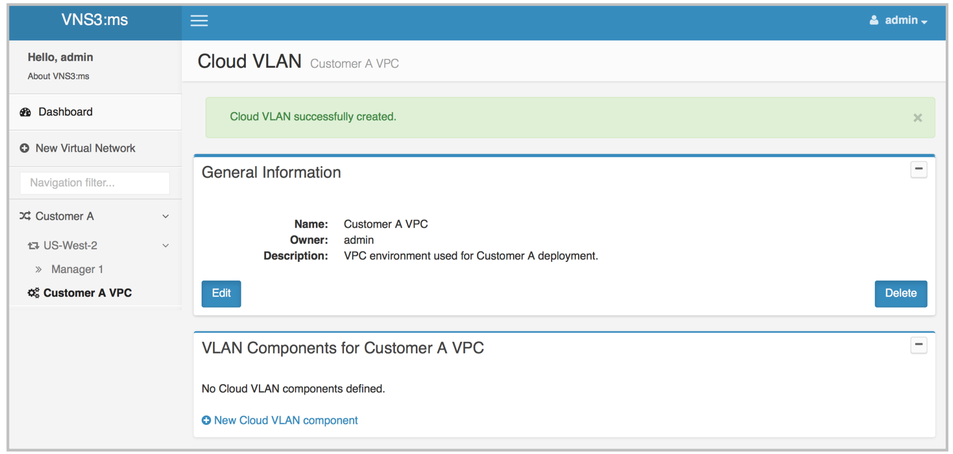
Enter a Name and Description of the Cloud VLAN and click **Save**.

Enter the following information for the Cloud VLAN Component to be monitored:

- Name
- Description
- Cloud Credentials - specify the credentials that were just added
- VLAN Component Region - region where the VLAN component is setup
- VPCs - select from a list of VPCs in the region specified

Click **Save**.



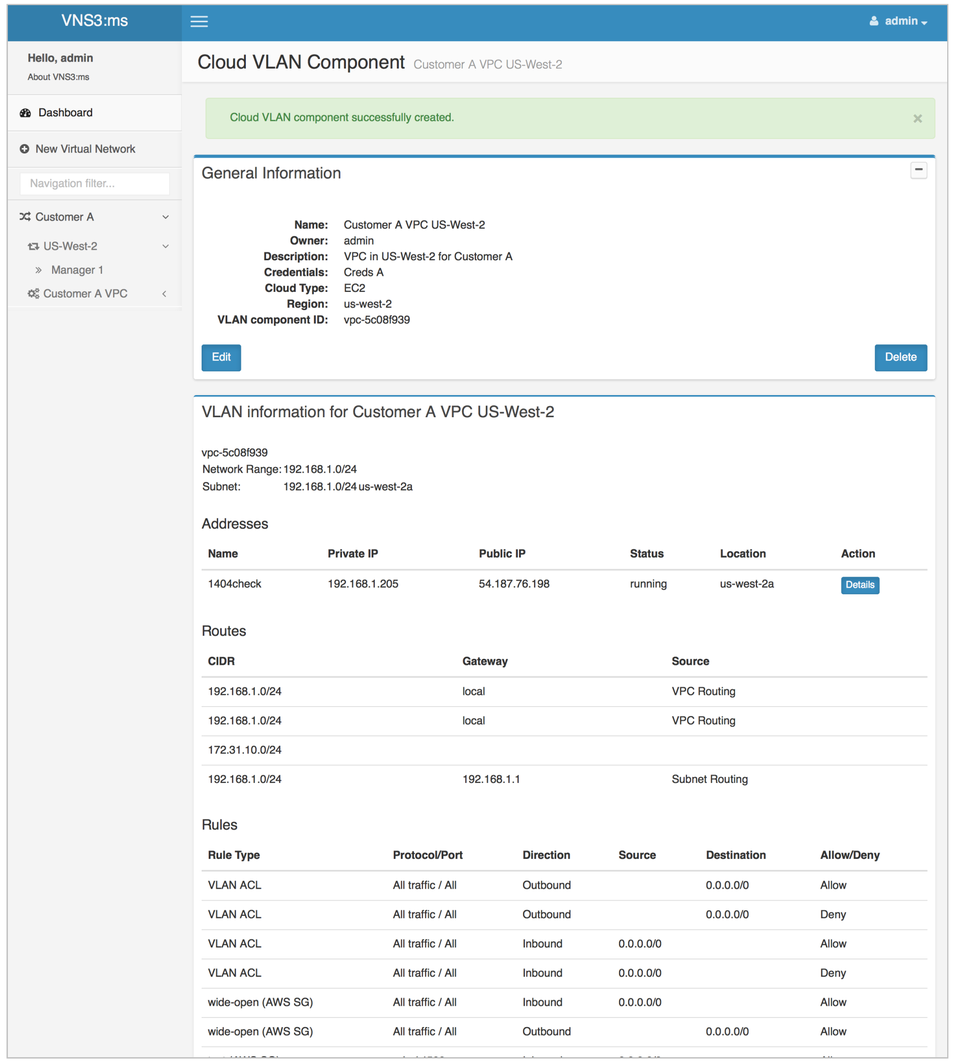


Cloud VLAN Component Status Page

Information on the Cloud VLAN Component Status page is broken down into component identification information surfaced by the cloud provider (e.g. vpc-id, subnet ids, etc.).

VNS3:ms then stitches together all the information into a single easy to consume page. The relevant information VNS3:ms provides is:

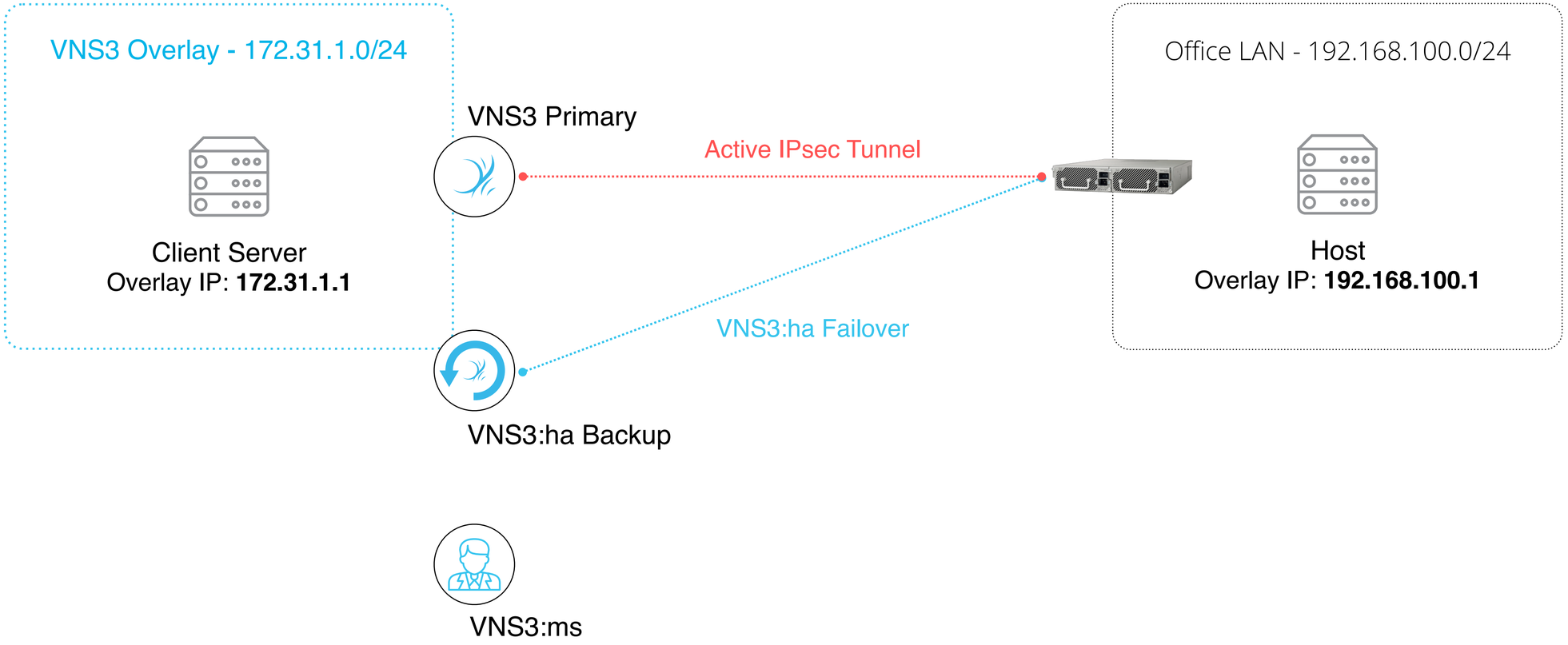
- Addresses - the instances currently running in the VLAN
- Routes - the routes setup in the VLAN that are being used by the VLAN instances
- Rules - ACL and Security Group rules for the VLAN and the instance running in the VLAN



Setup: VNS3:ha

VNS3:ha - Instance-based failover

An instance-based automatic IPsec VPN failover solution to reduce RTO in the event of cloud connectivity failure. If/when the VNS3 Primary or tunnel to VNS3 Primary fails, VNS3:ms can trigger an automated failover to the VNS3:ha Backup.



VNS3:ha - Requirements

- Currently restricted to AWS VPC resident controllers.
- Existing VNS3 controller with one or many IPsec tunnels negotiated, connected, and healthy.
- Use of an Elastic IP for the public IP of the VNS3 controller.
- VNS3:ha backup instance running **VNS3 v3.5.1.14--20160315** or later in the same VPC as the VNS3 primary controller.
- VNS3:ha backup instance needs to have the same API password as the primary VNS3 instance it will be associated with.
- Use of Overlay or Underlay networks for cloud-based instances.
- Ability to create and add cloud API credentials to allow your VNS3:ms instance to access your cloud account and run the required actions (ec2:Describe* + ec2:AssociateAddress, ec2:DisassociateAddress, ec2:ModifyInstanceAttribute, ec2:ReplaceRoute, and ec2:StopInstances).

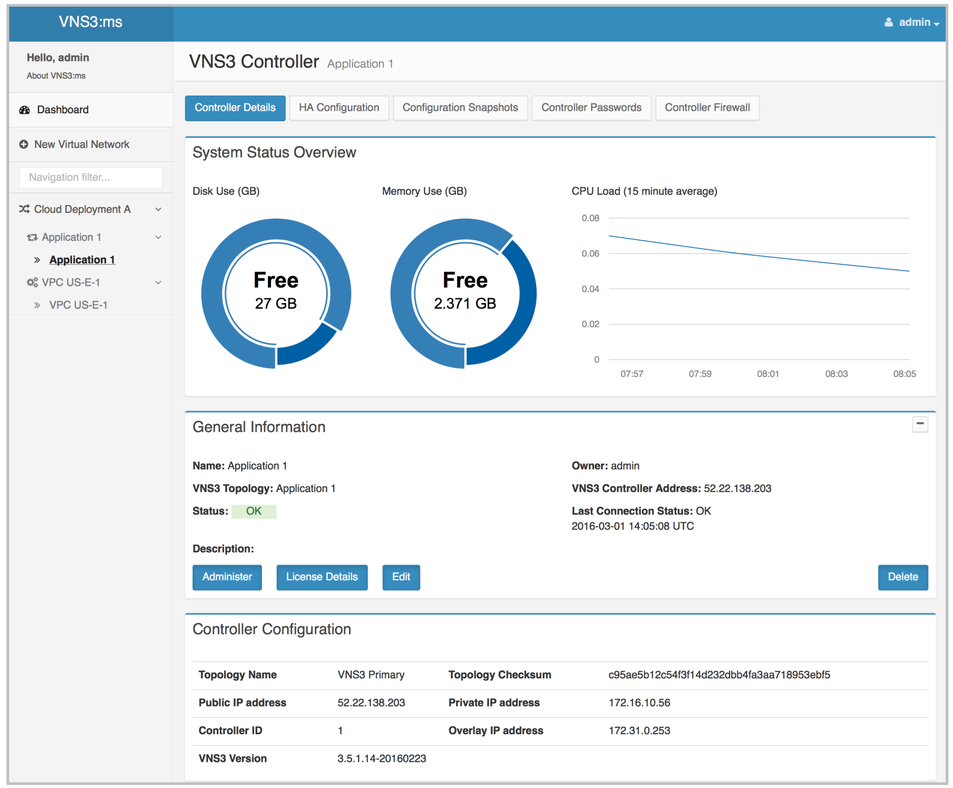
HA failover IAMs policy example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:ModifyInstanceAttribute",
                "ec2:ReplaceRoute",
                "ec2:StopInstances"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Enabling VNS3:ha controls

VNS3:ms instances are not enabled for HA controls by default. In order to have the HA Configuration tab available, a member of Cohesive Networks support staff needs to access the VNS3:ms instance to enable.

Contact sales@cohesive.net to enable VNS3:ha controls.



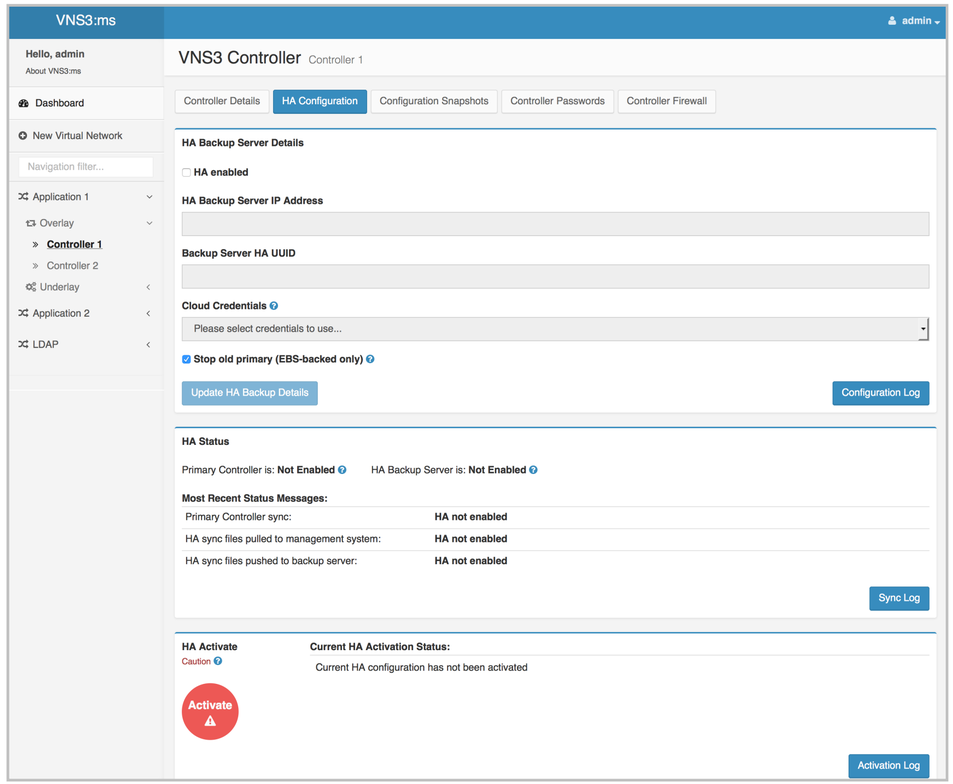
Add a VNS3:ha backup to an existing VNS3 controller

VNS3:ha backup instances are associated with a running and healthy VNS3 controller. In the event the VNS3 primary controller fails (instance, hardware, or connection failure), VNS3:ms can run an automated failover process where the VNS3:ha backup takes the place of failed VNS3 primary controller.

In order to setup a VNS3:ha backup you need to enter the following specific information on the HA Configuration tab

- VNS3:ha backup Public IP
- VNS3:ha backup UUID - see following page
- Cloud Credentials - cloud creds where the VNS3 primary and VNS3:ha backup instances are running.

NOTE: If you are using the Underlay Network, remember to Disable Src/Dst checks on the backup instance.

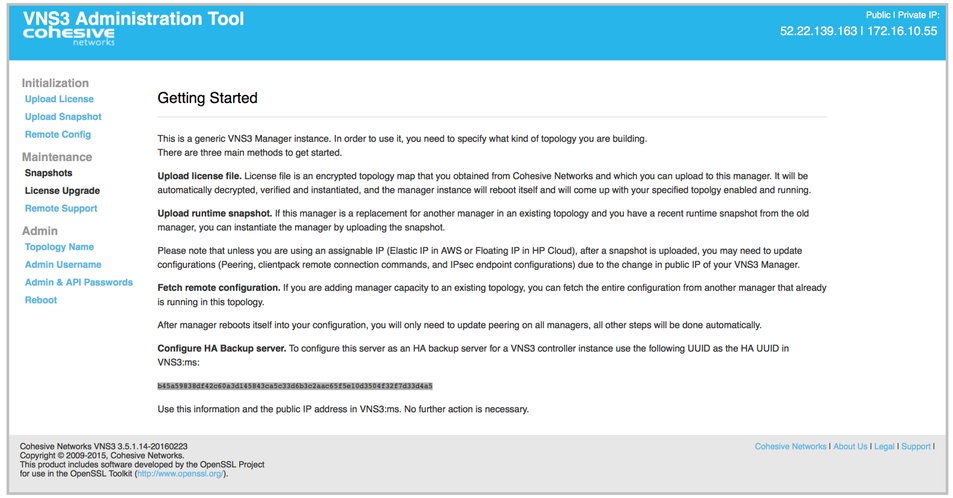


VNS3:back controller UUID

Per the VNS3:ha requirements, a VNS3 version 3.5.1.14 or later instance that will be used at the VNS3:ha backup is running in the same VPC and subnet as the VNS3 primary controller.

Do not apply a license to the instance you plan to configure as the VNS3:ha.

VNS3:ms handle the initialization. Simply log in and copy the VNS3:ha UUID listed on the status page.



Enter VNS3:ha information

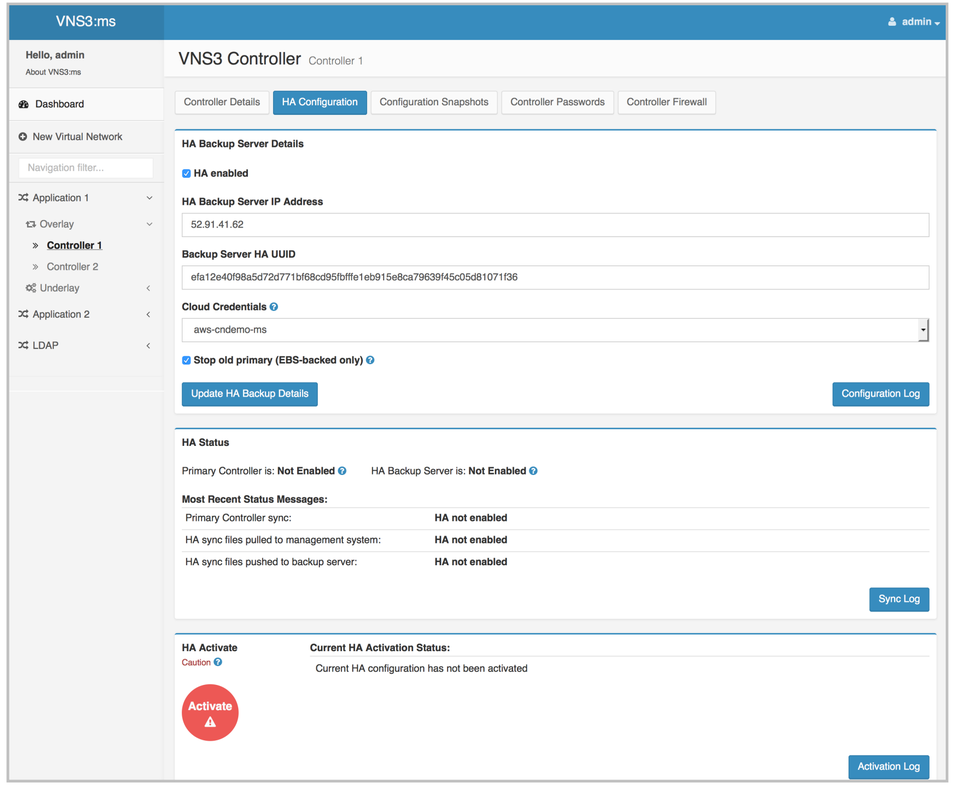
Once the VNS3:ha backup instance information is entered click **Update HA Backup Details**.

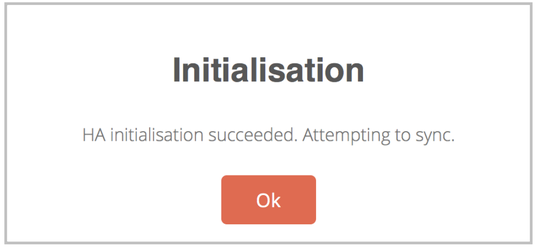
Then click **OK** in the resulting Initialization popup window.

The HA Status section will show the following:

- Status of the Primary and HA controllers.
- The last status messages for the automatic configuration sync between the primary, VNS3:ms and the backup HA controller. Messages are shown with a timestamp.

Log messages can be viewed from the three log file buttons on the page: Configuration log, Sync Log, and Activation log.

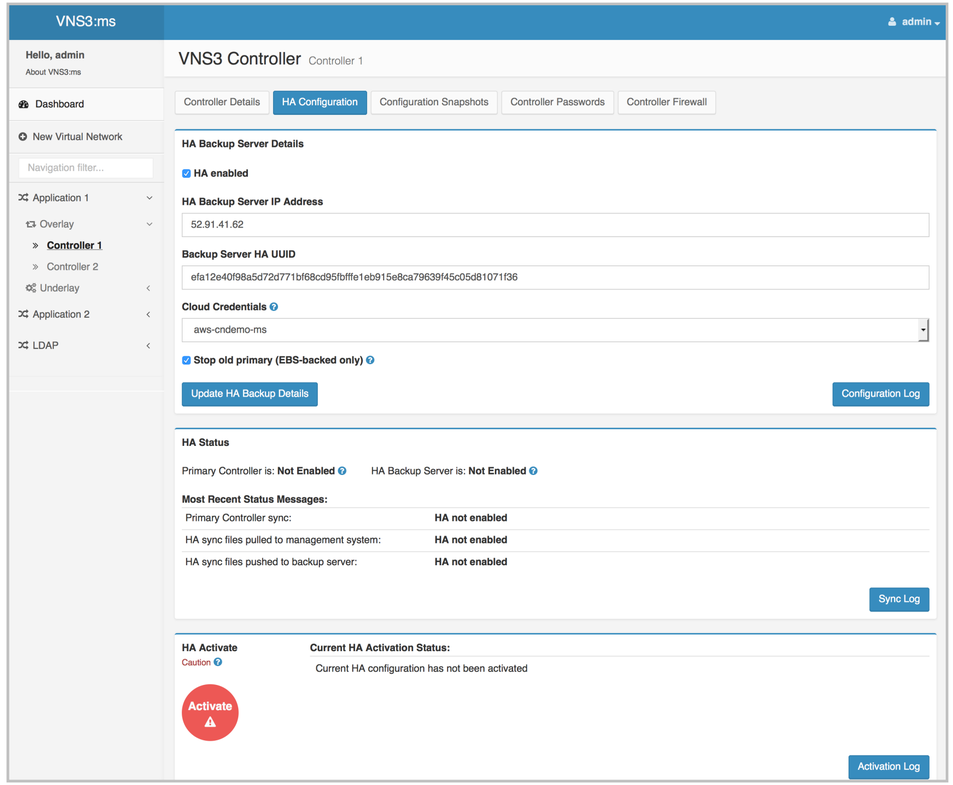




VNS3:ha stop primary

Depending on the version of the Primary VNS3 controller instance, there may or may not be a Stop old primary checkbox available.

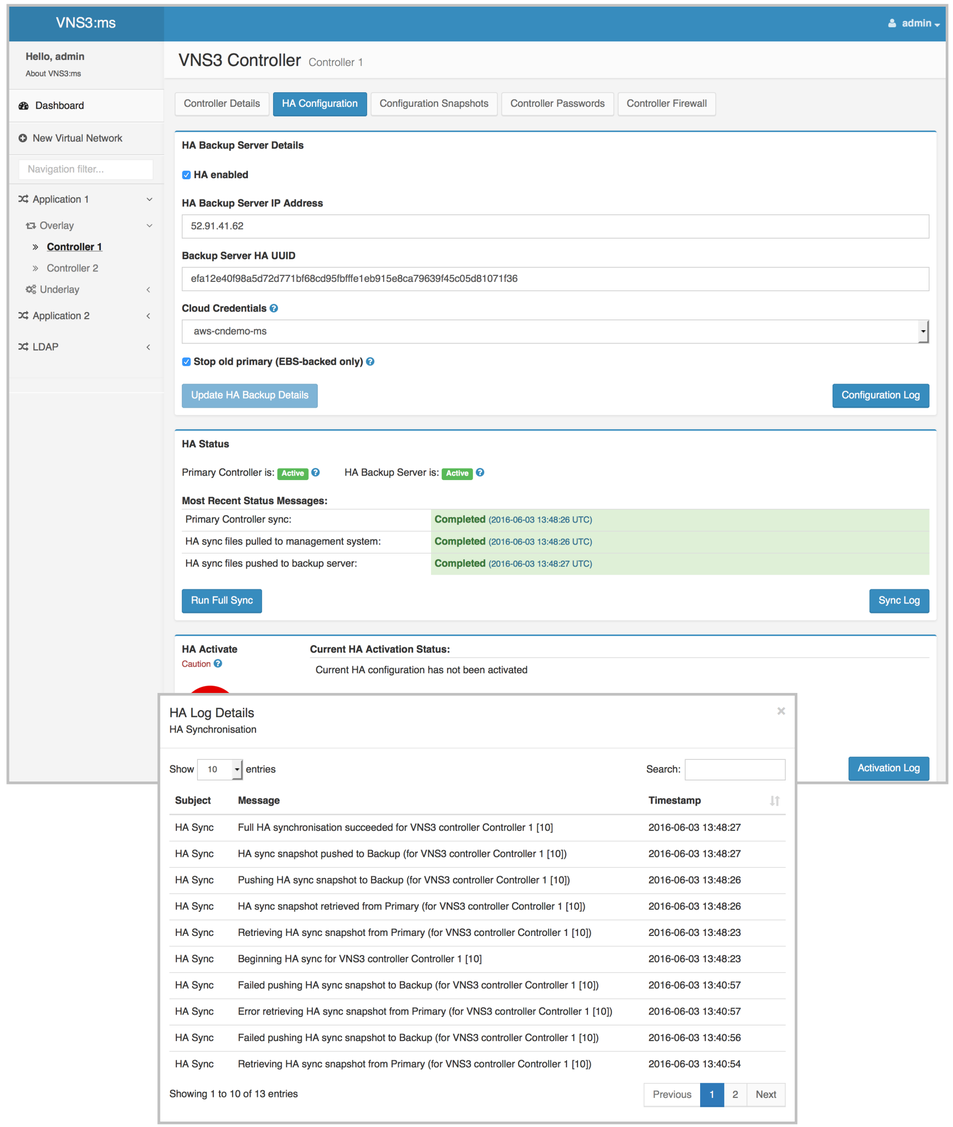
Starting with VNS3 version 3.5.1.14 and later, this option will be available. Stopping the old primary instance after a successful failover ensures all old connections to that device are moved over to the failed over VNS3:ha instance.



VNS3:ha configured state

Once a new VNS3:ha backup instance has been initialized and synced with the latest configuration of the Primary, you will see completed status messages.

VNS3:ms will then continue to update the VNS3:ha controller every 30 minutes with the primary VNS3 configuration. This ensure the recovery point objective for a VNS3:ha failover is always a configuration state of at most 30 minutes old.

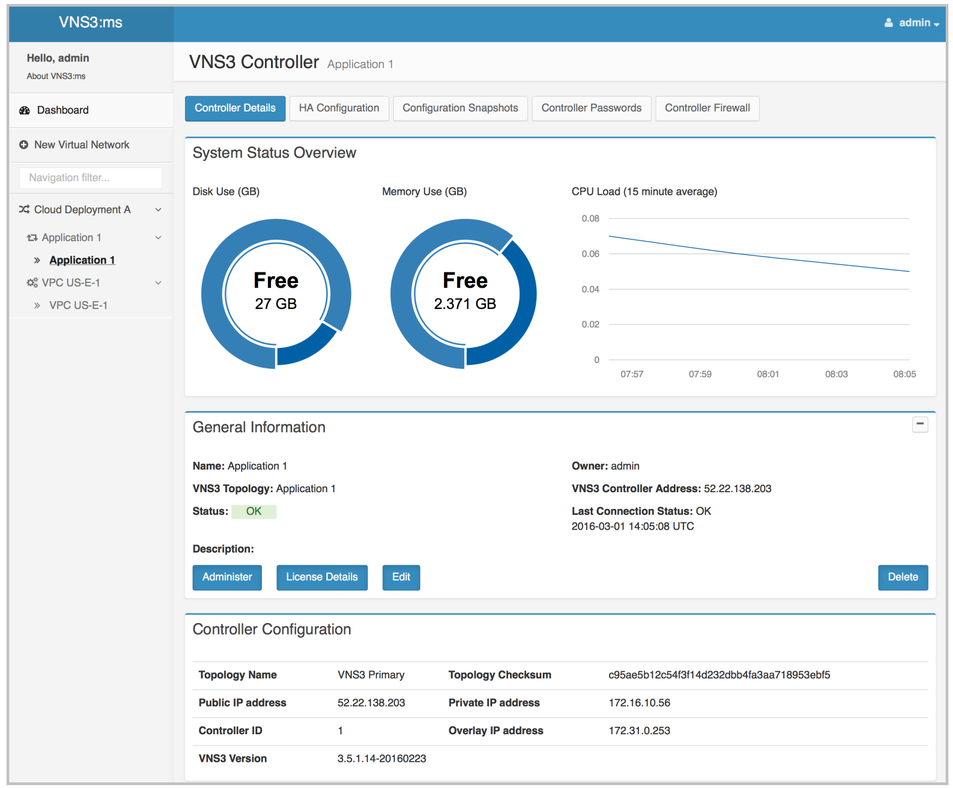


Manage: VNS3 Controller UI

Access VNS3 Instance UI via VNS3:ms

On Each VNS3 Controller Details page under General Information there is an Administer button.

Click Administer to goto the VNS3 Controller instance UI.



Manage: VNS3 Automatic Snapshots

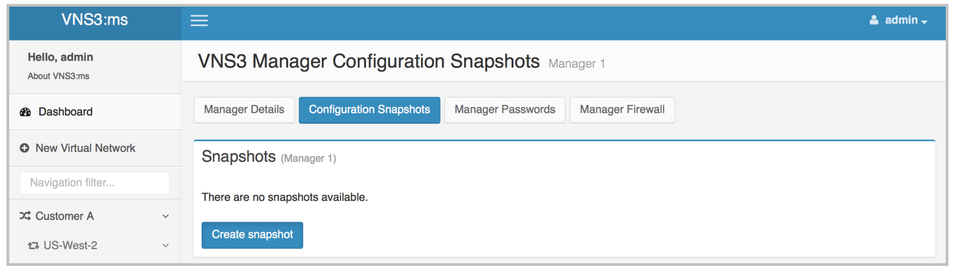
Automatic VNS3 Snapshot Creation and Storage

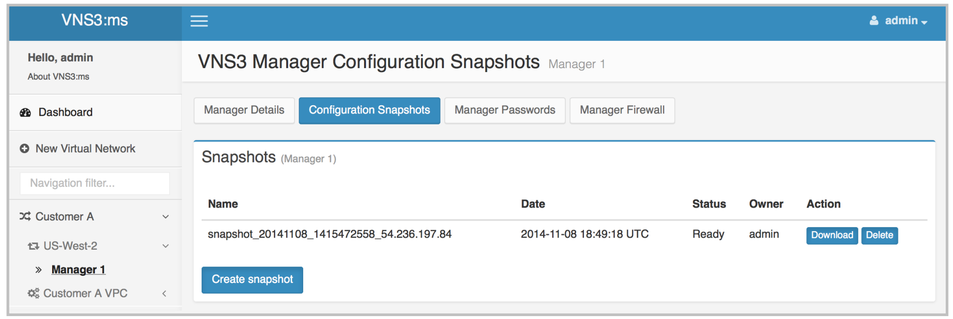
VNS3:ms automatic VNS3 Snapshot feature provides a mechanism to programmatically create, download and store snapshots of deployed VNS3 Controllers. Currently VNS3 captures snapshots once daily and stores the previous 10 days in the local snapshot repository. In the future users will be able to specify the periodicity of the snapshots and the length of history that is stored.

To kick off the process click on **Configuration Snapshots** sub menu on either the VNS3 Topology or VNS3 Controller pages.

On the resulting page click **Create snapshot**. This action takes the first snapshot and sets up the daily process.

Once a VNS3 Snapshot has been created, it is displayed on the Snapshot page and can be downloaded or deleted.



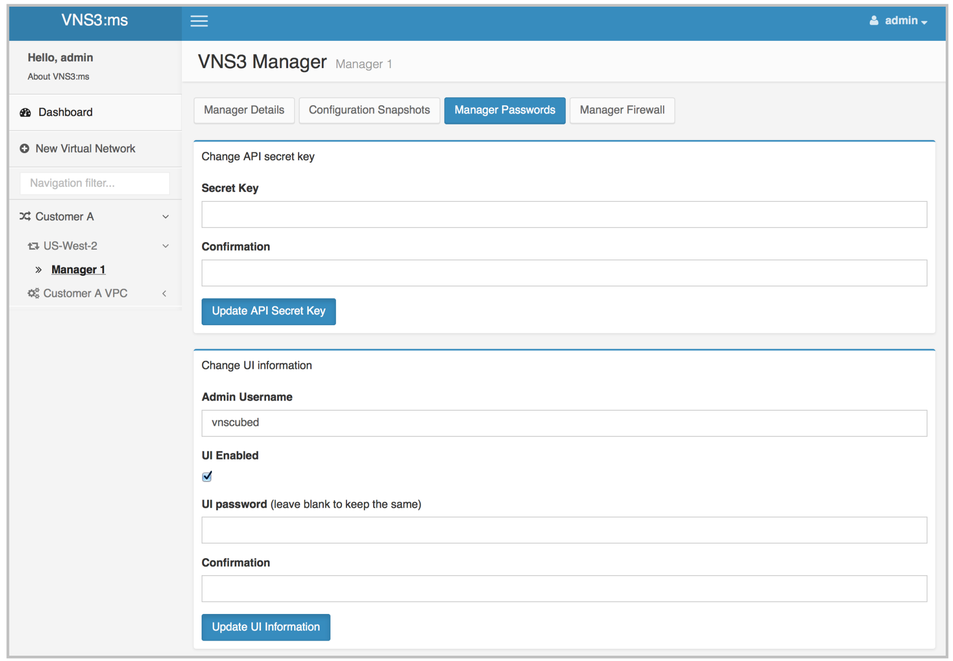


Manage: VNS3 Controller Passwords

VNS3 Controller Password Update and Recovery

VNS3:ms provides the ability to update both UI username/ password and API password to VNS3 Controller instances that have been added to the system.

Click **Controller Passwords** from a VNS3 Controller Details page.

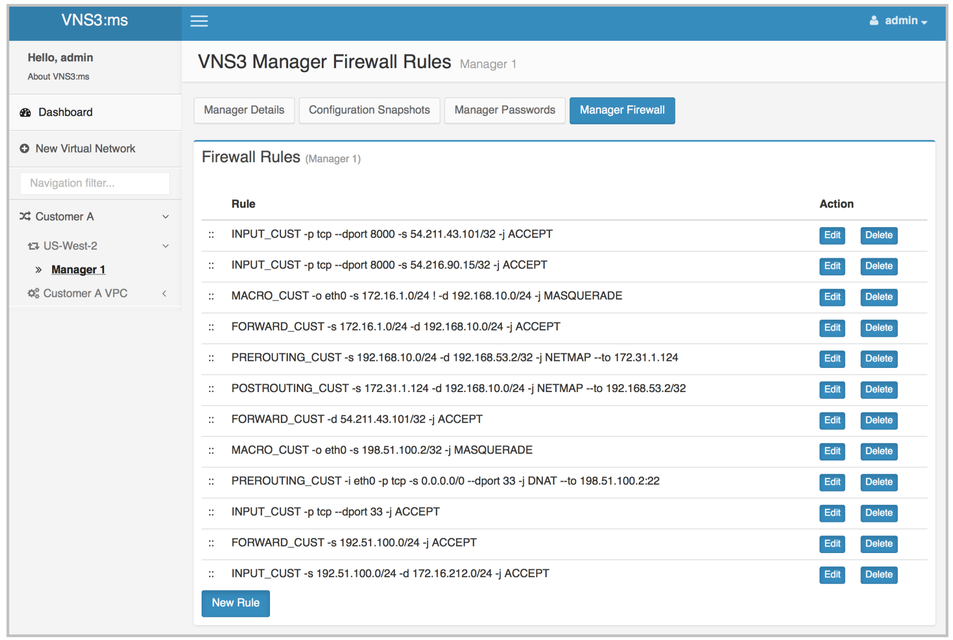


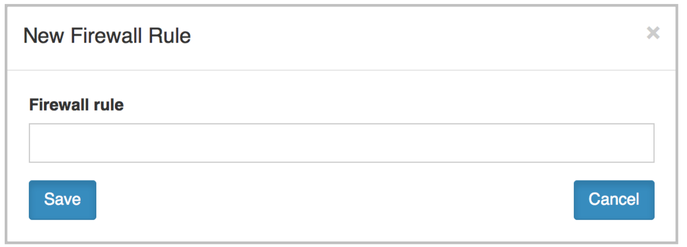
Manage: VNS3 Controller Firewall

Manage VNS3 Controller Instance Firewall

VNS3:ms provides the ability to view, edit and create VNS3 Controller Instance Firewall rules directly from the VNS3:ms console.

Click **Controller Firewall** from a VNS3 Controller Details page.





Manage: VNS3:ha failover event

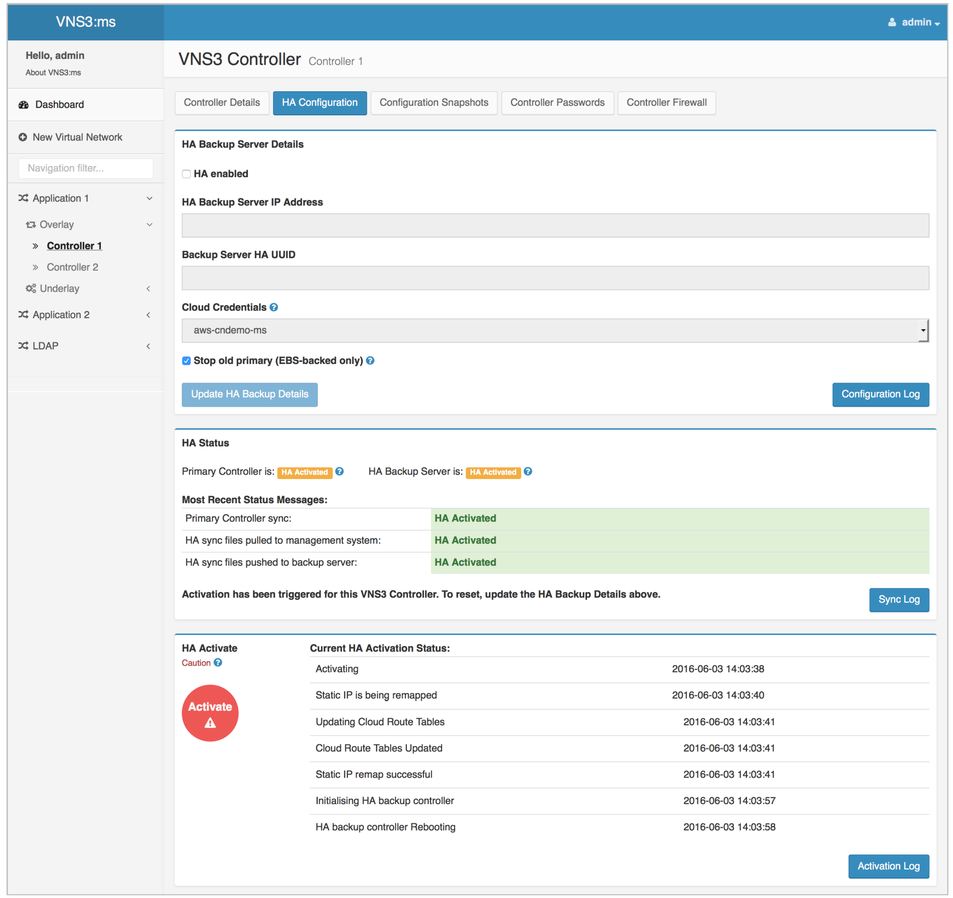
VNS3:ha trigger failover activation

A VNS3:ha failover event can be triggered at anytime once a VNS3:ha backup configuration has been added and all HA Status messages are "green" and completed.

When a trigger event happens, the VNS3:ms system does the following and provide status updates with timestamps in the HA Activate pane:

- Activating
- Primary static IP being remapped
- Updating cloud route tables
- Cloud route tables updated
- Static IP remap successful
- Initializing HA backup controller
- HA backup controller rebooting
- HA backup controller is now the Primary controller
- Stopping old Primary instance (if stop primary was configured)
- Stop request queued (if stop primary was configured)
- HA activation process is complete

To trigger a VNS3:ha failover event either click the **Activate** "big read button" or utilize the API.



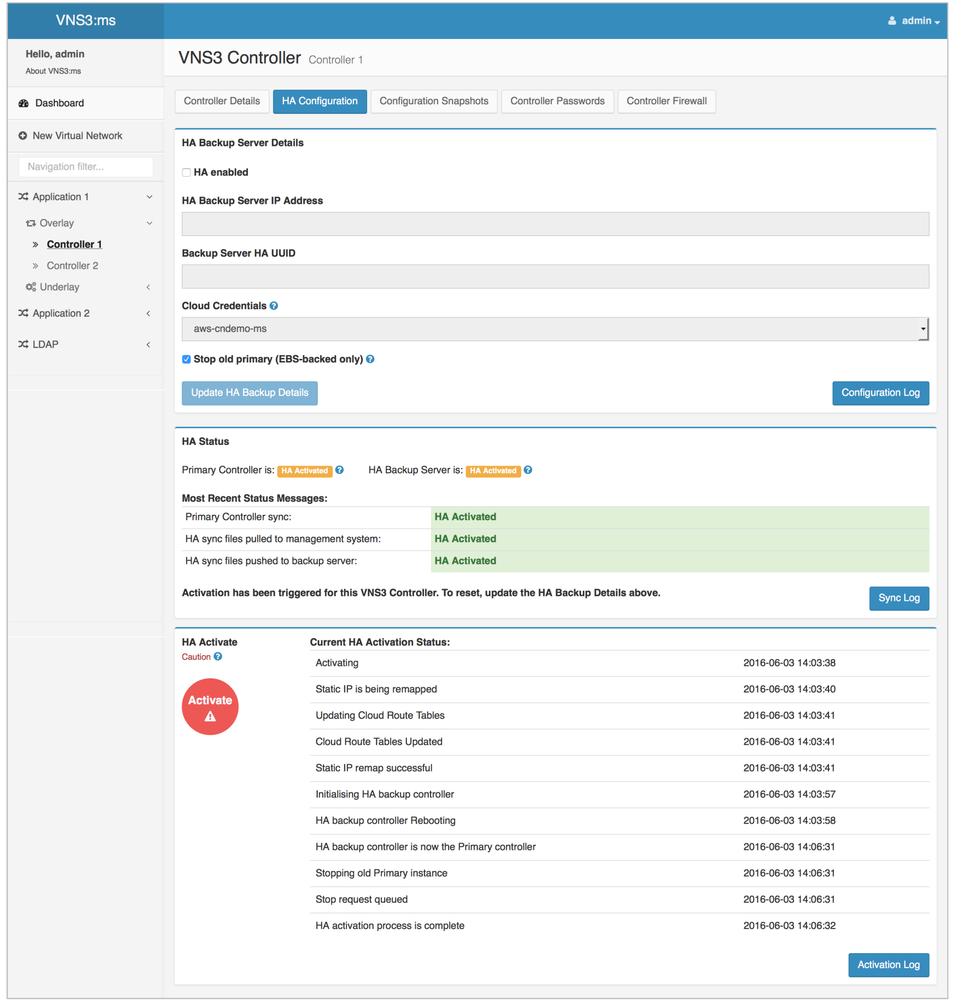
VNS3:ha failover activation complete

Once a failover activation event has completed and the HA backup controller is now acting as the primary.

The HA Configuration page will show that HA is no longer enabled for the now acting primary controller and will show the log messages from the last activation event.

A new HA configuration can be added to account for future failover events.

Log messages are saved in the three log files so users can review the HA events for a particular VNS3 controller network object.

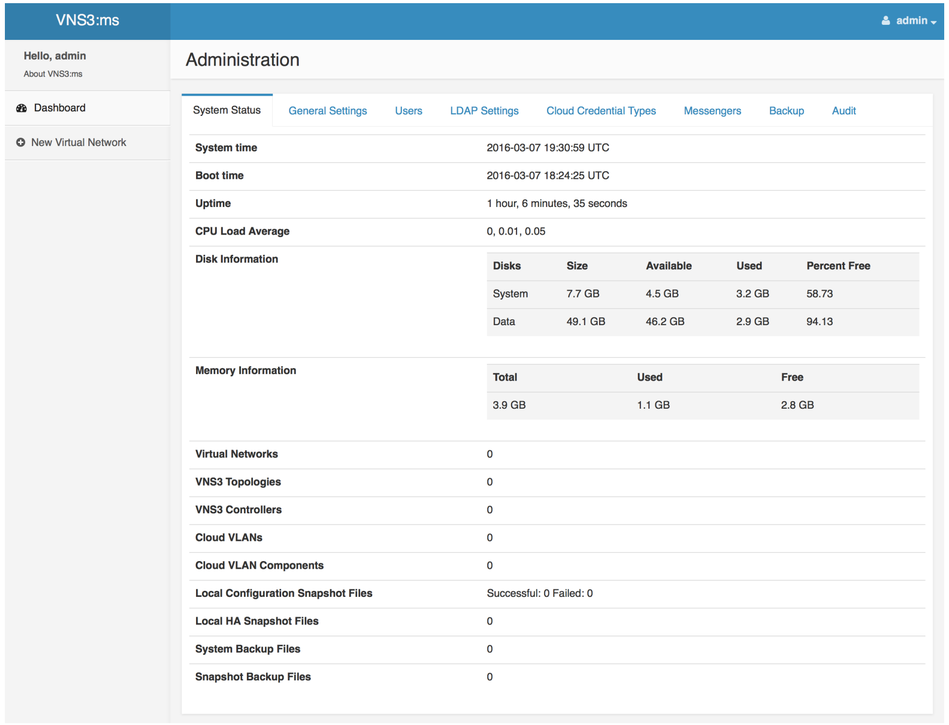


Administration

Administration: System Status

VNS3:ms Administration section is available by clicking on the **admin** top right corner drop down menu, then click on **System Administration**.

Click **Systems Status** to view instance specific status information for the particular VNS3:ms device. In addition to instance utilization information there are counts for the number of virtual networks, topologies, controllers, etc. that are being monitored.

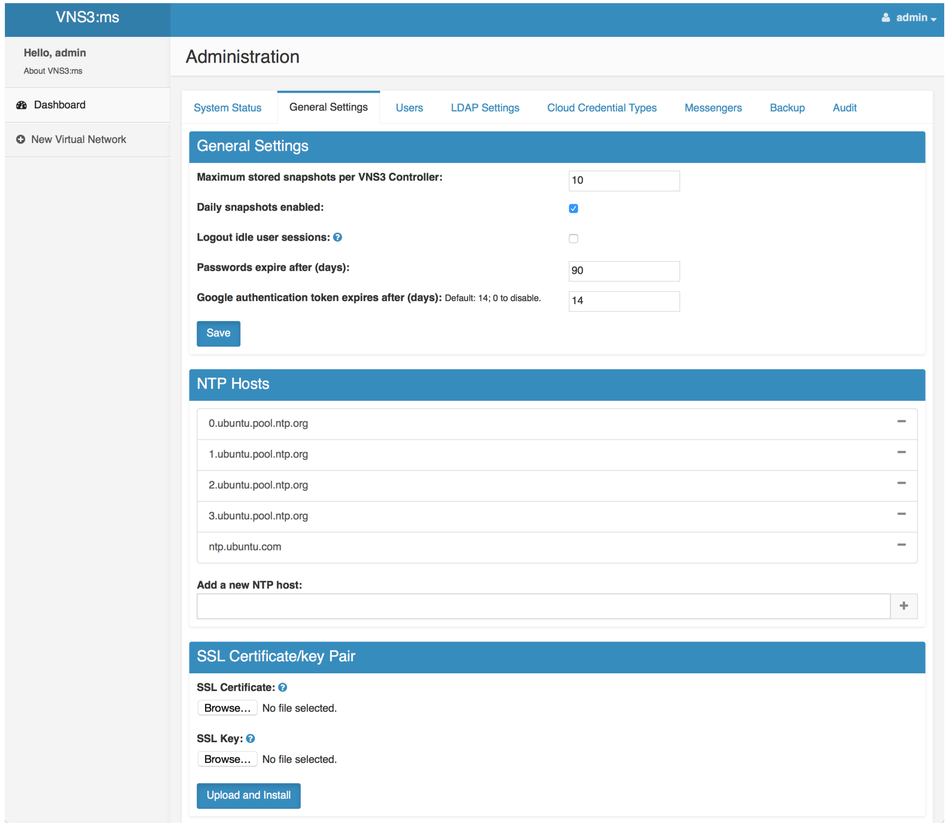


Administration: General Settings

Click **General Settings** to set the Maximum number of VNS3 Snapshots to be stored per Controller instance, password lifetime, 2fa token lifetime, NTP hosts and HTTPS SSL certificate.

NTP default servers are included but can be changed depending the type of network access allowed to the VNS3:ms instance.

VNS3:ms uses a self-signed certificate for HTTPS authentication by default. While Cohesive Networks might argue this is more secure than a certificate from one of the signing authorities, users can upload their own certificate to be used by the VNS3:ms instance.



Administration: General Settings - SSL Certificates

Before adding a custom SSL certificate to a VNS3:ms instance, Cohesive Networks strongly recommends creating and downloading a DB Backup from the System Administration>Backup page. This backup can be used to re-instantiate the VNS3:ms system in the event the certificate/key pair creates an error (usually due to a mismatch or wrong files specified).

If you are unsure about the SSL Certificate files to upload, contact Cohesive Networks support staff to review.

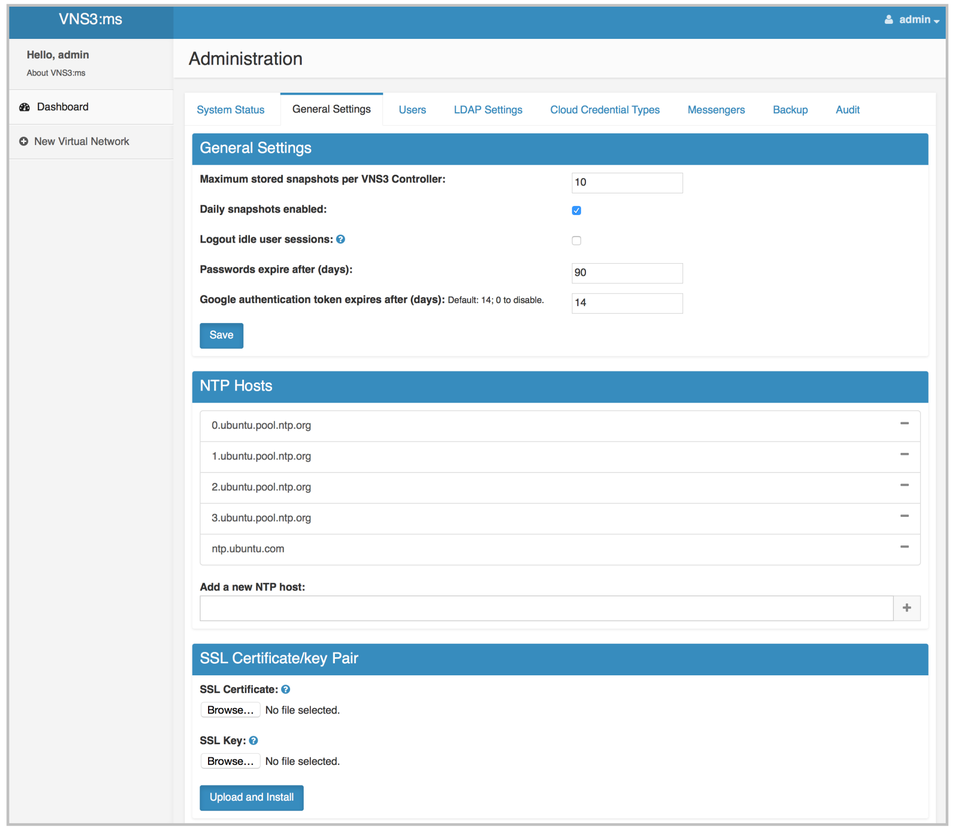
Very simply stated, SSL Certificates for HTTPS interactions provide web users website ownership verification (so users can make sure they are interacting with an organization they intend) and encryption of communication to that website.

In order to be granted an SSL Certificate, a site owner needs to create a private key file (use later in the interactions between the web browser and the actual web server). This private key file is then used to generate a Certificate Signing Request (CSR) that is sent to a Certificate Authority (CA) like Verisign or Geotrust.

The Certificate Authority then sends back the SSL Certificate which includes information about the owner of the certificate, period of validity, URL that is certified and the ID of the CA, the public key used for encrypting communications and a hash to ensure the certificate is valid and not compromised.

The SSL Certificate along with the Private key used to generate the CSR are the two files required to add the Certificate to a VNS3 instance.

The next page reviews the relevant items and how to upload the SSL Certificate to VNS3.



Administration: General Settings - SSL Certificates

To order an SSL Certificate from a Certificate Authority you need to validate you are the owner of the specific URL you are certifying (typically via email validation or similar depending on the CA) and generate a CSR to send to the CA. The CA then uses the CSR to create the SSL Certificate.

To generate a CSR you first must create a Private Key. This document's example uses openssl. NOTE: VNS3 requires the private key to be an RSA key.

```
openssl genrsa -out vns3-example-com.key 2048
```

Once the private key is created, use it to generate the CSR with the following:

```
openssl req -new -sha256 -key vns3-example-com.key -out vns3-example-com.csr
```

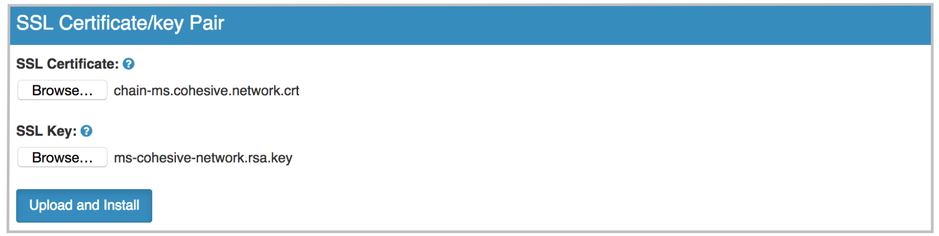
The CA will send back one or multiple Certificates:

- Root Certificate - typically not needed for VNS3
- Intermediate Certificate - included if the CA is not a Root CA
- End User Certificate - the certificate for the actual URL you plan on secure

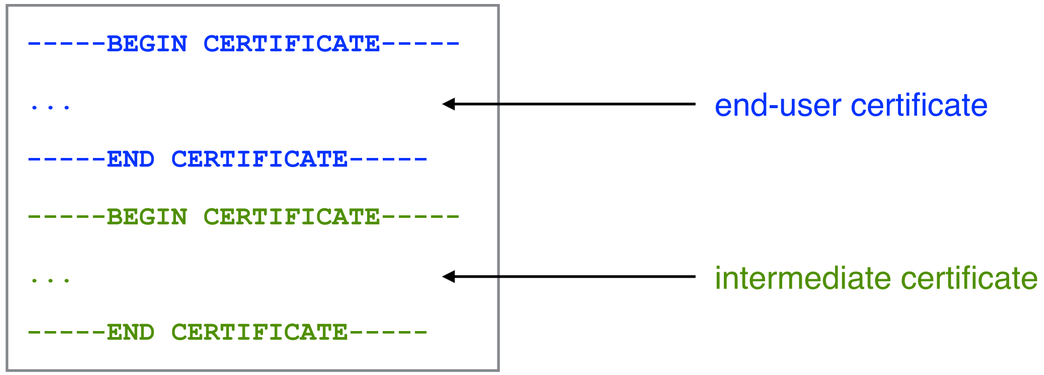
Upload the SSL Cert or SSL Certificate Chain in the event your CA provided an intermediate Certificate (see example to the right) under the SSL Certificate file selection. General begins with "-----BEGIN CERTIFICATE-----".

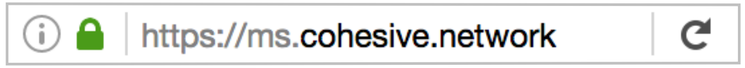
Then upload the Private RSA key file used to generate the CSR under the SSL Key file section. Generally begins with "-----BEGIN RSA PRIVATE KEY-----".

Click Upload and Install.



certificate-chain.crt



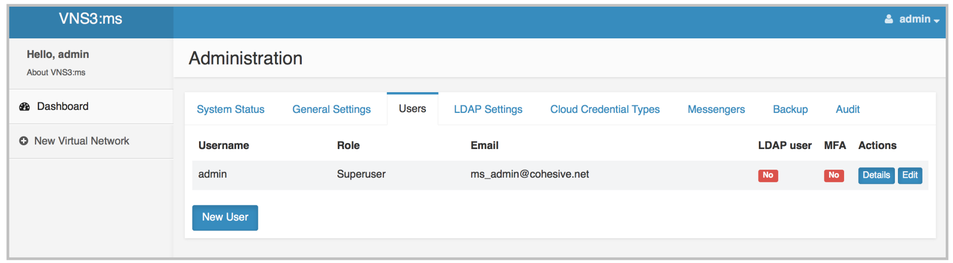


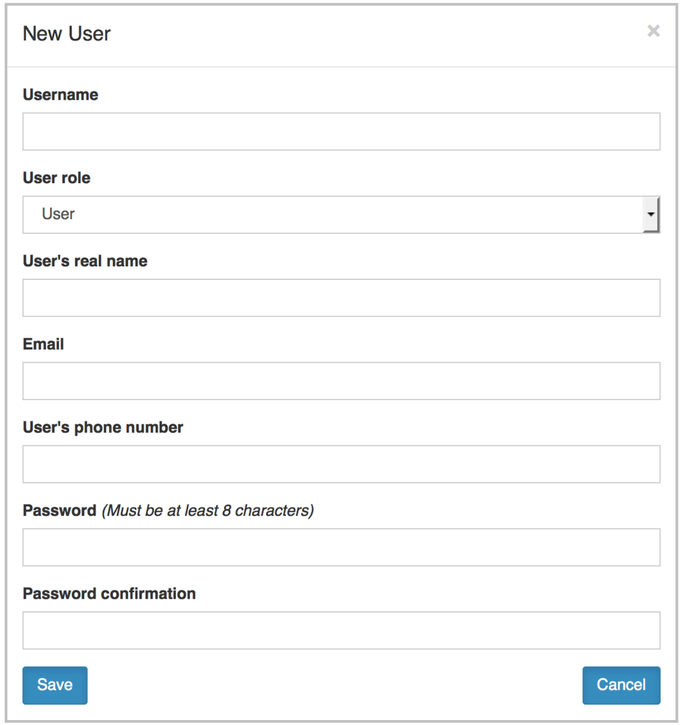
Administration: Users

Click **Users** to add VNS3:ms UI user accounts.

Currently two types of users are supported; admin and user (read-only).

To add a user click **Add User**, enter the required information, then click **Save**.





Administration: LDAP Settings

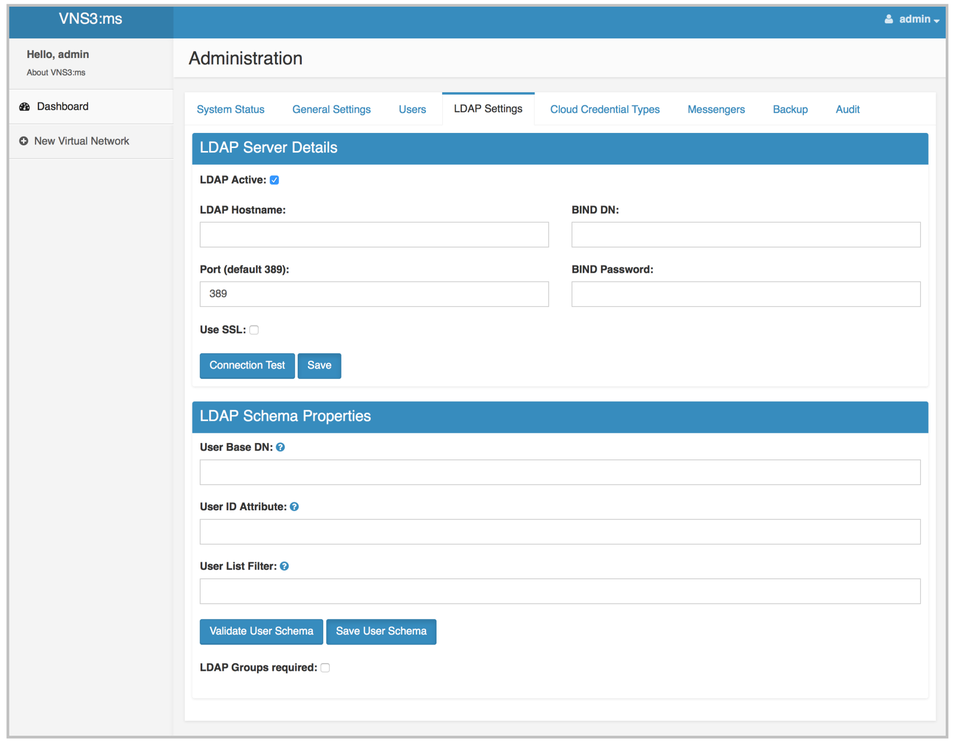
VNS3:ms Administration section is available by clicking on the **admin** top right corner drop down menu, then click on **System Administration**.

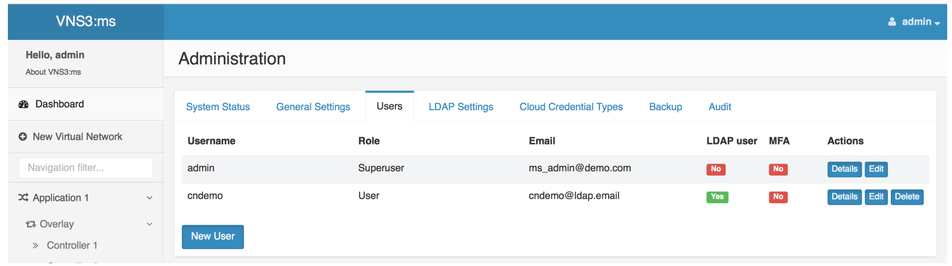
Click **LDAP Settings** to set to setup a connection between VNS3:ms and an existing LDAP server for user and role management.

The **Connection Test button** is useful in validating the VNS3:ms system has network extent to the LDAP server that's being configured.

Once an LDAP server and Schema Properties have been appropriately configured and saved, the LDAP users will be added to the user page and flagged as LDAP users. The default user role is the read-only user but administrator account privileges can be added by clicking the **Edit** button.

If the LDAP connection drops, the LDAP users will remain listed on the Users page but LDAP users will not be able to log into the VNS3:ms instance as the authentication with the LDAP server will not be able to complete.





Administration: Backup

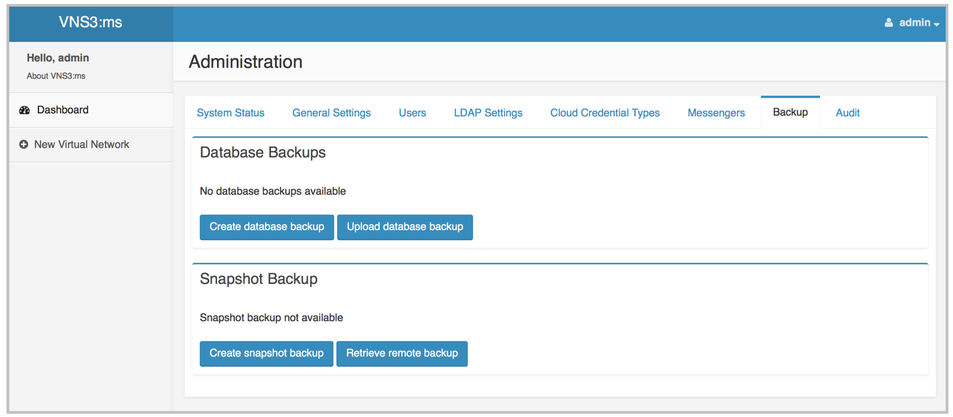
VNS3:ms Administration section is available by clicking on the **admin** top right corner drop down menu, then click on **System Administration**.

Click **Backup** to create and manage the back files for the VNS3:ms system. Backup files are very similar to the VNS3 Snapshots in they contain all the runtime configuration information of a VNS3:ms system.

From the Backup page you can create a Backup file, download that file locally, upload a Backup file or restore the state of the VNS3:ms system from one of the Backup files already created.

NOTE: if you decide to restore the VNS3:ms state from a previous Backup file, the system will reboot as it loads the Backup and you will be logged out.

It is recommended best practices to keep a current Backup file for recovery purposes.

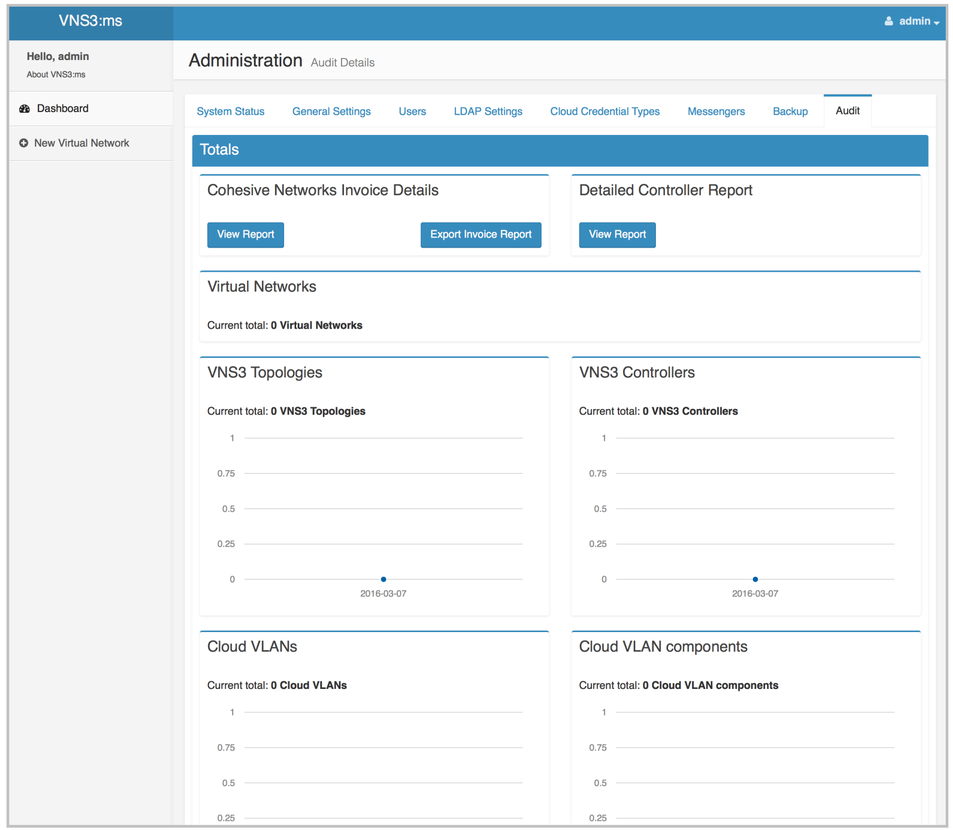


Administration: Audit

VNS3:ms Administration section is available by clicking on the **admin** top right corner drop down menu, then click on **System Administration**.

Click **Audit** to see your usage of VNS3:ms. Cohesive Networks charges for the VNS3:ms product using the Controller Month metric (Monitored VNS3 Controller Instance per month). Once a month you will send Cohesive Networks the audit file that will be used to generate the invoice.

NOTE: the audit file is a signed and encrypted zip file with usage info only, no password information is included.



VNS3 Document Links

VNS3 Product Resources - Documentation | Add-ons

VNS3 Administration Document
Covers the administration and operation of a configured VNS3 Controller. Additional detail is provided around the VNS3 Firewall, all administration menu items, upgrade licenses, other routes and SNMP traps.

VNS3 Docker Instructions
Explains the value of the VNS3 3.5 Docker integration and covers uploading, allocating and exporting application containers.

VNS3 Troubleshooting
Troubleshooting document that provides explanation issues that are more commonly experienced with VNS3.