virtana

VirtualWisdom 6.7 Administrator Guide

Download PDF version

Updated for VirtualWisdom 6.7.x releases

Table of Contents

Chapter 1

Installation and Configuration

Installation and much of the configuration of VirtualWisdom is performed with the assistance of Virtana Services.

Some aspects of the VirtualWisdom configuration can be done or modified after the initial configuration is complete. You must have administrator privileges to access the Settings tab, from which most configuration tasks are performed.

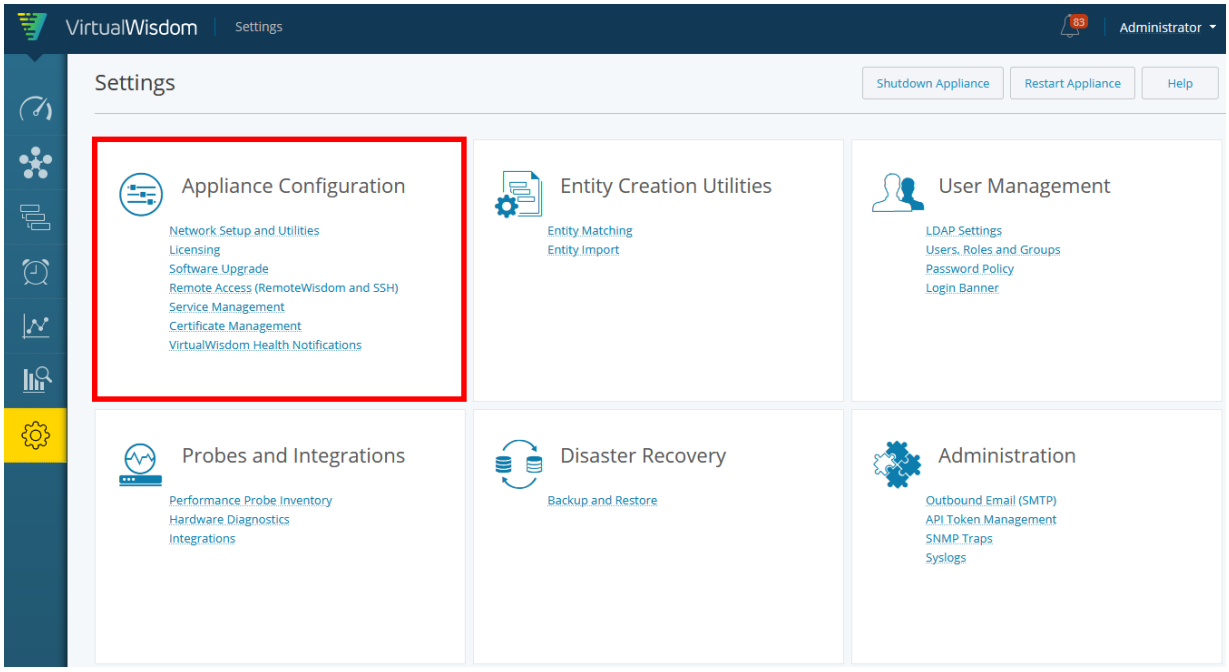
Appliance Configuration

NOTE
The appliance configuration feature is available only to users with the **vw-admin** role.

The VirtualWisdom Platform Appliance, Model 4220, also known as the Appliance, hosts the VirtualWisdom software stack, providing a platform for interacting with the data set collected from software and hardware probes.

The Appliance is a purpose-build hardware server that collects and correlates data from the VirtualWisdom probes and integrations. The Appliance also contains a feature called **RemoteWisdom** that allows remote access to the VirtualWisdom portal for troubleshooting, upgrades, and configuration.

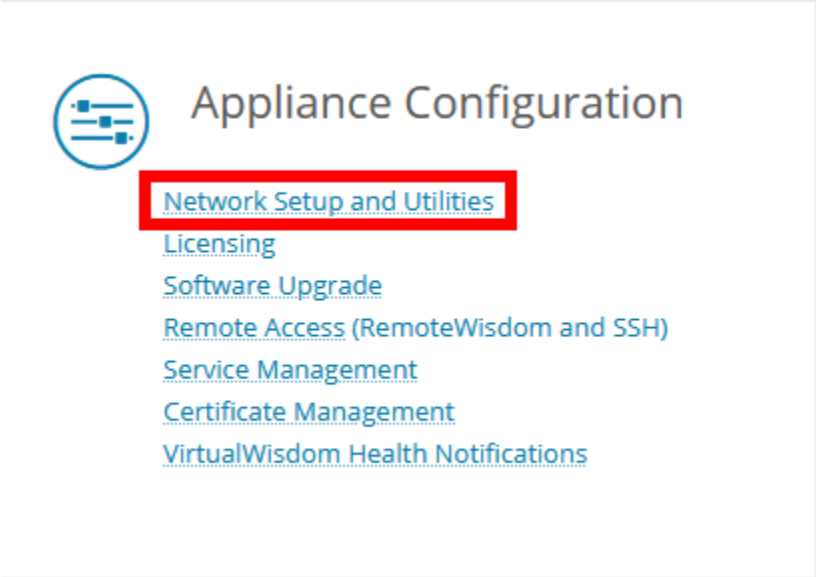
To manage the Appliance's configuration, navigate to **Settings** and refer to the **Appliance Configuration** section.



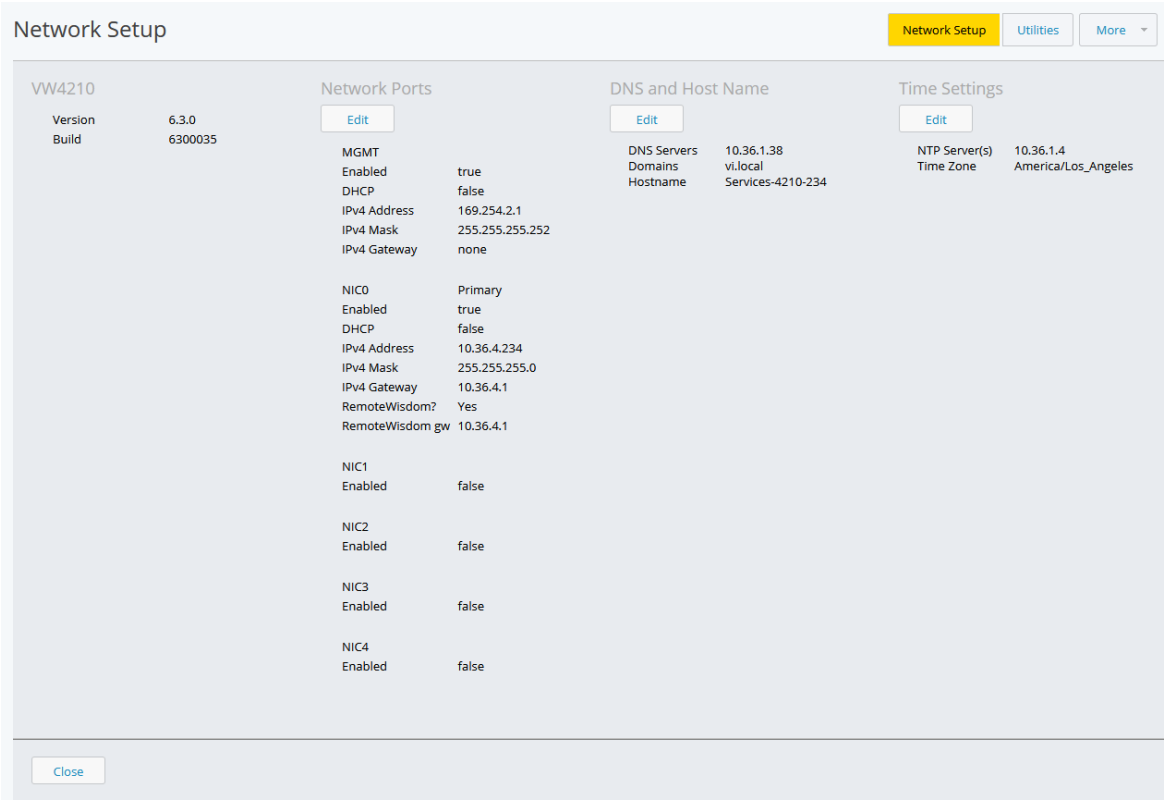
Network Setup and Utilities

The **Network Setup and Utilities** features lets you configure the VirtualWisdom Appliance's network.

1. Select **Network Setup and Utilities** from the **Settings** screen to modify the appliance's network settings.



2. The **Network Setup** page is displayed. This manages the configuration for a single NIC. See Configure Multiple NICs [8] for information on configuring more than one NIC.



> **NOTE**
> If you are deploying an OVA for the VirtualWisdom Virtual Edition, the **Network Ports** section of the **Network Setup** screen contains information for only the NIC0 port. The MGMT port as well as NIC1, NIC2, NIC3, and NIC4 do not apply to the Virtual Edition. See the VirtualWisdom Management Software, Virtual Edition Setup Guide for more information.

You can edit the following network settings for the appliance:

- DNS address
- Domain name
- Hostname
- Language
- NTP

> **NOTE**
> It is imperative that all VirtualWisdom data sources are synced to the same NTP sources that will be configured in VirtualWisdom, otherwise the platform might reject data. If syncing is not possible, then a data source's time should be set to the same time as VirtualWisdom.

- Timezone

> **NOTE**
> As specified in the VirtualWisdom Platform Appliance Guide, it is recommended that you set the time zone to the one in which the Appliance is deployed.

- NICs 0-4, and their associated DHCP or static IP settings

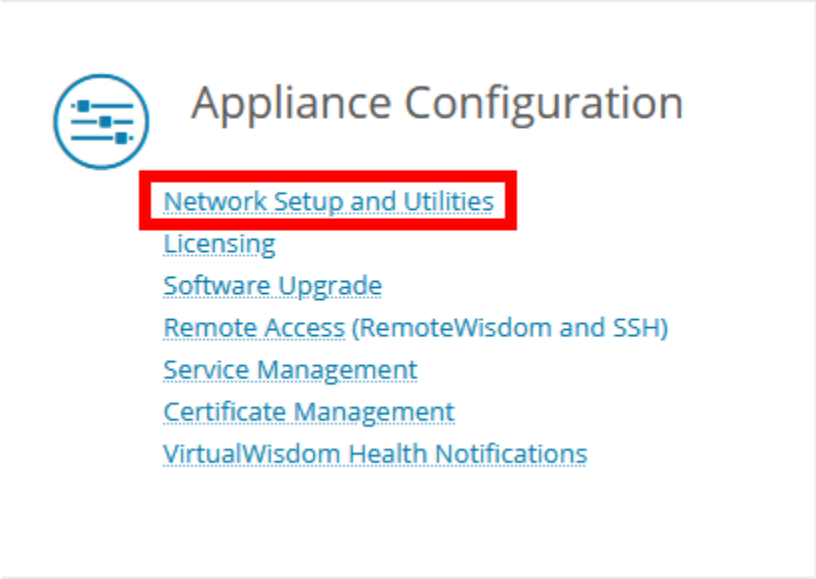
> **WARNING**
> If you change from static IP to DHCP connectivity as part of the network configuration of the VirtualWisdom appliance, the DNS settings are not updated by DHCP. You must manually update the DNS settings.

Configure Multiple NICs

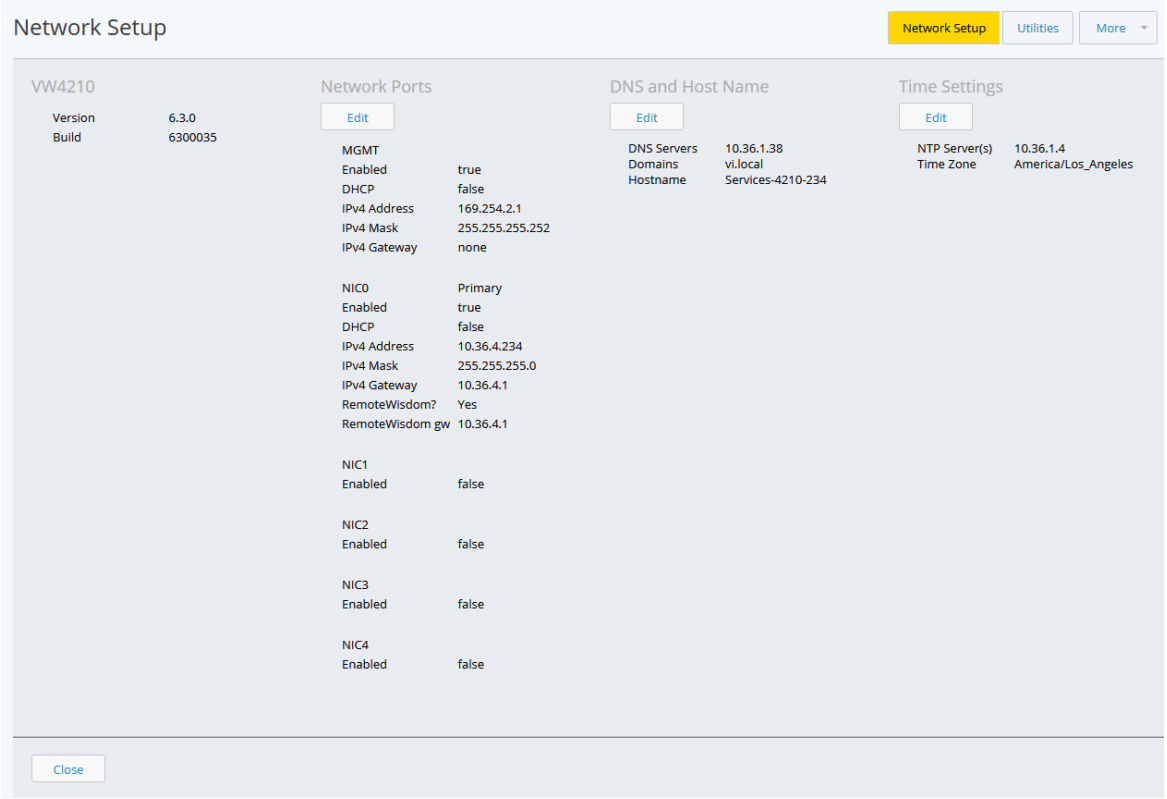
When you first set up your Appliance, you specify the configuration for NIC0 using the MGMT port. NIC0 is active by default and cannot be disabled. You can configure any, none, or all of the following NICs: NIC1, NIC2, NIC3, and NIC4. The example in this section configures NICs 1-4.

To configure the Appliance:

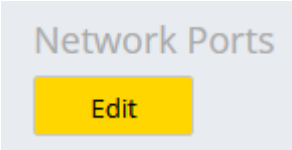
1. From the **Settings** screen, click **Network Setup and Utilities**.



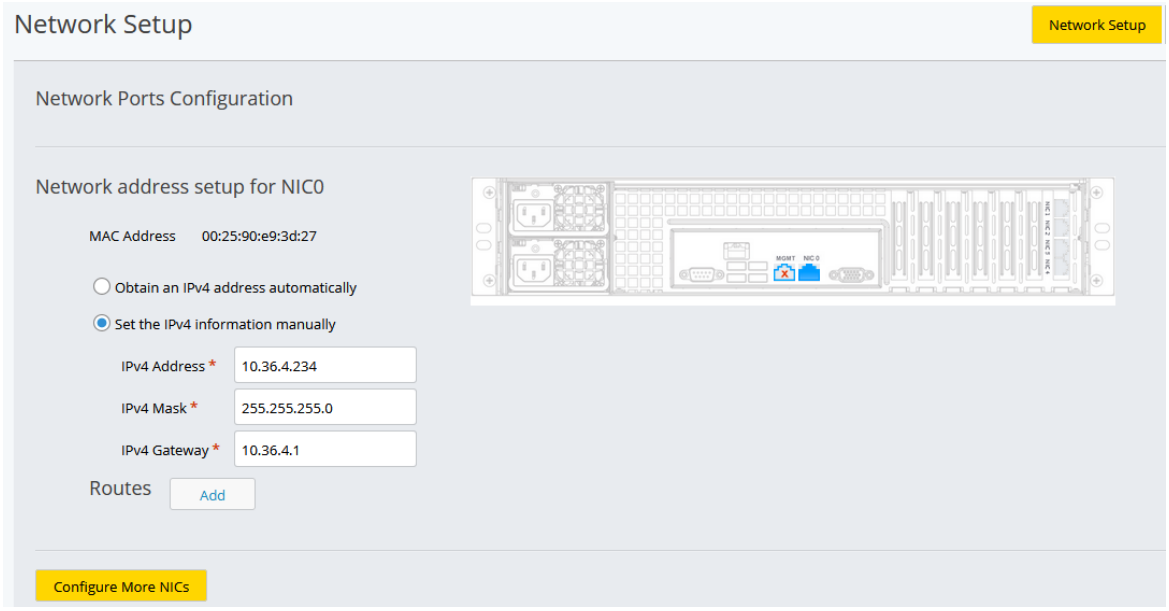
2. The current settings for VW4210/4220, Network Ports, DNS and Hostname, and Time and Region are summarized on the **Network Setup** page.



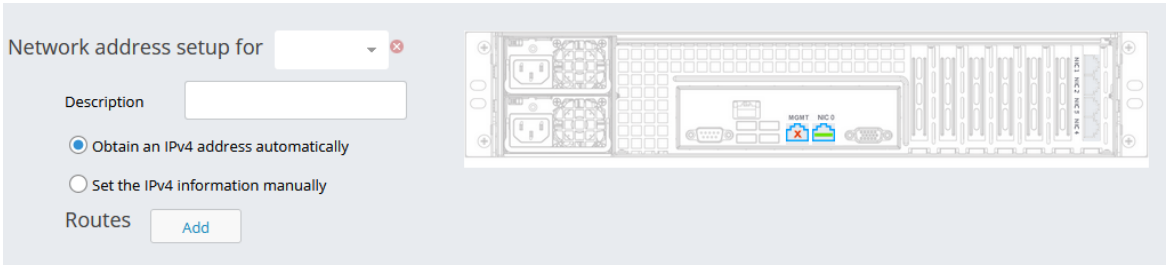
3. Click the **Edit** button corresponding to **Network Ports**.



4. The **Network Ports Configuration** page displays. Click the **Configure More NICs** button.



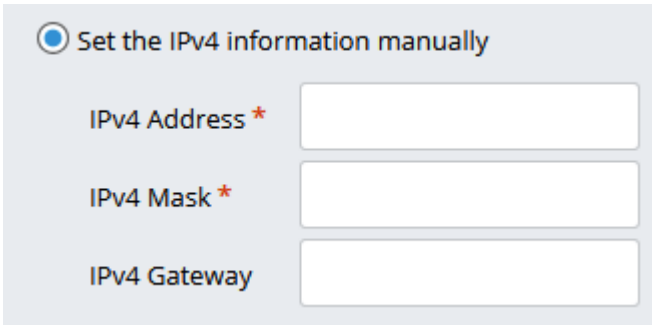
5. The screen area is displayed below the setup for NIC0 and above the **Configure More NICs** button.



You can click the "x," to the right of the **Network address setup for** drop down to remove the NIC configuration from the system.

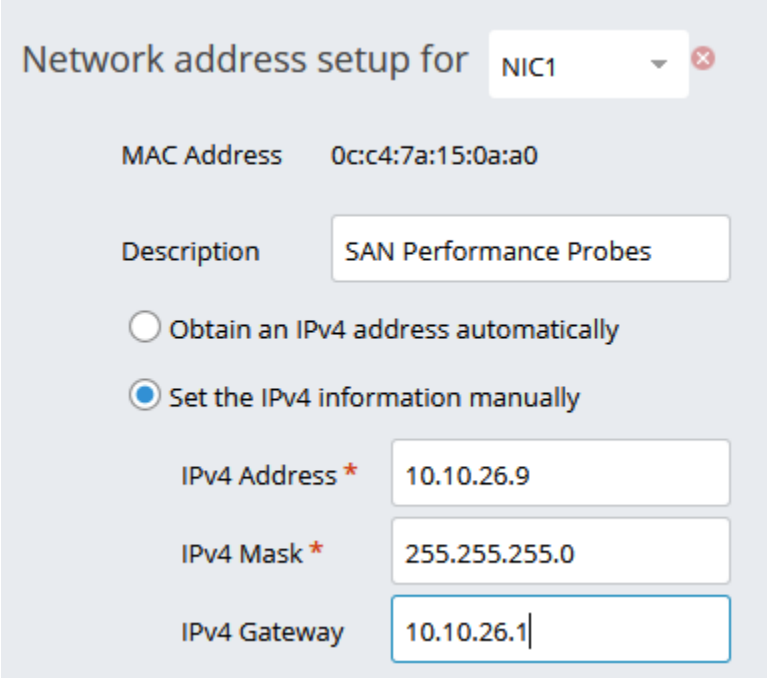
The **Obtain an IPv4 address automatically** radio button is selected by default. Use this button to configure the Appliance using DHCP.

If you want to configure the Appliance using a static IP address, select the **Set the IPv4 information manually** radio button. Selection of this radio button displays the **IPv4 address, IPv4 mask**, and **IPv4 gateway** fields.



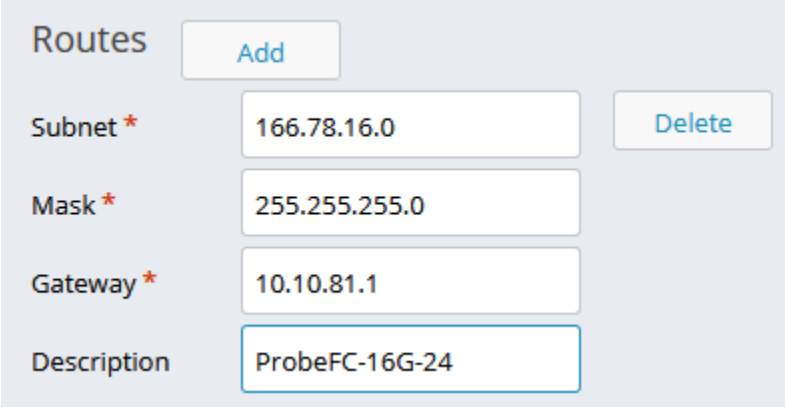
> **WARNING**
> If you change from static IP to DHCP connectivity as part of the network configuration of the VirtualWisdom appliance, the DNS settings are not updated by DHCP. You must manually update the DNS settings.

6. Start by configuring NIC1:
   a. Select **NIC1** from the **Network address setup for** drop down menu.
   b. Enter a **Description** for the NIC.
   In this example, the description for NIC1 is “SAN Performance Probes.”
   c. Select the **Set the IPv4 information manually** radio button and enter the information for the **IPv4 address, IPv4 mask** and **IPv4 gateway** fields.
   In this example, the IPv4 address is 10.10.26.9, the IPv4 mask is 255.255.255.0, and the IPv4 Gateway is 10.10.26.1.



7. Click the **Configure More NICs** button to configure another NIC. Each time that you click this button a new NIC configuration screen displays.
   Repeat Step ??? for each NIC that you want to configure.
8. Add the routes for the NICs you added. In this example, we'll add the route for NIC1.
   Click the **Add** button next to **Routes.**

9. Enter the route information (subnet, mask, gateway, and description) and click **Save**.



10. The **Info** dialog displays. The appliance restarts and returns you to the VirtualWisdom login page.
11. To verify the changes, return to the **Network Setup** page and review the configuration.

NOTE

If **RemoteWisdom** was enabled during the initial appliance set up, it was assigned to NIC0. If you choose to reassign RemoteWisdom to another NIC, follow these steps:

1. Select the NIC from the **Select required port for RemoteWisdom** drop-down menu. Only configured NICs are listed in this menu.
2. Optionally, you can specify a gateway for RemoteWisdom. If no Gateway is specified, the gateway of the RemoteWisdom NIC is used.

VirtualWisdom, Virtual Edition

You can deploy an OVA for the VirtualWisdom Virtual Edition. Once deployed, you can configure NIC0.

You can configure the network settings (IP addresses, DNS servers, and NTP servers) from VirtualWisdom, from VMware vCenter, or from the VMware OVF Tool.

See the *VirtualWisdom Management Software, Virtual Edition Setup Guide* for details.

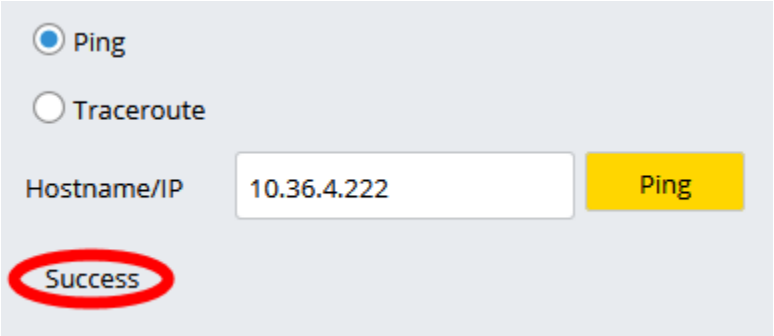
Utilities

The **Utilities** button allows you to manage the ping and traceroute diagnostic tools.

Using the Ping Utility

Ping functionality is specifically meant to provide feedback to the user on the connection status of NIC0, the port configured with the Initial Configuration Wizard. You can also use ping to check the connectivity of probes, DNS and NTP servers, SMI, switches, LDAP servers, backup destinations, or other data center components.

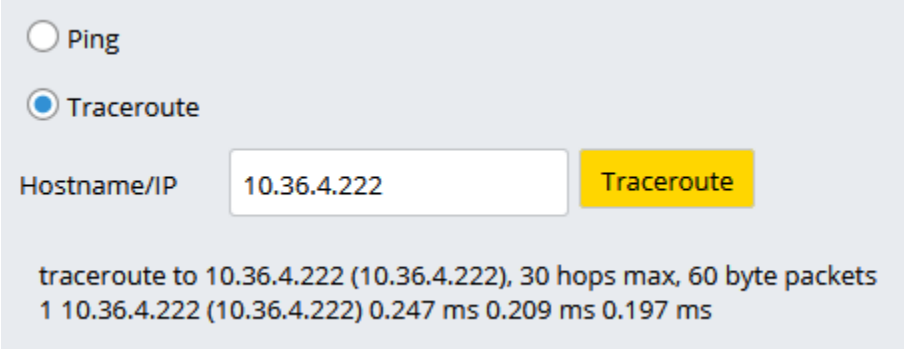
1. Type in the hostname or IP address that you wish to ping and click **Ping**.
2. A **Success** message indicates a successful ping. An **Error** dialog box indicates that the ping was not successful.



Using the Traceroute Utility

Traceroute allows you to verify the route (network path) of network packets. The ability to view this route makes it easier to determine where along a network path an error might have occurred.

1. Select the **Traceroute** option.
2. Type in the hostname or IP address that you want to trace the route for and click **Traceroute**.
3. The route that network packets travel from the Appliance to the hostname or IP address specified are listed.



Licensing

From the **Settings** page you can manage and import VirtualWisdom licenses, if you have administrator privileges.

Beginning with VirtualWisdom 6.2, licenses are purchased as a base license with add-on Wisdom Pack Licenses. Each Wisdom Pack incorporates an established set of VirtualWisdom components based on site requirements and infrastructure configuration. Licenses purchased prior to VirtualWisdom 6.2 must have been converted by Virtana before updating to 6.2 or later. Therefore, it is strongly recommended that you do not perform the update without the Wisdom Pack licenses ready.

Base Licenses

The Base License is the minimum license required for a VirtualWisdom installation. A Base License is required before installing Wisdom Pack Licenses in your environment.

A Base License can be a Perpetual, Subscription, or Evaluation type. Enterprise (Appliance) Edition and Virtual Edition of VirtualWisdom can accept Perpetual and Subscription Base License types.

Only one Base License type can be installed on a system. For example, you can install a Perpetual Base License for an Enterprise Edition, or a Subscription Base License for a Virtual Edition, etc.

The following components are included as part of the standard VirtualWisdom Base License:

- Core components of VirtualWisdom (Dashboard, Topology, Inventory, Alarms, Reports)
- All VirtualWisdom Analytics
- AppDynamics, Dynatrace, and ServiceNow Integrations
- REST API SDK

Related Topics

???

???

VirtualWisdom, Virtual Edition [0]

Wisdom Pack Licenses

Each Wisdom Pack can be purchased as either a Subscription or a Perpetual License for the Enterprise Edition or Virtual Edition of VirtualWisdom. Evaluation Licenses are also available for Wisdom Packs, so you can assess the value of any Wisdom Pack for your environment.

In addition to the Base License components, each Wisdom Pack includes specific components, required for particular environments. Following are the available Wisdom Packs, which can be implemented individually or in combination, depending on your needs:

Wisdom Pack	Description	Supports[1,2]	Comments
Operating System	Each (1) license can be applied to any included OS. Each count of the license also includes 5 NetFlow endpoints.	• Operating System integration • NetFlow integration (5 endpoints)	Example: If you purchase 1,000 Operating System Wisdom Packs, then you also receive licenses for 5,000 NetFlow endpoints, even if you do not purchase any IP Network Wisdom Packs.
Virtualization	Each (1) license can be applied to 1 included hypervisor or specialized OS. Each count of the license also includes 50 NetFlow endpoints.	• Microsoft Hyper-V integration • VMware vSphere integration • IBM PowerVM integration • NetFlow integration (50 endpoints)	Hyper-V, vSphere, and PowerVM are all licensed by host (specialized OS).

Enterprise Storage	Each (1) license enables monitoring of 1 controller. Depending on the array type, the controller can be managing N number of engines or nodes (usually 2 or 4). The ratio in the Supports column is read as "1 license to N engines / nodes".	• Dell EMC VMAX Integration: 1:2 engines (2 directors per engine) • IBM SVC Integration: 1:2 nodes • Dell EMC Isilon Integration: 1:4 nodes • NetApp FAS Integration: 1:4 nodes	Example: To monitor 1000 Isilon nodes and 500 SVC nodes, you need 500 counts of the Enterprise Storage Wisdom Pack, in which 250 would be consumed to monitor 1000 Isilon nodes (250 controllers) and 250 consumed to monitor 500 SVC nodes (250 controllers).
Software-defined Storage	Each (1) license enables monitoring of 1 SDS node	• Dell EMC VxFlex OS integration • VMware vSAN integration	
SAN Switch	Each (1) license enables monitoring of 1 SAN switch port.	• Brocade SAN integration • Cisco SAN integration	
Wiredata	Each (1) license includes 4 Link Credits, where each count of each type of Link consumes a certain number of Link Credits.	Credits consumed per count of each link type: • 10GE Links: 0.5 • 4GFC Links: 0.25 • 8GFC Links: 0.5 • 16GFC Links: 1 • Cisco STS Links: 0.25	Hardware probes decrement the license count based on types of ports on the probes (current link speed). If the current speed on the link changes, the counts are automatically recalculated. Cisco STS decrements the count based on number of Cisco STS-enabled ports used. With 1 Wire Data Wisdom Pack, some examples of what you can monitor include: 16 x 4GFC Links, *OR* 8 x 10GE Links, *OR* 8 x 8GFC Links, *OR* 4 x 16GFC Links, *OR* 16 Cisco STS Links

FC32 Wiredata	Each (1) license includes 4 Link Credits.	1 credit consumed per link.	Hardware probes decrement the license count based on types of ports on the probes (current link speed). If the current speed on the link changes, the counts are automatically recalculated. One (1) FC32 Wiredata Wisdom Pack can monitor 4 x 32GFC Links Note: FC32 Wiredata Wisdom Pack licenses are currently not compatible with line speed rates other than 32G
IP Networks	Each (1) license enables monitoring of 1 NetFlow endpoint.	NetFlow Integration (1 endpoint)	

1 - A single quantity of a Wisdom Pack that includes multiple integration types cannot be allocated to multiple VirtualWisdom servers. For example, if you have a Virtualization Wisdom Pack, you cannot allocate a Hyper-V integration on server A and allocate the NetFlow Integration on server B.

2 - Additional supported items can be added between releases. Check with Virtana for the latest support information.

3 - Each unique monitored IP address consumes 1 count of NetFlow license, whether it is the source or destination IP at the time it was first discovered. Multicast/broadcast IP addresses do not consume NetFlow licenses.

Related Topics

???

???

Evaluation Licenses

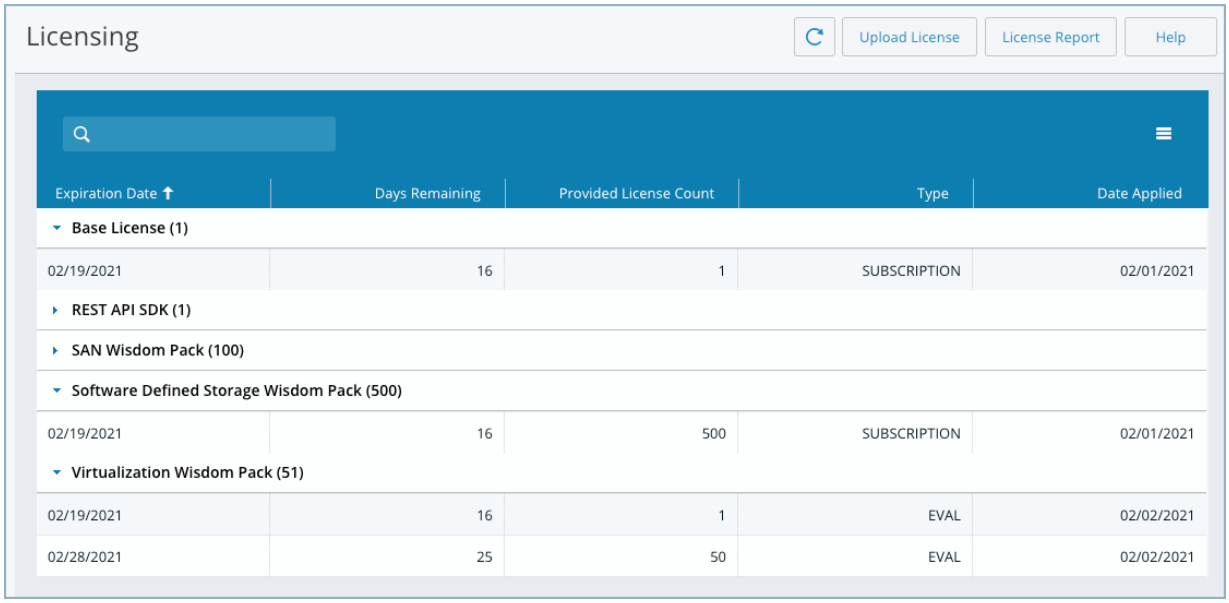
Wisdom Pack evaluation licenses are available for VirtualWisdom integrations. These licenses allow you to easily try out any integrations in your environment.

Wisdom Pack evaluation licenses are separate from, and do not affect, paid VirtualWisdom subscription or perpetual licenses. However, each evaluation license does add a fixed number of integration licenses to the licenses already on the appliance.

Evaluation licenses expire at a fixed date after *generation* of the license (not installation date). Different evaluation licenses can have different expiration dates. When an evaluation license expires, all licenses it added to the license pool are removed. Once expired, the license cannot be added to any VirtualWisdom platform.

You can upload multiple Wisdom Pack evaluation licenses to an appliance, but each evaluation license can be installed only once on a particular VirtualWisdom instance.

The type and number of evaluation licenses can be viewed on the Licensing page, accessed from the Settings tab. The Licensing table also displays the date the license was applied, the expiration date (after license *generation*), and the number of days remaining before the license expires.



Expiration Date	Days Remaining	Provided License Count	Type	Date Applied
Base License (1)				
02/19/2021	16	1	SUBSCRIPTION	02/01/2021
REST API SDK (1)				
SAN Wisdom Pack (100)				
Software Defined Storage Wisdom Pack (500)				
02/19/2021	16	500	SUBSCRIPTION	02/01/2021
Virtualization Wisdom Pack (51)				
02/19/2021	16	1	EVAL	02/02/2021
02/28/2021	25	50	EVAL	02/02/2021

Evaluation licenses can be applied to VirtualWisdom 6.7.1 or later. The licenses will continue to work after VirtualWisdom upgrades.

Contact your account team or Virtana Support to request an evaluation license.

License Types

The Base License and Wisdom Pack Licenses are installed as a Perpetual, Subscription, or Evaluation License type.

- Perpetual Base
  - Does not expire
  - Full access (Access to version upgrades requires an active Maintenance Contract)

  - Use with Perpetual Wisdom Packs and Evaluation Wisdom Packs
- Subscription Base
  - Expires at end of paid subscription term
  - Full access (as long as the license is not expired)
  - Use with Subscription Wisdom Packs and Evaluation Wisdom Packs
- Evaluation Base
  - Expires upon end of agreed evaluation period (typically 30 or 60 days)
  - Full access, with some limits
  - Use with Evaluation Wisdom Packs

A single VirtualWisdom Server can only accept one (1) type of Base License. The base license type determines which wisdom pack license types can be used.

Uploading a License

All license types are installed the same way.

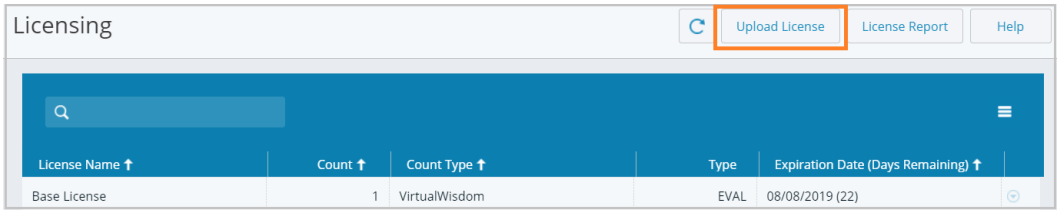
You cannot use a Perpetual License or a Subscription License on an OVA with an Evaluation License. You must deploy a new OVA and upload a new license.

Prerequisites

You must have downloaded the proper license file to a system that is available to VirtualWisdom.

You must have administrator privileges on VirtualWisdom.

1. From the *Settings* tab, click **Licensing**.
   The *Licensing* page displays information about the VirtualWisdom Base License and all of the WisdomPack licenses installed.
   Licenses are contained in a single file that can be replaced with new values. Values can be replaced, but not added, to a license file.
2. Click **Upload License**.



3. Use the **Browse** button to select the license file and click **Upload**.
   A dialog box displays, warning you that the upload deletes previous licensing information.
4. Click **OK**.

The new license file is uploaded and a message informs you that the license file was successfully loaded.
The new license displays on the Licensing page.

TIP
You can view license usage details by accessing License Reports.

License Notifications

Licensing notifications display in the VirtualWisdom UI, such as warnings that a license is about to expire. The content of the Licensing dialog box is different, depending on whether you are logged in as a VirtualWisdom administrator (with the *vw-admin* role assigned) or a user that is not assigned administrator privileges.

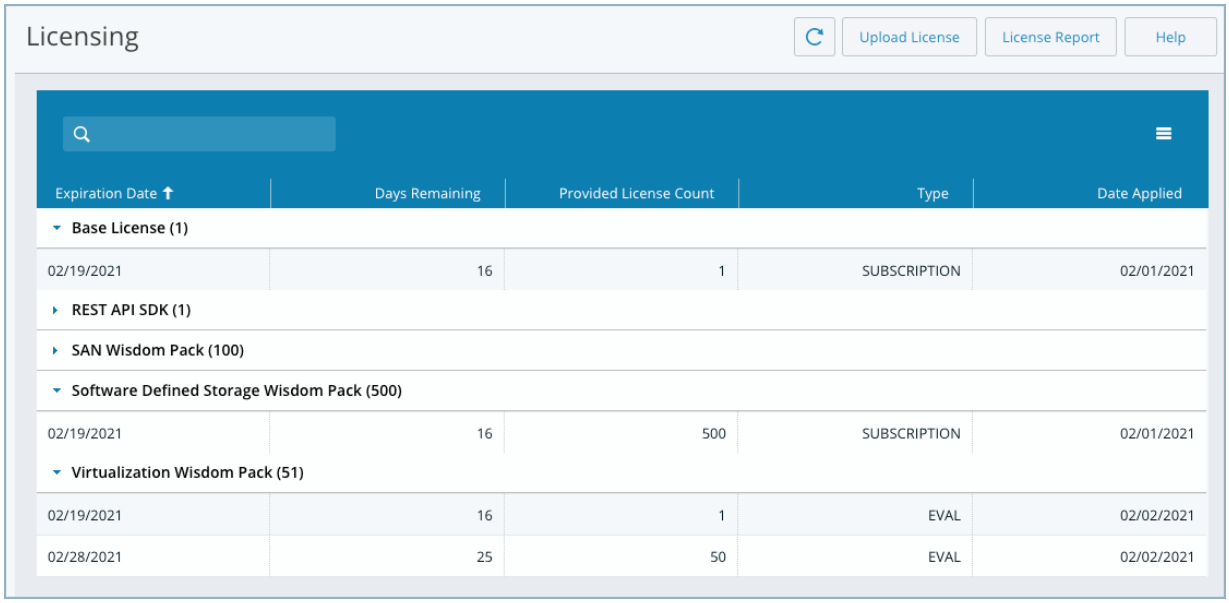
Non-administrators do not have access to configuration settings in VirtualWisdom and so cannot upload or modify licenses.

NOTE
If you restore a backup on an appliance with no license, no health notifications are generated to notify you that the license is not there. Always ensure the appliance is licensed after restoring from a backup.

NOTE
Oversubscription health notifications are not generated for software integrations after a VirtualWisdom 6.1 restore. Restoring a VW 6.1 backup overwrites the licenses.

Expiring Licenses

You can view the expiration date of any WisdomPack License, Base License, or Evaluation License from the Licensing page on the Settings tab.



Expiration Date	Days Remaining	Provided License Count	Type	Date Applied
Base License (1)				
02/19/2021	16	1	SUBSCRIPTION	02/01/2021
REST API SDK (1)				
SAN Wisdom Pack (100)				
Software Defined Storage Wisdom Pack (500)				
02/19/2021	16	500	SUBSCRIPTION	02/01/2021
Virtualization Wisdom Pack (51)				
02/19/2021	16	1	EVAL	02/02/2021
02/28/2021	25	50	EVAL	02/02/2021

Within thirty days of a Base or Wisdom Pack license expiring, VirtualWisdom alerts the user in the following ways:

- Displays a dialog in the UI with a warning that licenses are about to expire
- Displays the expiring licenses in red font on the Licensing page

When a Base or Wisdom Pack license expires and results in oversubscription, VirtualWisdom alerts the user and Virtana in the following ways:

- Displays a message in the UI with a warning that licenses have expired
- Displays the expiring licenses in red font on the Licensing page
- Sends an email alert to all VirtualWisdom administrators

Evaluation licenses expire based on the requested length of time assigned to the license, starting from the day the license is generated (not installed). When the license is about to expire, a notification is sent. When the license expires, all license counts associated with the Evaluation license are removed from the appliance.

License Reports

From the *Licensing* page and from the *Integrations* page you can access a **License Report** that shows license usage information, based on license type, such as storage controller, wiredata, OS, etc. For each license type, the report displays the total number of licenses, as well as the number of used and remaining licenses.

Following is a sample License Report page.

TIP

Each license type (wiredata, storage, OS, etc.), is associated with a WisdomPack License. You can view information about each WisdomPack License, such as number and types of licenses, as well as expiration dates, by accessing the Licensing page.

Software Upgrade

Use the VirtualWisdom **Software Upgrade** task on the Settings tab to upload an update of VirtualWisdom to the Appliance.

About This Task

If provided an experimental bundle by technical support, also see ???.

Prerequisites

- You must have downloaded the update bundle to a place from which your web browser can access it.
- You must have administrator privileges on VirtualWisdom.
- All users, other than the administrator performing the upgrade, must be logged out of VirtualWisdom

Steps

1. From the Settings tab, click **Software Upgrade**.
   The *Software Upgrade* page displays.
2. Use the **Browse** button to select the update file.
3. Click **Upload** to upload the selected file.
   The *Software Upgrade* page displays file upload and validation progress. If validation is successful, the update is ready to apply.
   If installing a bundle provided by technical support outside of the normal release cycle, it might not be signed for general distribution. These bundles display a warning notice that you are uploading an experimental bundle. See "Installing an Experimental Bundle" if you see that warning.

   NOTE
   Uploading an update of VirtualWisdom does not actually update the Appliance, rather *it uploads an update of VirtualWisdom to a staging area in the Appliance.*

4. To apply the VirtualWisdom update, click the **Update** button.
   When you click **Update**, the *Info* dialog box is displayed.
   If you decide not to apply the bundle, click **Remove File** to clear the staged bundle.
5. Click **OK** to confirm the update.

If the update requires an appliance reboot, a status box displays instructing you to wait for VirtualWisdom to come up and stating that you will be redirected to the VirtualWisdom login page when the process completes.

VirtualWisdom update reboots your system without warning when the progress reaches 100%. If the page does not automatically update after 10 minutes, manually refresh the browser.

Installing an Experimental Bundle

Typically, VirtualWisdom update bundles are certified for general distribution to all customers, and are digitally signed for that purpose. Occasionally, technical support might provide, and work with you to install, an experimental update bundle intended to address a specific issue that you are experiencing.

Experimental bundles are not available for general distribution and, when uploaded to the appliance, generate a warning that you are uploading an experimental bundle.

If you see this warning unexpectedly, remove the update from the appliance and contact technical support.

Certificate Management

The Certificate Management task allows you to generate a security certificate for use with VirtualWisdom. You can bypass the trusted security certificate warning by generating your own security certificate request and using that request to get a certificate signed by a certificate authority such as Verisign.

It is recommended that you generate your own security certificate and have it signed by the certificate authority of your choice.

Follow these steps to generate a security certificate for VirtualWisdom:

1. From the *Settings* screen, click **Certificate Management**.
   The *Certificate Management* screen is displayed.
2. Click **Generate CSR** to generate a certificate signing request.
   The *Generate CSR* dialog box displays.
3. Enter the following information in the *Generate CSR* dialog box:

Table 1. Generate CSR Dialog Parameters

Parameter	Definition
Country	Two-letter ISO code for the country in which you are located. Required.
State	Province, region, county, or state in which you are located (no abbreviations). Required.
City	Name of the city in which you are located (no abbreviations). Required.
Company	Name of your company. Required.
Department	Name of your department or organizational unit. Required.
Server FQDN	Fully-qualified domain name for your organization. Required.
Email	Email address of the contact at your company, generally an administrator or the IT department.

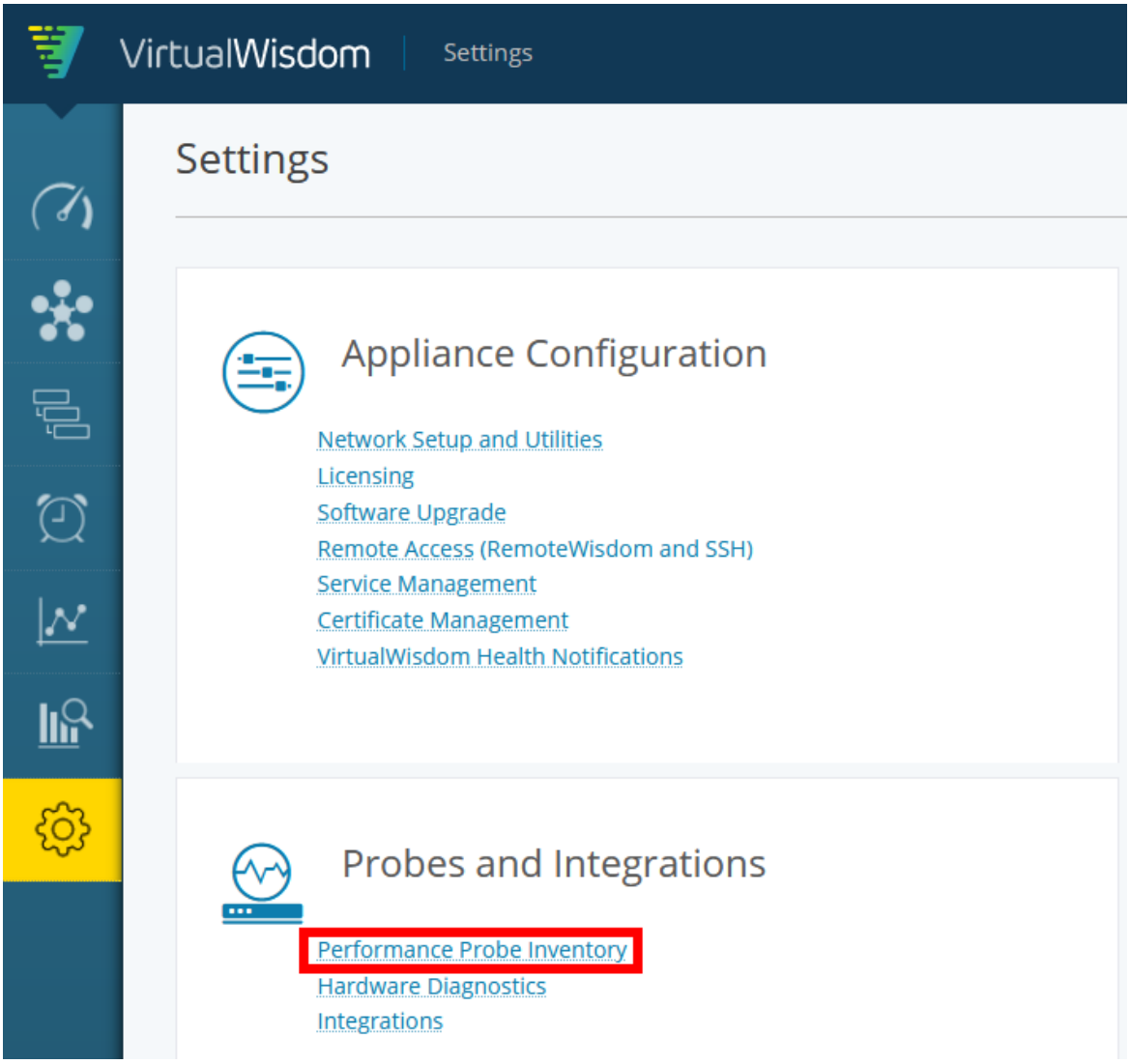
> **WARNING**
> Do not use backslash (\) or double quote (") character in the **Certificate Management Request.**

4. Click **OK**.
   The *Generate CSR* dialog box disappears and you see a message is displayed indicating CSR generation as well as the date and time of the CSR's generation.
5. Click the CSR to get the option to view or download the CSR.
6. Deliver the generated CSR to your certificate authority using your normal process.
   After you get your certificate back from the certificate authority, follow these steps:
7. Complete the SSL Certificate by clicking **Browse** to find your SSL certificate. Concatenate the root certificate, all intermediate certificates, and the signed certificate into one file.
8. Click **Upload** to upload the certificate.
   You are logged out of your UI session. In approximately one minute you are directed to the VirtualWisdom Login screen.

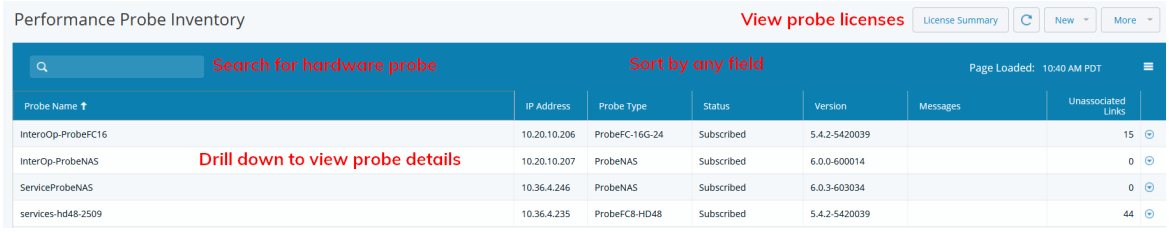
Performance Probe Inventory

The **Performance Probe Inventory** page lets you view and manage your inventory of VirtualWisdom hardware probes.

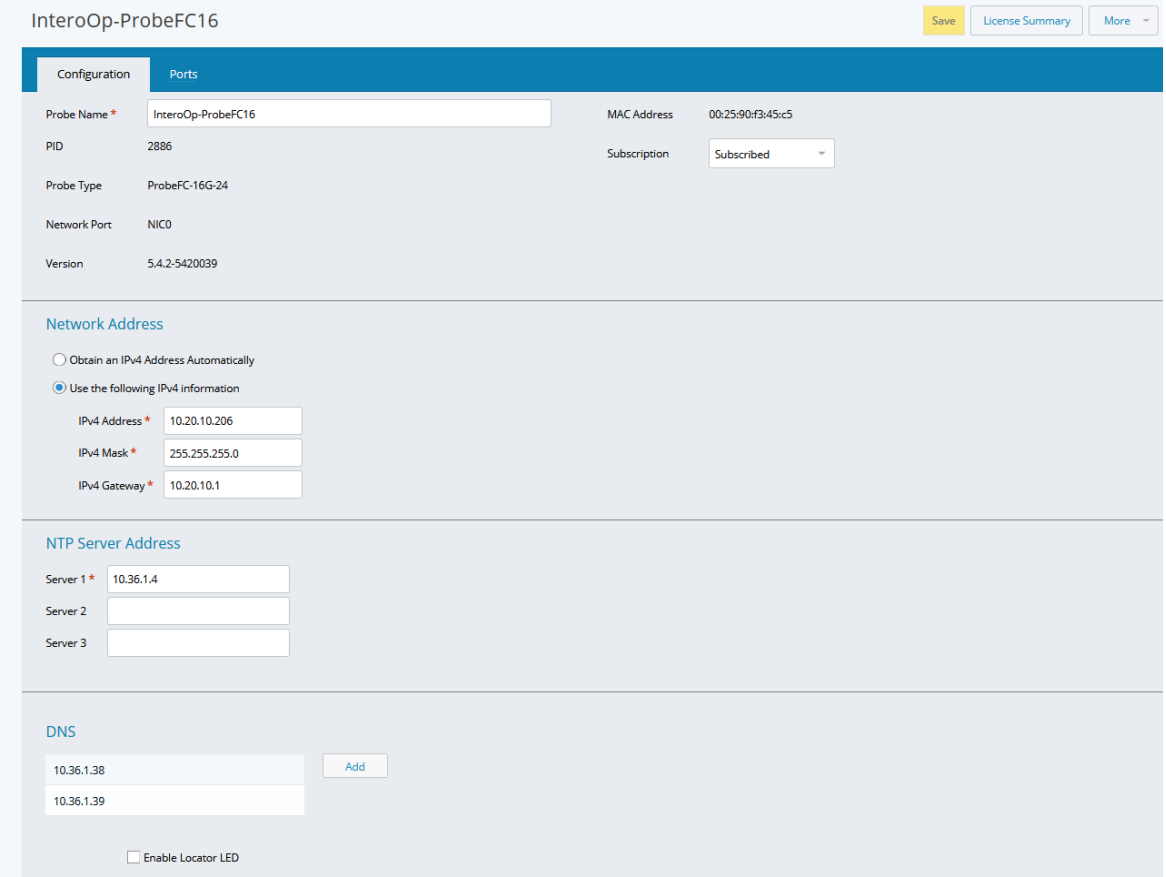
1. To access your hardware probe inventory, select **Performance Probe Inventory** from the **Probes and Integrations** section on the **Settings** page.



2. A list of hardware probes is displayed.
You can use the search field to find a specific probe, sort the list by any of the fields, view licensing information, download logs, add a new probe, or bulk edit.



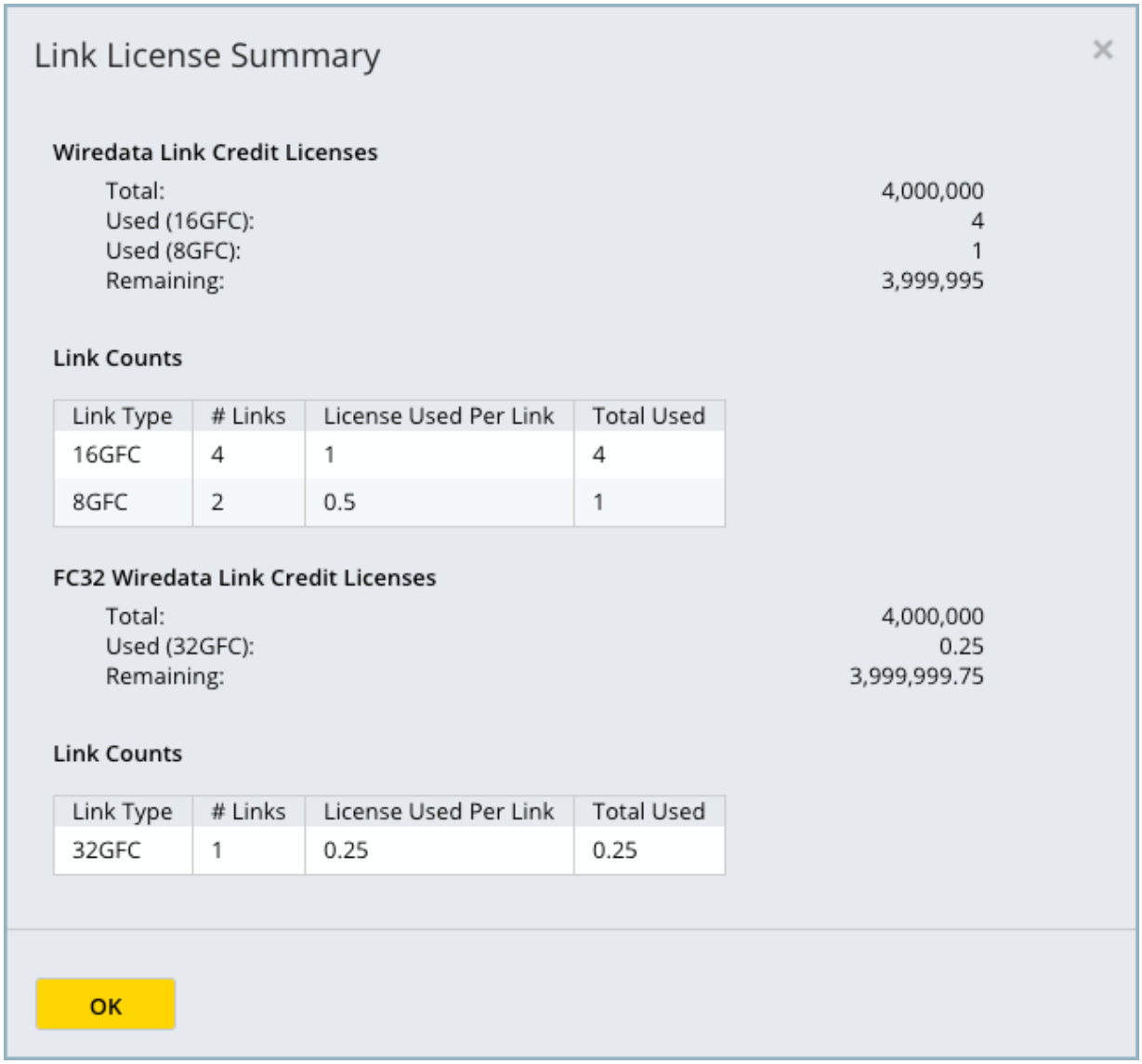
3. Drill down to view probe configuration details.



Viewing Probe Licenses

Click the **License Summary** link to view a summary of all hardware probe licenses available on your system.

A summary of all hardware probe licenses is displayed.



Link License Summary

Wiredata Link Credit Licenses

Total:	4,000,000
Used (16GFC):	4
Used (8GFC):	1
Remaining:	3,999,995

Link Counts

Link Type	# Links	License Used Per Link	Total Used
16GFC	4	1	4
8GFC	2	0.5	1

FC32 Wiredata Link Credit Licenses

Total:	4,000,000
Used (32GFC):	0.25
Remaining:	3,999,999.75

Link Counts

Link Type	# Links	License Used Per Link	Total Used
32GFC	1	0.25	0.25

OK

TIP

Each license type (wiredata, storage, OS, etc.), is associated with a WisdomPack License. You can view information about each WisdomPack License, such as number and types of licenses, as well as expiration dates, by accessing the Licensing page.

ProbeFCs

Power supply units (PSUs) in NAS and SAN probes are numbered 1 and 2, from left to right, as viewed when facing the back panel. The PSUs are hot-swappable.

> **NOTE**
> Before configuring hardware probes, it is recommended that any Brocade and/or Cisco SAN Integrations are configured and have completed their initial discoveries.

Follow these steps to create any of the hardware probes.

1. From the *Settings* page, click **Performance Probe Inventory** to access *Probes and Integrations*.
   The *Performance Probe Inventory* page is displayed.
   The column headings are defined in the following table:

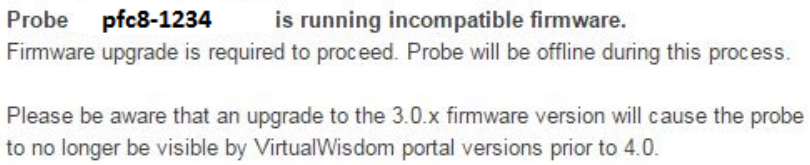
Table 2. Performance Probe Inventory Parameters

Column Heading	Definition
Probe Name	The name you assign to the probe
IP Address	IP address of the probe
Probe Type	Type of hardware probe, for example, ProbeFC-16G-24
Status	Status of the probe: Subscribed, Unsubscribed, Offline, or Faulted (subscribed, but not receiving data).
Version	Firmware version, for example, 6.2.1
Messages	Status information
Unassociated Links	Number of “unassociated links” (links that VirtualWisdom is unable to autoplace); this value is a whole number.

2. Select *ProbeFC* from the **New** drop down menu.
   ProbeFC refers to all probes in the ProbeFC family.
3. Enter the IP address of the probe and click **Next**.

You can use the VirtualWisdom UI to change a Performance Probe's IP address if the initial configuration (Initial IP) is already set. IP addresses can be changed if the old and new IP addresses can be routed from the appliance.

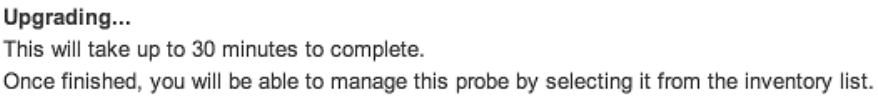
If the probe firmware is incompatible with VirtualWisdom, a message is displayed that identifies that the probe is running incompatible firmware and the Upgrade button displays on the page.



Proceed to Step 4.

If the probe firmware is compatible with VirtualWisdom, the *Create New ProbeFC* page displays. Proceed to Step 5.

4. Follow these steps to upgrade the probe firmware.
   a. Click **Upgrade** to upgrade the firmware.
      The "Upgrading message" and **Close** button appear.

   b. Click **Close**.
      The Hardware Probes Inventory page displays, with the probe listed in the inventory. Notice the that Version column in the inventory shows the firmware version, followed by `Upgrading...`
      A firmware upgrade takes approximately fifteen minutes, during which time you are not able to configure the probe.
      When the upgrade is finished, click the probe in the inventory list to display the *Create New ProbeFC* page. Proceed to Step 5.

   Assuming that your probe is running compatible firmware, the *Create New ProbeFC* page displays. This page is pre-populated with information discovered regarding the probe of the specified IP address. Use the scroll bar to navigate the full *Create New ProbeFC* page.

5. Verify the probe configuration.
   With the exception of the *Subscription* status, the information regarding the probe on the *Create New ProbeFC* page is auto-detected from the hardware probe configuration (and was input from either the probe LCD screen or the Configuration Wizard of the probe).
   Descriptions of the parameters on this page are as follows:

Table 3. Create Hardware Probe Parameters

Parameter	Description
Probe Name	Hostname of the probe
Serial Number	Probe ID
Probe Type	Type of probe: ProbeFC8, ProbeFC8-HD, ProbeFC8-HD48, ProbeFC-16G-24, ProbeFC-16G-12
Version	Firmware version of the probe
Network Address	Network settings (static or DHCP) of the probe
NTP Server Address	NTP server configuration for the probe, can specify up to three
DNS	DNS server setting for the probe, typically two
MAC Address	Network port MAC address
Subscription	Subscribe or unsubscribe the probe, values are Subscribed (default) or Unsubscribed
Enable Locator LED	Enable the locator LED on the probe

The following are descriptions for the column headings in the *Ports* section of the page:

Table 4. Column Headings in the Ports Section

Column Heading	Definition
Port	Port Number.
Link Mode	Auto or manual link association, auto is the default.

Column Heading	Definition
Link	Link association of the link, values are Discovering or *WWN_dev* <--> *WWN_switch*, meaning that the association between the device and switch has been discovered, (*WWN_dev* is the WWN of the device, and *WWN_switch* is the WWN of the switch). **NOTE** Before Link Associations can be configured the following conditions must be met: • Brocade and/or Cisco SAN Integrations must have completed their discoveries • Probes must be subscribed for at least 10 minutes to allow NTP to synchronize and provide relevant data • Hardware Diagnostics for each Probe must show no link errors
Link License	Type of license, values are Auto Assign, None, 4 G, 8 G, 16G, where Auto Assign chooses the license based on link speed.
Configured Speed	Configured speed, values are: no sync, Auto Sense (sense automatically), 1 Gb, 2 Gb, 4 Gb, 8 Gb and 16 Gb. If set to Auto Sense, VirtualWisdom applies the license type to the discovered speed. If no licenses are available for the specific link speed observed, VirtualWisdom attempts to assign a higher link speed license (if available).
Current Speed	Current detected speed, values are: no sync,1 Gb, 2 Gb, 4 Gb, 8 G, 16 Gb, 24 Gb.
Bulk Configuration	Allows for bulk configuration of ports

6. In the *Ports* section of the page, select each port that you want to configure by checking the check box by the port number.
   If you want to configure all the selected ports with the same *Link License* and *Configured Speed* values, you can do a "Bulk Configuration" of multiple ports. Skip to Step 9.
7. Choose the *Link License* for each selected port by clicking on the corresponding *Link License* column and choosing the link license value from the drop down menu.
8. Choose the *Configured Speed* for each selected port by clicking on the corresponding *Configured Speed* column and choosing the configured speed from the drop down menu.
9. After selecting multiple ports to be configured, click **Bulk Configuration**.
   The *Bulk Configure Ports* dialog box displays.
10. Choose the *License Speed* and *Configured Speed* for the selected ports. Click **OK**.

11. Verify that the settings that you chose as well as the pre-populated ones are correct.
12. Click **Save** on the *Create New ProbeFC* page to commit the changes and create the new hardware probe.
    The *Hardware Probes Inventory* page displays, with your newly created probe listed in the inventory list.

ProbeNAS

ProbeNAS supports 10G Ethernet ingress/egress traffic for NFSv3 protocols running over TCP/IPv4, and aggregated data-plane links formed by common Link Aggregation methods such as IEEE 802.1AX/802.3ad or Cisco EtherChannel. It does not process *Out of Order* traffic, but collects occurrence counts per flow.

ProbeNAS enables monitoring for SMBv2/3-based storage and is supported by the following entities: SMB Conversation and SMB File System.

ProbeNAS also enables monitoring traffic for iSCSI protocol and is supported by the following entity: iSCSI Conversation.

Power supply units (PSUs) in NAS and SAN probes are numbered 1 and 2, from left to right, as viewed when facing the back panel. The PSUs are hot-swappable.

Follow these steps to create a ProbeNAS.

1. From the *Settings* page, click **Performance Probe Inventory.**
   The *Performance Probe Inventory* page is displayed.
   The column headings are defined in the following table:

Table 5. Performance Probe Inventory Parameters

Column Heading	Definition
Probe Name	The name you assign to the probe
IP Address	IP address of the probe
Probe Type	Type of hardware probe, for example, ProbeNAS
Status	Status of the probe: Subscribed, Unsubscribed, or Faulted (subscribed, but not receiving data).
Version	Firmware version, for example, 5.4.2
Messages	Status information

Column Heading	Definition
Unassociated Links	Number of “unassociated links” (links that VirtualWisdom is unable to autoplace), this value is a whole number.

2. Select *ProbeNAS* from the **New** dropdown menu.
   The *Discover New Probe* page displays.
3. Enter the IP address of the probe and click **Next**.
   The *Create New Probe* page is displayed, populated with information discovered about the probe at the specified IP address. Use the scroll bar to display the full page.
   You can use the VirtualWisdom UI to change a Performance Probe’s IP address if the initial configuration (Initial IP) is already set. IP addresses can be changed if the old and new IP addresses can be routed from the appliance.
   Except for the *Subscription* status, the probe information on the page is auto-detected from the hardware probe configuration, which was entered from either the probe LCD screen or the probe Configuration Wizard.
   Descriptions of the parameters on this page are as follows:

Table 6. Create Hardware Probe Parameters

Parameter	Description
Probe Name	Specified during creation
PID	Probe ID
Probe Type	Type of probe: ProbeNAS
Version	Firmware version of the probe
Network Address	Network settings (static or DHCP) of the probe
NTP Server Address	NTP server configuration for the probe, can specify up to three
DNS	DNS server setting for the probe, typically two
MAC Address	Network port MAC address
Subscription	Subscribe or unsubscribe the probe, values are Subscribed (default) or Unsubscribed
Enable Locator LED	Enable the locator LED on the probe
TCP Window Close Threshold	Integer value in bytes at which an alert is posted, and displayed in the upper right corner of the page (default=4096)

The following are descriptions for the column headings in the *Ports* section of the page:

Table 7. Column Headings in the Ports Section

Column Heading	Definition
Port	Port Number (1-16, can be toggled ascending/descending)
Link License	Type of license: Auto Assign, None, 10G Active, 10G Passive Auto Assign chooses 10G Active licenses first, unless 10G Passive is specified.
Configured Speed	10G only
Current Speed	10G only
Filer Type	This setting only applies to NFS. OS of file server: None, VNX, Isilon, NetApp, Linux, FreeBSD, Solaris
LAG Group	Link Aggregation Group: ports in LAGs must be assigned within a set of probe-port groups.

4. Choose the *Link License* for each selected port by clicking on the corresponding *Link License* column and choosing the link license value from the drop down menu.
   Auto Assign chooses 10G Active licenses unless 10G Passive is specified, until no more Active licenses are available. If no more Active licenses are available, Passive licenses are assigned.
   Active/passive threshold: Sa port with traffic that is > 100KB/sec = active.
5. Choose the *Configured Speed* for each selected port by clicking on the corresponding *Configured Speed* column and choosing the configured speed from the drop down menu.
   Only 10G is currently supported.
6. Specify (optional) Link Aggregation Groups (LAGs).
   A port can be a member of only one LAG, and at least two ports comprise a LAG:
   - LAG 0/1, Ports 1-4
   - LAG 2/3, Ports 5-8
   - LAG 4/5, Ports 9-12
   - LAG 6/7, Ports 13-16

   If LAG assignments are changed, the probe must be rebooted.
7. Verify that the settings that you chose as well as the pre-populated ones are correct.
8. Click **Save** on the *Create New Probe* page to commit the changes and create the new hardware probe.
   The *Performance Probe Inventory* page displays, with your newly created probe listed in the inventory.

Additional Options from the New Hardware Probe Screens

The following are several additional functions available from the hardware probe screens.

Rebooting the Probe

You can reboot a probe by selecting the probe and then clicking **Reboot** on the **More** drop-down menu.

Click **OK** to confirm the reboot.

Updating the Probe

If there is a firmware update available for a probe, a message displays next to the *Version* field in both the *Hardware Probes Inventory* page and the configuration page for the probe. Probe firmware updates are delivered as a `.upd` file. This file should be installed from the *VirtualWisdom Update* screen to make the update available for the following procedure.

1. Click the new version number to upload the update to the probe.
   The screen indicates that the firmware has been uploaded and is ready to be installed.
2. Click the blue Install button to install the update.
   A *Probe update is in progress* message displays on your screen. An update can take approximately five to ten minutes.

The firmware version that is uploaded to the VirtualWisdom Appliance is viewable on the Performance Probe Inventory page, next to the License Summary button.

Downloading All Probe Logs

You can download all Performance Probe logs by selecting **Download Logs** from the **More** drop-down menu on the *Hardware Inventory* screen.

This option collects all of the logs of the hardware probes, zips them into a file, and downloads the logs to the local machine. Once the logs are downloaded you can provide them to Virtana Technical Support. Use this option to help troubleshoot issues with the hardware probes. This operation attempts to download logs for all probes that are connected to VirtualWisdom.

Downloading Individual Probe Logs

You can download individual Performance Probe logs by selecting the drop-down menu from the arrow at the end of each probe's row.

This option collects all of the logs for the selected hardware probe, zips them into a file, and downloads the logs to the local machine. Once the log is downloaded you can provide it to Virtana Technical Support. Use this option to help troubleshoot issues with a specific hardware probe that is connected to VirtualWisdom.

Hardware Diagnostics

You can view hardware diagnostic information from the *HW Diagnostics* screen. The statistics on this screen do not automatically refresh. To refresh the statistics, click the circling arrow refresh button.

You can use the information on this screen to diagnose issues with the probe, such as connectivity or dirty cables.

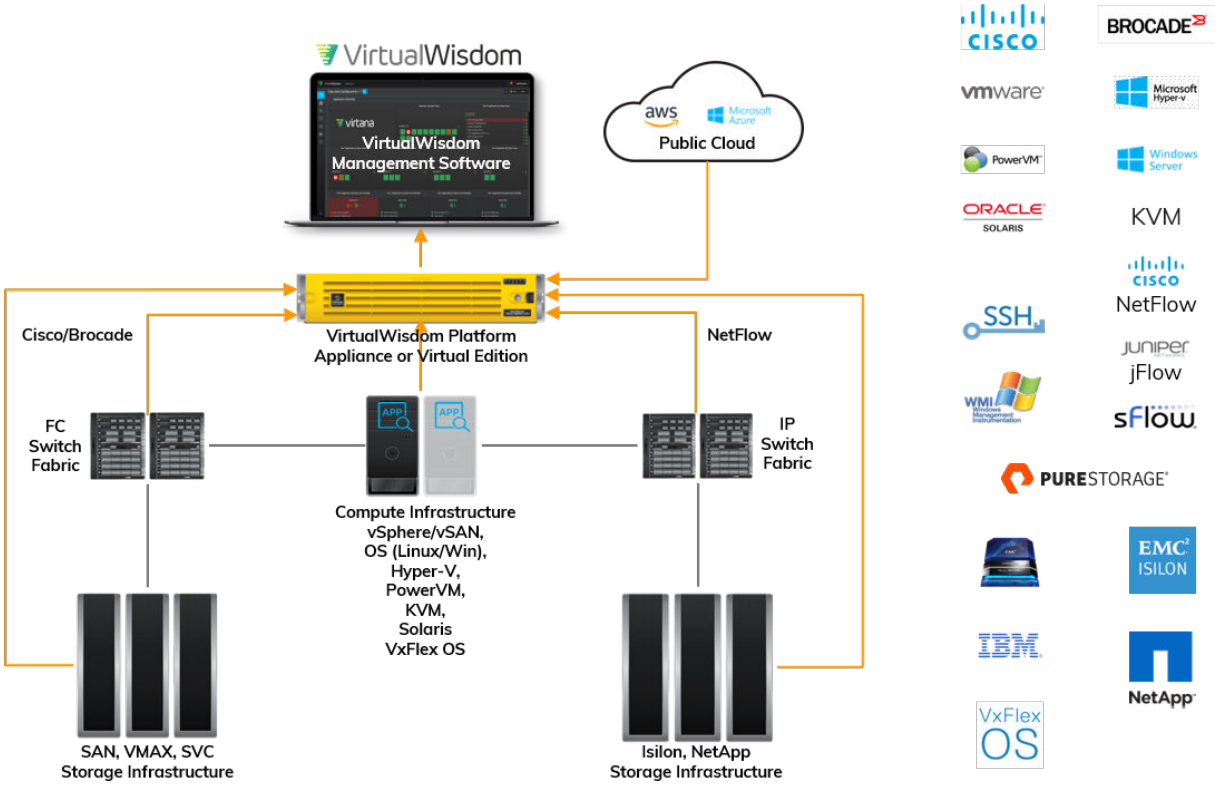
1. From the *Settings* screen, click **HW Diagnostics** in the *Probes and Integrations* group. The *HW Diagnostics* screen is displayed, including the time the page was loaded
2. Click the options menu (horizontal bars) to display two choices: *Columns* and *Export*. *Columns* displays a list of possible column headings for the *HW Diagnostics* grid. Select or deselect the columns that you want displayed in the grid. The definitions for these columns are identical to the metric descriptions. *Probe Name* and *Port* are the only required column headings.
3. Hover on *Export* to display two options: *Export Data as CSV* or *Export Data to Clipboard*.
   Data as CSV saves to a CSV file. *Data to Clipboard* saves to clipboard.
4. Click *Settings* to return to the *Settings* page.

The **Clear Diagnostics** button clears information for a selected probe. If no probe is selected, it clears the entire grid.

Integrations

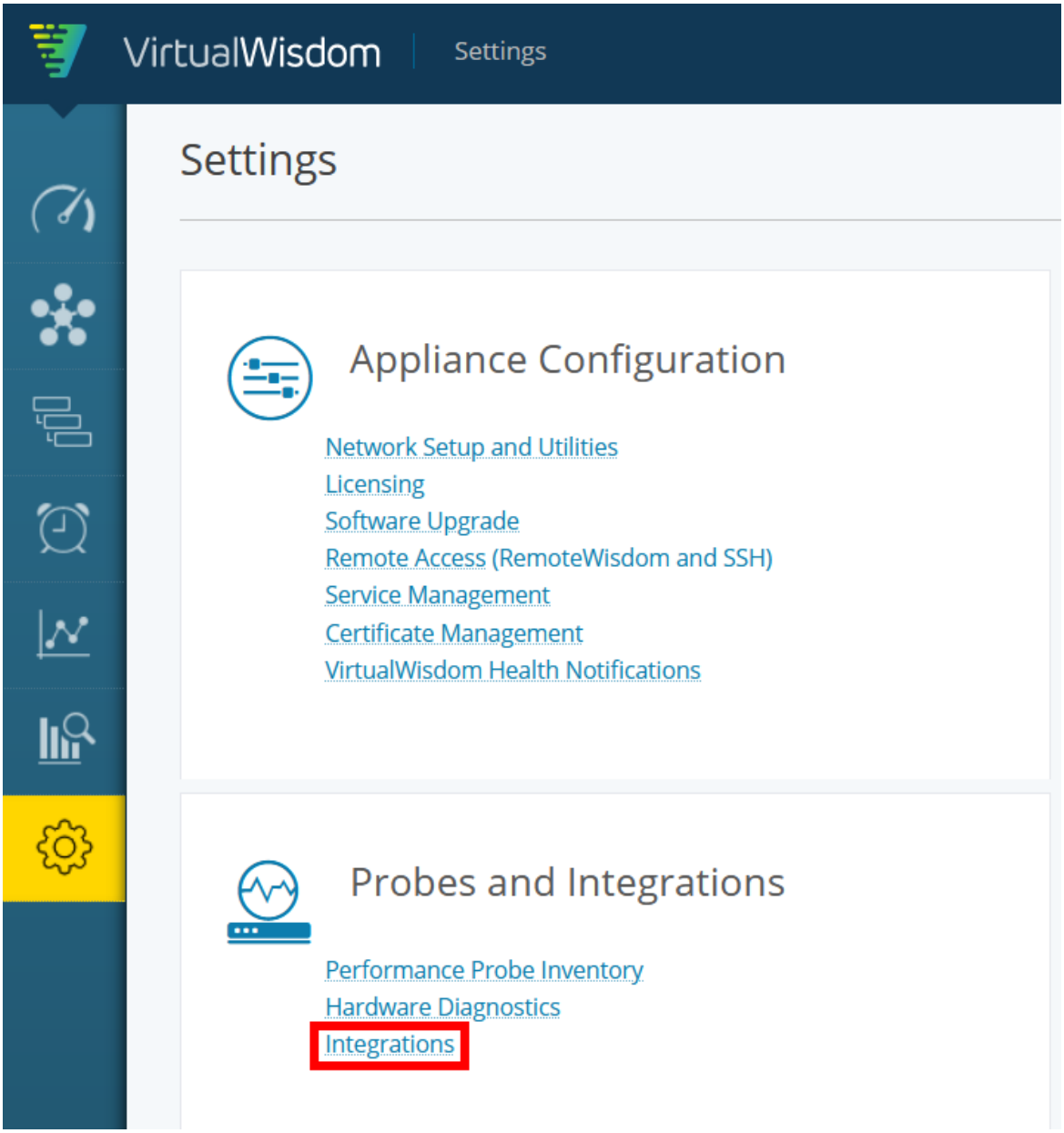
VirtualWisdom includes multiple software integrations for discovering infrastructure entities and collecting data from infrastructure and APM and CMDB sources.

Software Integrations for Network, Compute, and Storage Infrastructure Monitoring

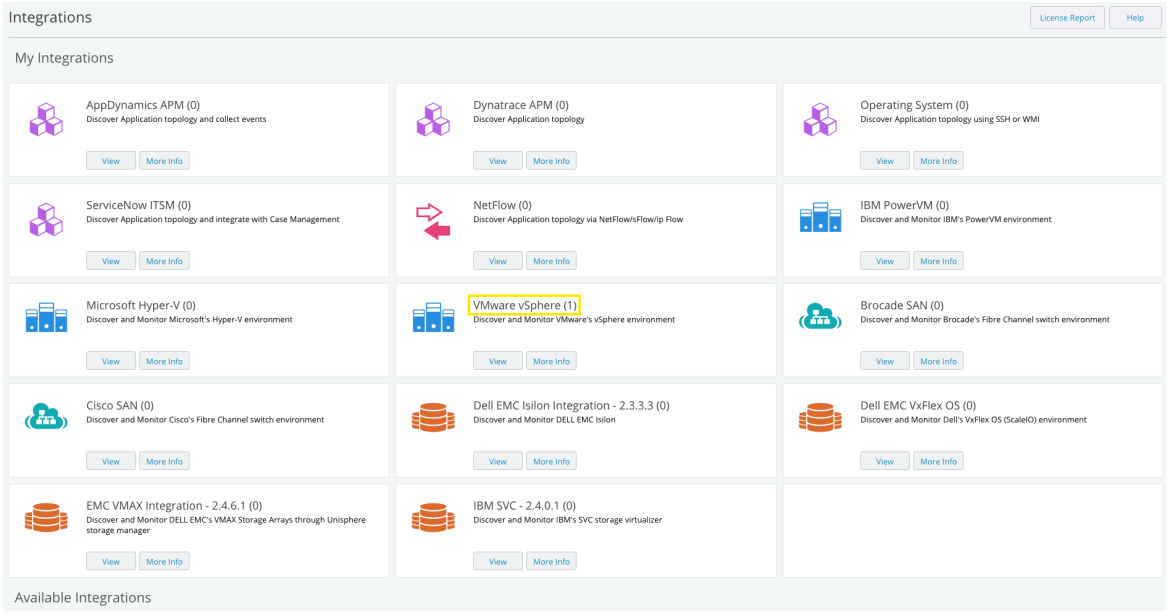


Additional integrations might be made available between releases of VirtualWisdom. Documentation for additional integrations is available on the Support portal. Access requires that you log into the portal.

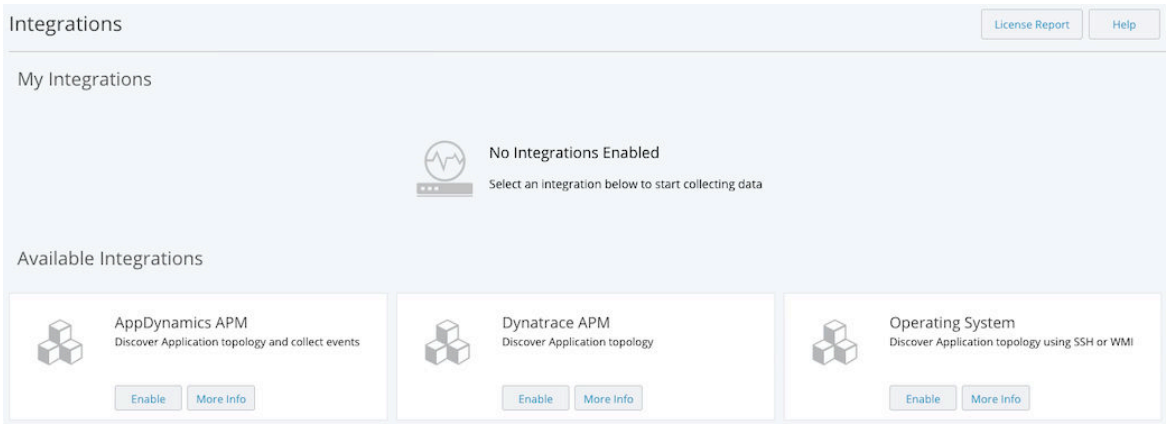
1. To view the integrations installed on your VirtualWisdom portal, navigate to the **Settings** page then select **Integrations** from the **Probes and Integrations** section.



2. A page showing all available integrations is displayed. A number indicates that the integration has been installed in your portal.

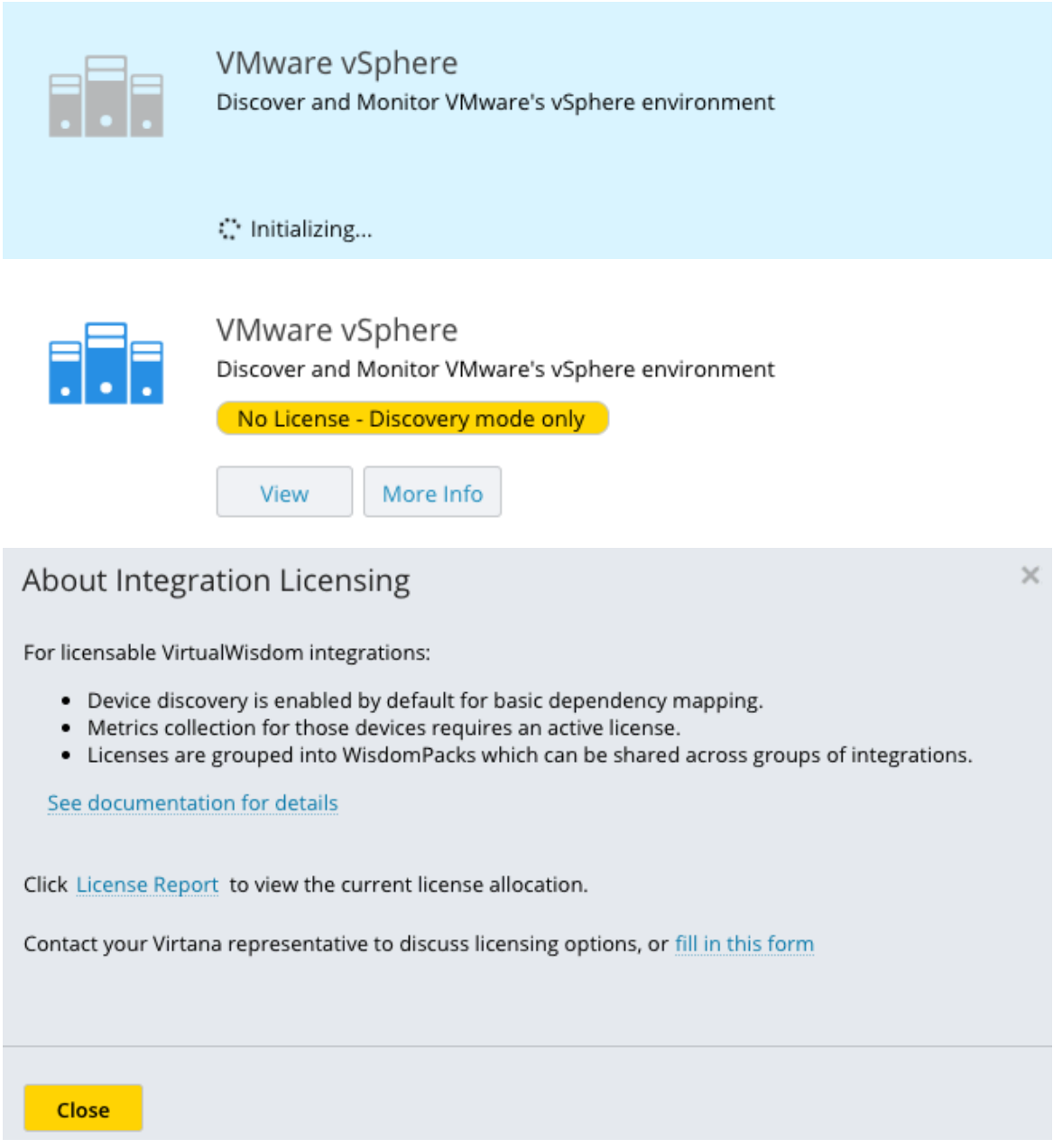


Initially, all integrations are disabled and ready to be enabled.



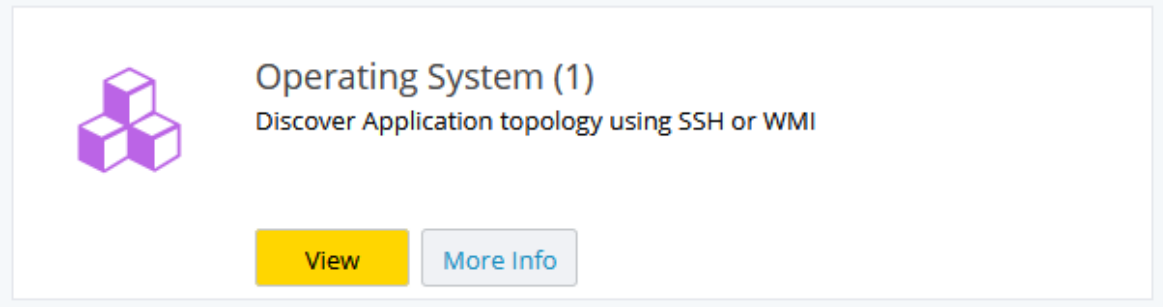
To enable an integration, click on the **Enable** button on its card. Any Services related to newly activated integrations will be started. Note: related integrations will be enabled together. For example, enabling the Brocade SAN Integration will also enable the Cisco SAN Integration because they share a common Service.

If an integration is enabled before the applicable license has been installed, the integration card will appear as shown in the following two images. Note: while an integration can be configured before it's properly licensed, only discovery may proceed, and no metrics will be collected. Also, Topology, Report Templates, Default Alarms, etc. for that integration will not be available until a license has been applied. See the third image below for the warning that appears in the UI when the **No License - Discovery mode only** button is clicked.

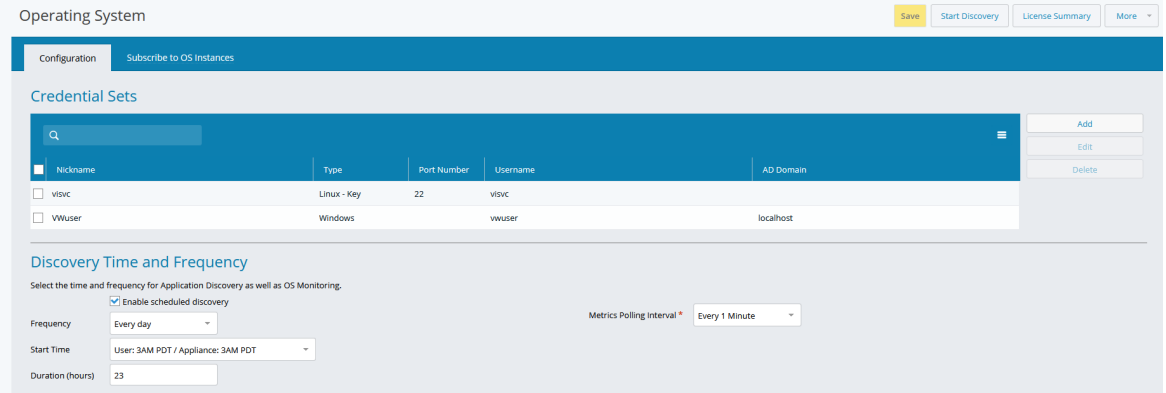


NOTE
To request additional software integrations, contact Virtana Sales.

3. Select **View** to view details about the integration.



4. The configuration page for the integration is displayed. You can use this page to view configuration information that is unique to the configuration. Each page is different based on the integration but there are some common features for managing discovery and polling intervals across all integrations.



Integration Inventory

Some integration pages display an inventory list for the integration. The fields displayed in the list view include the following:

Table 8. Integrations Inventory Fields

Column Heading	Definition
Name	User-defined name for the integration, often the IP address or the type of integration.
Subscription	Unsubscribed or Subscribed. For Brocade SAN Integration only, if subscribed, shows a ratio of the number of configured switches that are subscribed/the total number of configured switches. For example, 1/5 means that one configured switch is subscribed, out of 5 possible configured switches.

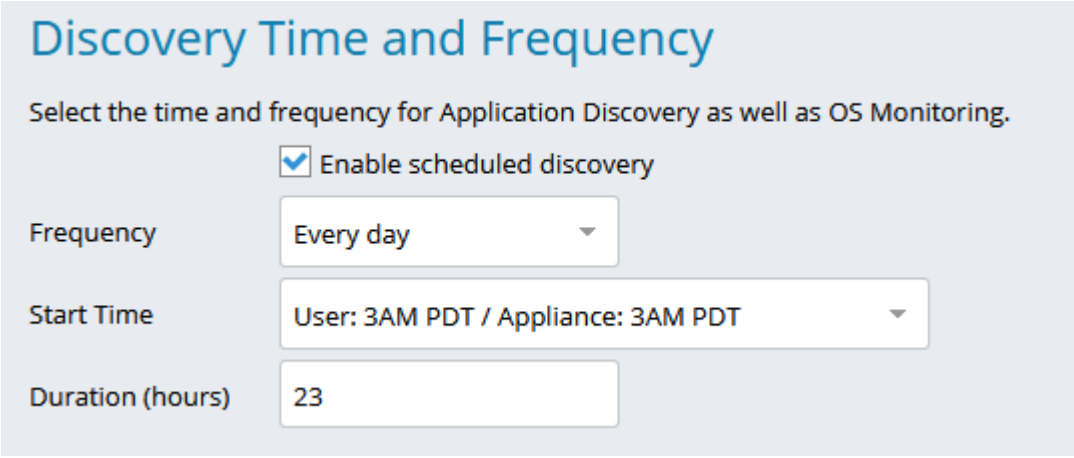
Column Heading	Definition
Last Discovery	Date and time that the integration was last discovered, discovering or currently discovering, no discovery, discovery failed, or warned. For Discovery failed or Discovery warned, you can hover over the cell to view the error or warning as a tooltip.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, Metrics collection failed for failed metrics collection, followed by a ratio of the number of failed subscribed switches to total subscribed switches, no collection for no metrics collection, or Warned followed by a timestamp and with no ratio, for a warning. For both failures and warnings, there is no mouse-over tool tip and the user has to drill down and see the failures /warnings in the switch grid. You are notified if an integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification as well as an email notification.

A down arrow is displayed at the end of each row. The arrow provides a short cut to configure, test a connection, start discovery, or delete the integration.

Managing Discovery Times and Frequencies

Most integrations include a feature to manage auto-discovery of entities. This feature is found on the Integration's configuration page in **Settings**.

You can select whether to enable scheduled discovery. If the box is checked, entity discovery will proceed automatically at the frequency selected below. You can also set a start time for the discovery.

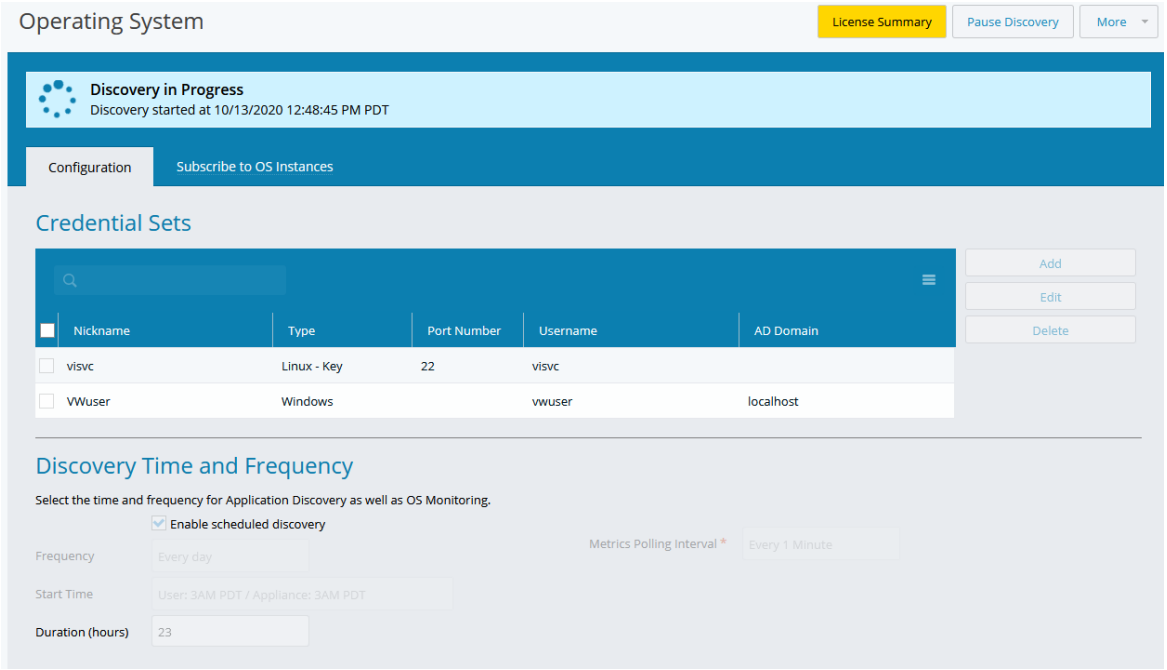


Manual Discovery

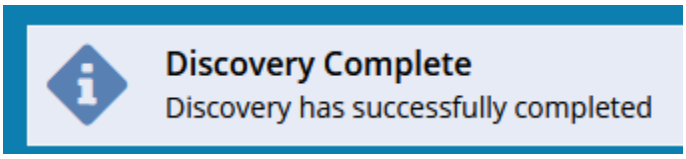
If auto-discovery is disabled, you must perform manual discovery if you wish to discover new entities that have been added to your infrastructure.

1. To perform manual discovery, select **Start Discovery** from the integration's configuration page.

2. A message is displayed on the integration's page indicating that discovery is in progress. You cannot edit the **Discovery Time and Frequency** while discovery is in progress.



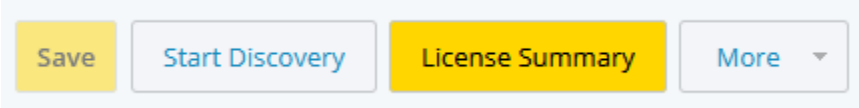
3. A subsequent message is displayed when discovery is complete.



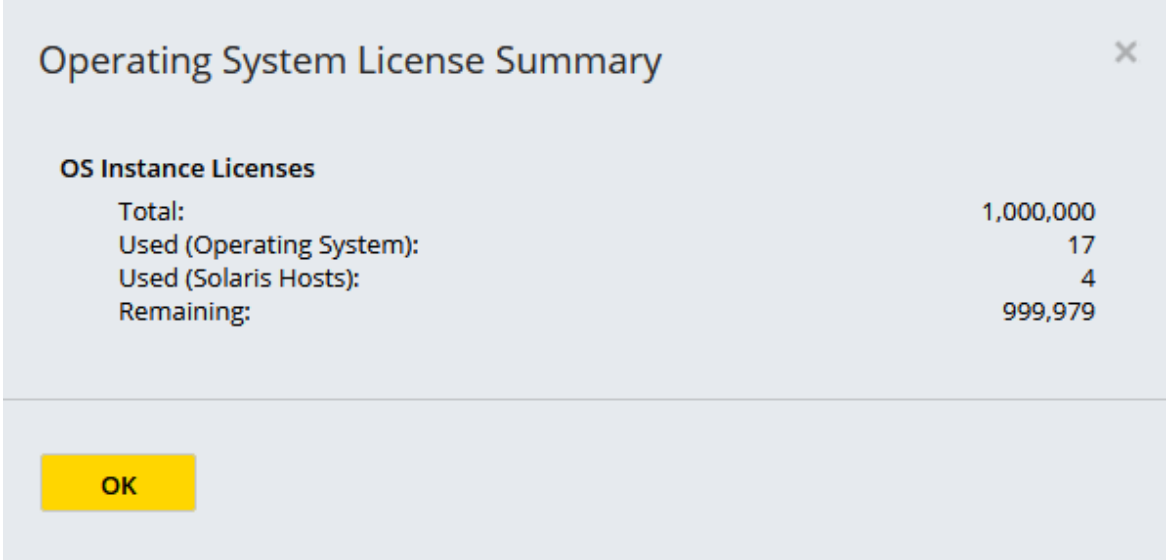
Viewing Integration Licenses

Each integration configuration page provides a link to view a summary of licensing for a specific integration.

1. Click the **License Summary** link to view the a summary of the integration license information.



2. A summary showing total, used, and remaining licenses is displayed, as in the following example.



NOTE
To request additional licenses, contact Virtana Sales.

License Reports

From the *Licensing* page and from the *Integrations* page you can access a **License Report** that shows license usage information, based on license type, such as storage controller, wiredata, OS, etc. For each license type, the report displays the total number of licenses, as well as the number of used and remaining licenses.

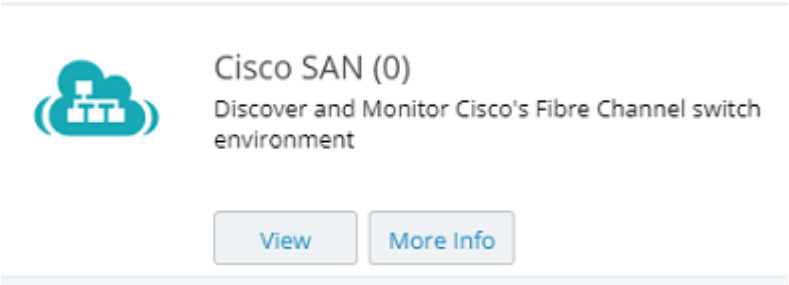
Following is a sample License Report page.

TIP

Each license type (wiredata, storage, OS, etc.), is associated with a WisdomPack License. You can view information about each WisdomPack License, such as number and types of licenses, as well as expiration dates, by accessing the Licensing page.

Cisco SAN Integration

Collect port health and utilization statistics.



The Cisco SAN Integration is an agentless software solution that utilizes storage and network information from SNMP MIB (management information base) to gather switch performance and link error statistics in a non-intrusive manner. These switch statistics are correlated with other system-wide metrics, as well as metrics from other integrations. This integration supports Cisco Fibre Channel switches and creates an unbiased view of switch port performance. VirtualWisdom utilizes the data collected to track switch performance, identify oversubscribed resources, conduct historical trending analysis, and alert administrators of link error problems or performance bottlenecks. Mini-discovery requires that scheduled discovery be enabled on at least one Cisco SAN integration.

To collect FCoE metrics from Cisco switches, configure the Cisco SAN Integration to use *SNMP Version* 2c or 3, and leave *SNMP GetBulk Operation* enabled (do **not** click the checkbox).

NOTE
Occasionally, a switch might time out while collecting FCoE metrics. If this happens, increase the polling interval to allow the switch more time to process the metrics.

Prerequisites

You can configure Cisco SAN Integration for SNMP discovery.

For HBA card-HBA port associations to be discovered, the following conditions must be met, in this order:

1. Cisco SAN Integration needs to be set up to monitor the same environment as Microsoft Hyper-V Integration, IBM PowerVM Integration, and VMware vSphere Integration.

2. Cisco SAN Integration full discovery (either scheduled or manual) must have completed prior to the Microsoft Hyper-V Integration, IBM PowerVM Integration, or VMware vSphere Integration full discovery (either scheduled or manual).

If this order is changed or these conditions are not met, HBA ports are displayed without their HBA card associations.

Configuring an integration for SNMP Discovery

> **NOTE**
> If your switches use ACLs, you must add the VirtualWisdom Platform IP address to those configurations.

> **NOTE**
> Switches that have an IPv6 address on the mgmt0 interface should not be configured for use with this integration.

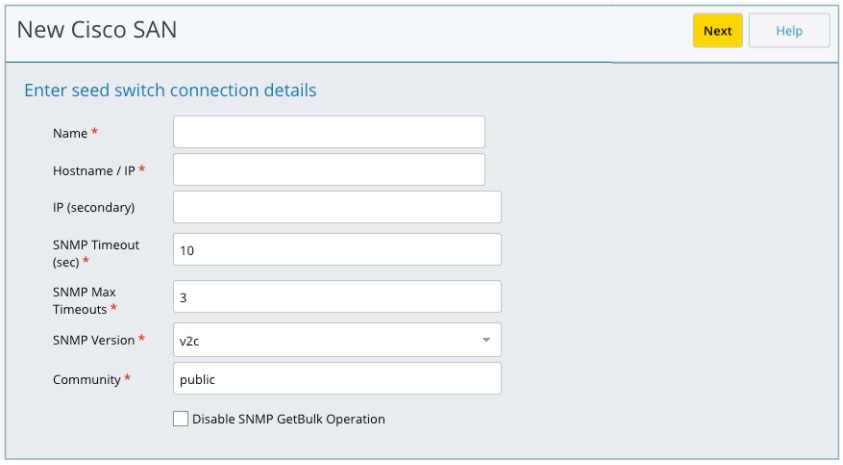
1. From the *Settings* screen, click **Integrations** in the *Probes and Integrations* section. The *Integrations* screen displays.
2. Click **View** under *Cisco SAN*.
   The *Cisco SAN* screen displays.
   The column headings in the main part of the screen are defined as follows:

Column Heading	Definition
Name	User-defined name for the integration, often the integration IP address or the type of integration. For example, Brocade_BNA_27, or seed_switch_1.
Subscription	Unsubscribed or Subscribed. For Cisco SAN Integration and Brocade SAN Integration only, if subscribed, shows a ratio of the number of configured switches that are subscribed/the total number of configured switches. For example, 1/5 means that one configured switch is subscribed, out of 5 possible configured switches.

Column Heading	Definition
Last Discovery	Date and time that the integration was last discovered, discovering for currently discovering, no discovery, Discovery failed, or Warned. For Discovery fail or discovery Warned, you can mouse over the cell shows the error or warning as a tool tip.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, Metrics collection failed for failed metrics collection, followed by a ratio of the number of failed subscribed switches to total subscribed switches, no collection for no metrics collection, or Warned followed by a timestamp and with no ratio, for a warning. For both failures and warnings, there is no mouse-over tool tip and the user has to drill down and see the failures /warnings in the switch grid. You are notified if an integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification as well as an email notification.

At the end of each row is a down arrow, which, if you click it, provides a short cut to *Configure*, *Test Connection*, *Start Discovery*, or *Delete* the integration in the associated row.

3. Click **New**.
   The *New Cisco SAN* screen displays.



4. Enter the details for a Cisco seed switch connection:

> **NOTE**
> An NPV-enabled switch cannot be used as a seed switch.

- Name for the integration discovery instance

The Name field can be edited after the configuration is saved.

- Hostname/IP as an IP address
- Optional IP (secondary) as an IP address
- SNMP Timeout (sec)
- SNMP Max Timeouts
- SNMP Version (v1, v2c, v3 Auth Privacy, v3 Auth No Privacy, v3 No Auth No Privacy)
- Community: Default is **public**
- Enable or disable the *Disable GetBulk Operation* check box

Depending on the SNMP version detected, there might be more or fewer values to enter.

5. Click **Next**.
   VirtualWisdom tests the connection to the seed switch and tries to find all of the switches accessible from that seed switch. This process can take up to five minutes. When the process completes, the *Create New Integration* screen displays.
6. The *Vendor*, *Hostname / IP*, *Secondary IP*, and *SNMP version* details are carried over from the previous screen. The *Name* field is user configurable.
   Enter the integration *Name*.
   Regularly scheduled discovery is enabled for Cisco SAN Integration and Brocade SAN Integration configurations by default. You can specify the *Frequency* and *Time of Day* of discovery. Uncheck the *Enable scheduled discovery* check box if you would like to disable regularly scheduled discovery.
   You can also enable *Mini Discovery* (disabled by default) and specify the frequency in minutes. If you disable (uncheck) scheduled discovery, Mini is also disabled.
   If mini discovery is disabled, full discovery discovers and detects changes in FCIDs for both FC Ports and Proxy FC Ports.
   If mini is enabled:
   - Full discovery does not discover FCIDs for FC Ports or Proxy FC Ports.
   - Mini discovery discovers FCIDs for FC Ports or Proxy FC Ports immediately after the first full discovery finishes, and then associates FCID with FC Port.
   - Mini discovery detects changes in FCIDs and updates existing FCIDs.
7. Optionally, click **Test Connection** to test the connection.
8. The switches in the *Switches* table on the *Create New* window are those switches that were auto-detected.
   You use the information in the *Switches* table to configure/unconfigure and subscribe/unsubscribe specific switches.The columns headings in the *Switches* table are defined as follows:

Table 9. Switches Table Fields

Fields	Definition
Switch Name	Auto-detected name of the switch.
Port Count	Active port count.
Status	Discovered, Configured, Subscribed.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, metrics collection failed, or no collection for no collection. You are notified if a software integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification alert as well as an email notification.
Metrics Polling Interval	Metrics polling interval set for the switch.
Error	Configuration or subscription errors. Mousing over an error displays a tool tip containing the error text.

At the end of each row is a down arrow, which, if you click it, provides a short cut to *Configure*, or *Unconfigure* the integration in the associated row.

> **NOTE**
> The seed switch cannot be unconfigured.

9. Select the switch or switches that you want to configure by selecting the check box associated with the switch or switches.
10. Click **Configure**, or, if you only chose one switch, you can also choose the Configure option from the drop-down menu at the end of the selected row.
    If you selected one switch, the *Switch Configuration* dialog box displays. Proceed to Step 11.
    If you selected more than one switch, the *Bulk Switch Configuration* dialog box displays. Proceed to Step 12..
11. If you select one switch, the *Switch Configuration* dialog box displays.
    The *Name*, *Vendor*, *Hostname/IP*, and *SNMPVersion* are auto-detected. You can override the *IP* and *SNMP Version*. If auto-detect for the IP address failed, you must enter the IP address. Depending on the SNMP version detected, there might be more or less values to fill in.
    The values in the other fields are filled out with default values. You can edit these fields, but it is recommended that you keep the default values provided. In some

cases, such as when SNMP version 3 usernames and passwords are required, we cannot provide defaults, and you have to enter the information manually.

> **NOTE**
> SNMP Timeout multiplied by SNMP Max Timeouts cannot exceed half of the Polling Interval.

> **NOTE**
> For Core switches discovery times out, workaround is to increase the timeout value to 45 seconds and the metrics polling interval need to be set to 5 minutes, click OK and re-run the discovery.

Click **OK** to apply the configuration. Proceed to Step 13.

12. If you select two or more switches, the *Bulk Switch Configuration* dialog displays. Select the properties that you want to configure and click **OK**.
    A Switch Configuration dialog displays, with the selected properties ready to be configured. Enter the values for the selected properties and click **OK** to apply the configuration.
13. Subscribe to the switches by selecting the switch or switches to which you would like to subscribe and click **Subscribe**. When you click **Subscribe**, VirtualWisdom also validates that there are sufficient licenses.
14. Click **Save** to save all of your changes.
    The *Discovery* dialog box displays, asking if you want the discovery process to start upon saving. Immediate discovery is recommended, as no metrics are collected until discovery is complete.
15. Click **Yes** to start immediate discovery.
    After clicking yes, you get returned to the main grid of all software integration configurations, and the integration that you just created has "Discovering..." in its last discovery time column.
    If you drill down into the integration configuration again, a banner displays on your screen saying that discovery is taking place. While the discovery is taking place you are in read-only mode. You cannot make any changes to the integration or switch configuration.

NOTE

If discovery completes with the error, “Illegal action: attempt to associate archived parent,” re-run discovery on the integration configuration that failed for it to unarchive the port.

Cisco SAN Integration Alias and Zone-Based Topology Matrix

Aliases are automatically imported during Cisco SAN Integration discovery if you are using any of the following supported combinations.

Vendor	Alias Type	Alias By	Zoned By	VirtualWisdom Naming*	VirtualWisdom Topology**
Cisco	fcalias	wwpn	alias	yes	yes
Cisco	fcalias	wwpn	wwpn	yes	yes
Cisco	fcalias	fcid	fcalias, fcid	yes	yes
Cisco	device-alias	wwpn	device-alias	yes	yes
Cisco	device-alias	wwpn	wwpn	yes	yes
Cisco	fcalias, device-alias	interface	interface	no	no

* Retrieves alias definitions from the switches that are used for WWN-to-name resolution

** Retrieves zone information that is used to define the intelligent topology within VirtualWisdom

Cisco SAN Telemetry Streaming

The following are supported with SAN Telemetry Streaming: DS 9700 32G, DS-X9648-1536K9 Module and MDS 9132T Switch.

The Cisco switch supports monitoring SAN Telemetry Source (STS) storage data from licensed ports of target edge switches. ProbeFC supports approximately 500 metrics. The Cisco switch currently has 72 metrics available. These metrics are sent to the VirtualWisdom appliance using the gRPC protocol, and are available per Initiator-Target-LUN and port. With Compact-GPB encoding on NX-OS 8.3(2), Cisco limits 20K ITLs per

9100 switch and 40K ITLs per 9700 switch, and a minimum STS streaming interval of 30 seconds. VirtualWisdom 6.x supports 200K ITLs from multiple Cisco switches.

Cisco MDS NX-OS Release 8.3(2) supports Google Protocol Buffers (GPB) and GPB compact encoding over gRPC transport. Ensure you follow the appropriate steps below if using Cisco NX-OS Release 8.3(2). Virtana and Cisco recommend using GPB-compact encoding with VirtualWisdom 6.0.1 and NX-OS 8.3(2).

To collect STS data from the MDS 9700 switch you need SAN_ANALYTICS_PKG or SAN_TELEMETRY_PKG, and for MDS9132T switch you need SAN_TELEMETRY_PKG.

Perform the following steps to configure analytics and telemetry on the switch:

1. Ensure all Cisco switches that will configured for telemetry streaming are NTP synced to the same source(s) as VirtualWisdom.
2. Enable analytics and telemetry globally:
   `feature analyticsfeature telemetry`
3. Enable the interfaces to collect data:
   `interface fc<x/y>analytics type fc-scsi`

   NOTE
   To improve performance, enable analytics only on the ports which need to be monitored. VirtualWisdom supports analytics on the storage edge switch port.

4. Configure a push query:
   `analytics query "select all from fc-scsi.scsi_target_itl_flow" name virtana_query type periodic clear differential`
   `clear` clears all the min, max, and peak metrcis after every query (streaming) interval. By default, `min/max/peak` values are sticky.
   `differential` streams only ITL records that have changing data. By default, every ITL record is streamed all the time.
   `periodic` is the streaming interval. The default streaming interval is 30 seconds.
   `scsi_target_itl_flow` should be used for the target edge switch port.
5. Choose one of the following to configure streaming for the query.
   - Configure streaming for VirtualWisdom 6.0 and Cisco NX-OS 8.3(1):
     MDS9706# configure terminal
     MDS9706(config)# telemetry
     MDS9706(config-telemetry)# sensor-group 100
     MDS9706(conf-tm-sensor)# path analytics:virtana_query
     MDS9706(conf-tm-sensor)# destination-group 100

MDS9706(conf-tm-dest)# ip address 10.10.60.97 port 5888 protocol gRPC encoding GPB <-Receiver VW IP address and port
MDS9706(conf-tm-dest)# subscription 100
MDS9706(conf-tm-sub)# snsr-grp 100 sample-interval 30000
MDS9706(conf-tm-sub)# dst-grp 100

NOTE
Use the following to remove the VirtualWisdom IP address as a gRPC receiver:

MDS9706# configure terminal
MDS9706(config)# telemetry
MDS9706(config-telemetry)# destination-group 100
MDS9706(conf-tm-dest)# no ip address 10.10.60.97 port 5888 protocol gRPC encoding GPB <-Receiver VW IP address and port

NOTE
The default server port on the VirtualWisdom appliance to receive STS metrics is 5888. If port 5888 is unavailable, use port 5889 or 5890 to receive the STS metrics from the switch.

Follow these steps to change the port on the switch from 5888 to 5889:
MDS9706# configure terminal
MDS9706(config)# telemetry
MDS9706(config-telemetry)# destination-group 100
MDS9706(conf-tm-dest)# no ip address 10.10.60.97 port 5888 protocol gRPC encoding GPB
MDS9706(conf-tm-dest)# ip address 10.10.60.97 port 5889 protocol gRPC encoding GPB
MDS9706(conf-tm-dest)# copy running-config startup-config
After changing the port on the switch, a property change is required on VirtualWisdom Appliance. Contact Virtana Support.

- Configure compact GPB streaming with VirtualWisdom 6.0.1 and Cisco NX-OS 8.3(2):

NOTE

- With Cisco MDS NX-OS 8.3(2), Cisco switch supports Google Protocol Buffers (GPB) and GPB compact encoding over gRPC transport. Ensure that all destinations under a destination group, and all destination groups under a subscription, are using the same encoding type.
- Virtana and Cisco recommend using compact-GPB encoding with VirtualWisdom 6.0.1 and NX-OS 8.3(2).
- Use numbers from <1-4095> for sensor-group, destination-group, subscription, snsr-grp and dst-grp
- Refer to *Configuring SAN Telemetry Streaming* in the Cisco MDS 9000 Series SAN Analytics and SAN Telemetry Streaming Configuration Guide, Release 8.x for more information.

```
MDS9706# configure terminal
MDS9706(config)# telemetry
MDS9706(config-telemetry)# sensor-group 200
MDS9706(conf-tm-sensor)# path analytics:virtana_query
MDS9706(conf-tm-sensor)# destination-group 200
MDS9706(conf-tm-dest)# ip address 10.10.60.99 port 5888 protocol gRPC
encoding GPB-compact
MDS9706(conf-tm-dest)# subscription 200
MDS9706(conf-tm-sub)# snsr-grp 200 sample-interval 30000
MDS9706(conf-tm-sub)# dst-grp 200
MDS9706(conf-tm-sub)# copy running-config startup-config
```

6. Choose one of the following to verify configured streaming.
   - Verify the configured streaming at Cisco NX-OS 8.3(1):

     ```
     MDS9706# show running-config telemetry all
     feature telemetry
     telemetry
     sensor-group 100
     path analytics:virtana_query <-- analytics query name (step-3)
     destination-group 100
     ip address 10.10.60.97 port 5888 protocol gRPC encoding GPB
     subscription 100
     snsr-grp 100 sample-interval 30000 <-Streaming sample-interval 30000 is in
     milliseconds
     dst-grp 100
     ```

   - Verify the configured streaming at Cisco NX-OS 8.3(2).

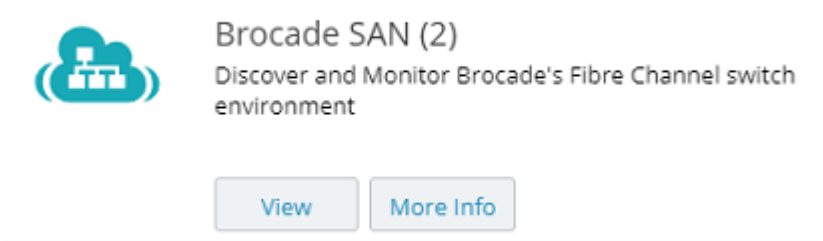
```
MDS9706# show running-config telemetry all
feature telemetry
telemetry
sensor-group 200
path analytics:virtana_query
destination-group 200
ip address 10.10.60.99 port 5888 protocol gRPC encoding GPB-compact
subscription 200
snsr-grp 200 sample-interval 30000
dst-grp 200
```

7. In the Discovered Telemetry Sources tab, subscribe to the ports to collect STS metrics. To collect Cisco STS data, the Cisco edge switches (host/storage) must first be configured and discovered successfully. A configured and successfully discovered Cisco switch and its STS capable ports appear in the Discovered Telemetry Sources tab in Cisco SAN Integration. It contains information about Ports, Storage Port Name, License, and Last Observed Time. Reports and charts can be created with STS metrics by navigating to Storage > Fibre Channel > Cisco STS.
8. Verify the telemetry transport.

```
MDS9706# show telemetry transport
Session Id IP Address Port Encoding Transport Status
--------------------------------------------------------------------------------
1 10.10.60.99 5888 GPB-compact gRPC Connected
--------------------------------------------------------------------------------
Retry buffer Size: 10485760
Event Retry Messages (Bytes): 0
Timer Retry Messages (Bytes): 10399055
Total Retries sent: 179
Total Retries Dropped: 1341
```

Brocade SAN Integration

Collect SAN metrics using Brocade SAN SMI-S and SNMP-SSH.



The Brocade SAN integration is an agentless software solution that utilizes storage and network information from information from Storage Management Initiative Specification (SMI-S) and SNMP MIB (management information base) to gather switch performance and link error statistics in a non-intrusive manner. These switch statistics are correlated with other system-wide metrics, as well as metrics from other integrations. This integration supports Brocade Fibre Channel switches, creating an unbiased view of switch port performance. VirtualWisdom utilizes this data to track switch performance, identify oversubscribed resources, conduct historical trending analysis, and alert administrators of link error problems or performance bottlenecks.

NOTE

Access Gateway switch ports that are connected to the core switch are missing the WWNs.

Configuring a Brocade SAN Integration for BNA SMI-S Discovery

Prerequisites

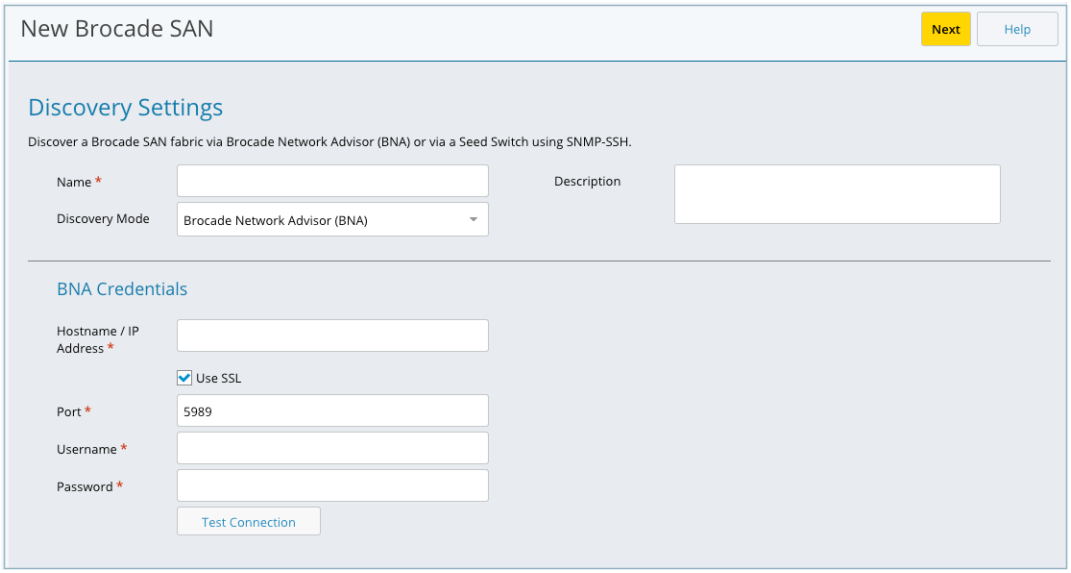
Before configuring an instance of a Brocade SAN Integration where BNA (SMI-S) discovery will be used, it is recommended that the heap size be adjusted from the default 1GB to one of the settings indicated in the table below. Open the file $INSTALLDIR/conf/cimomsvc.conf, locate the line that contains set.MAX_HEAP_SIZE and change it to set.MAX_HEAP_SIZE=N, where N equals the heap setting shown below, which is based on the number of Brocade SAN Integration ports to be configured.

# of Brocade SAN Ports to be Configured	BNA Heap Setting
1 - 1,000	1GB
1,002-2,560	2GB
> 2,560	4GB

Before configuring an instance of a Brocade SAN Integration where BNA (SMI-S) discovery will be used, make sure that BNA has completed its discovery.

If you are using Brocade Network Advisor (BNA) network management tool for discovery, you need to configure SMI-S.

1. From the *Settings* screen, click **Integrations** in the *Probes and Integrations* section.
   The *Integrations* screen is displayed.
2. Click **View** for the integration.
   The *Brocade SAN* screen is displayed.
3. Click **New**.
   The *New Brocade SAN* screen is displayed.
4. Enter a name for the integration discovery instance.
   A name is required. The Name field can be edited after the configuration is saved.
5. Select the **Brocade Network Advisor (BNA)** Discovery Mode.



6. Complete the rest of the information on the *New Brocade SAN* screen as follows:

Field	Definition
Hostname / IP Address	Hostname or IP address of the SMI-S provider.
Use SSL	Enables or disables use of SSL for login.
Port	Port of the SMI-S provider. If the SSL check box is selected, the port is 5989. If the SSL check box is not selected, it is port 5988.
Username	Username of the SMI-S provider, for example, the username for the Brocade BNA.
Password	Password of the SMI-S provider, for example, the password for the Brocade BNA.

7. Click **Test Connection** to verify the connection.

VirtualWisdom tests the connection (hostname and credentials) and tries to find all the switches. This process can take up to five minutes.

8. Click **Next**.
   Discovery begins for all the switches accessible. This process can take several minutes, depending on the number of switches to be discovered.
   The *New Integration* page opens to display the *Configuration* tab.
   The *Namespace* field is auto-detected.The *Vendor*,*Hostname/IP*, *Port*, *Username*,*Password*, and *Use SSL* fields are carried over from the previous screen.
   The *Name* field is user-configurable.
9. Enable or disable scheduled discovery.
   By default, regularly scheduled discovery is enabled for Brocade SAN Integration configurations. If you would like to disable regularly scheduled discovery, uncheck the *Enable scheduled discovery* check box. If you would like to have discovery scheduled regularly, keep the box checked and choose a discovery frequency and time of day. By default, the frequency and time of day for Brocade SAN Integration is every other day and 2am appliance time.
10. Click **Save**.
11. Click on the **SNMP Sources** tab on the New Integration page.
    A list of available auto-detected SNMP switch sources displays.
12. Select the switches you want to use with the integration and click **Add**.
    You can configure multiple switches at one time. The columns headings in the *Switches* table are defined as follows:

Table 10. Switches Table Fields

Fields	Definition
Switch Name	Auto-detected name of the switch.
Port Count	Active port count.
Status	Discovered, Configured, Subscribed.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, metrics collection failed, or no collection for no collection. You are notified if an Integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification as well as an email notification.
Metrics Polling Interval	Metrics polling interval set for the switch.
Error	Configuration or subscription errors. Mousing over an error displays a tooltip containing the error text.

13. With the switches still selected, click **Configure**.
    If you selected one switch, the *Switch Configuration* dialog box displays. Proceed to Step 14.
    If you selected more than one switch, the *Bulk Switch Configuration* dialog box displays. Proceed to Step15.
14. If you select one switch, enter the values in the *Switch Configuration* dialog.
    The *Name*, *Vendor*, *IP*, *SNMPVersion* are auto-detected. You can override the *IP* and *SNMP Version*. If auto-detect for the IP address failed, you must enter the IP address. Depending on the SNMP version detected, there might be more or less values to fill in. The values in the other fields are filled out with default values. You can edit these fields, but it is recommended that you keep the default values provided. In some cases, such as when SNMP version 3 usernames and passwords are required, we cannot provide defaults, and you have to enter the information manually.
    Proceed to Step16.
15. If you select two or more switches, select the properties to configure in the *Bulk Switch Configuration* dialog.
16. Click OK.
17. With the switches still selected, click **Subscribe**.
    When you click **Subscribe**, VirtualWisdom validates that there are sufficient licenses.
18. Click **Save** to save all of your changes.
    The *Discovery* dialog box displays, asking if you want the discovery process to start upon saving. Immediate discovery is recommended, as no metrics are collected until discovery is complete.
19. Click **Yes** to start immediate discovery.
    After clicking yes, you are returned to the main grid of all configurations, and the integration that you just created has "Discovering..." in its last discovery time column.
    If you drill down into the configuration again, a banner displays on your screen saying that discovery is taking place. While the discovery is taking place you are in read-only mode. You cannot make any changes to the integration or switch configuration.

> **NOTE**
> If discovery completes with the error, “Illegal action: attempt to associate archived parent,” re-run discovery on the integration configuration that failed for it to unarchive the port.

Configuring a Brocade SAN Integration for SNMP-SSH Discovery

When configuring Brocade SAN for SNMP over SSH, you configure a “seed switch”. From that switch, other interconnected switches on the network can be discovered, so you do not have to add and configure each switch individually.

Prerequisites

Because Brocade zoning information is not available through SNMP, VirtualWisdom discovers it via SSH by running the FOS commands shown below. VirtualWisdom also discovers virtual fabrics using SSH. This is required to discover switches in other virtual fabrics. VirtualWisdom requires a user with the chassis role of "user" and read-only access to the switches to run these commands.

FOS Command	Purpose
lscfg -show	Discover virtual fabric ID; used to discover switches in other fabrics
fabricshow -chassis	Discover chassis WWN and name
zoneshow	Discover zone, zone set and zone aliases
fcrproxydevshow -a lsanzoneshow -s	Discover proxy FC ports (routed fabrics)

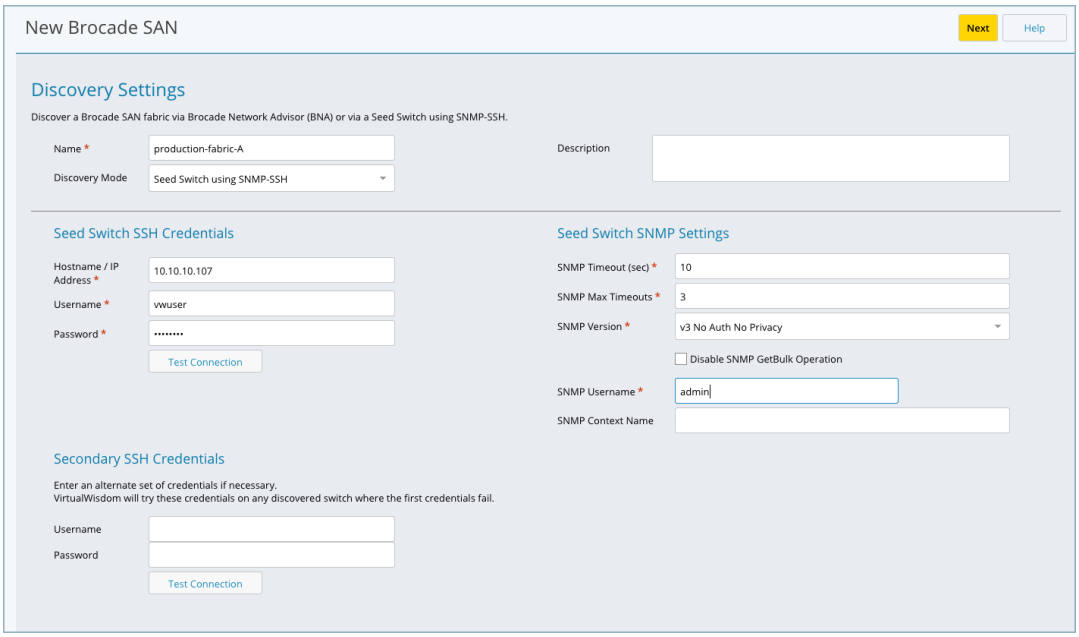
NOTE
An NPV-enabled switch cannot be used as a seed switch. Also, a Brocade Access Gateway cannot be used as a seed switch.

NOTE
VirtualWisdom assumes the fabric will have the same SSH credentials as the seed switch. If the credentials are not the same as the seed switch, the switches will not be discovered. To add switches with different credentials, there is an option to manually add switches. Refer to the Adding Switches to the SNMP Sources List [70] section for more information.

1. From the *Settings* screen, click **Integrations** in the *Probes and Integrations* section. The *Licensed Integrations* screen is displayed.
2. Click **View** for *Brocade SAN*. The *Brocade SAN* screen is displayed.
3. Click **New**.

The *New Brocade SAN* screen displays, with some default settings.

4. Enter a name for the integration discovery instance.
   A name is required. The Name field can be edited after the configuration is saved.
5. In the Discovery Settings section of the window, select **Seed Switch using SNMP-SSH** from the *Discovery Mode* drop-down menu.
   You can provide an optional *Description*.



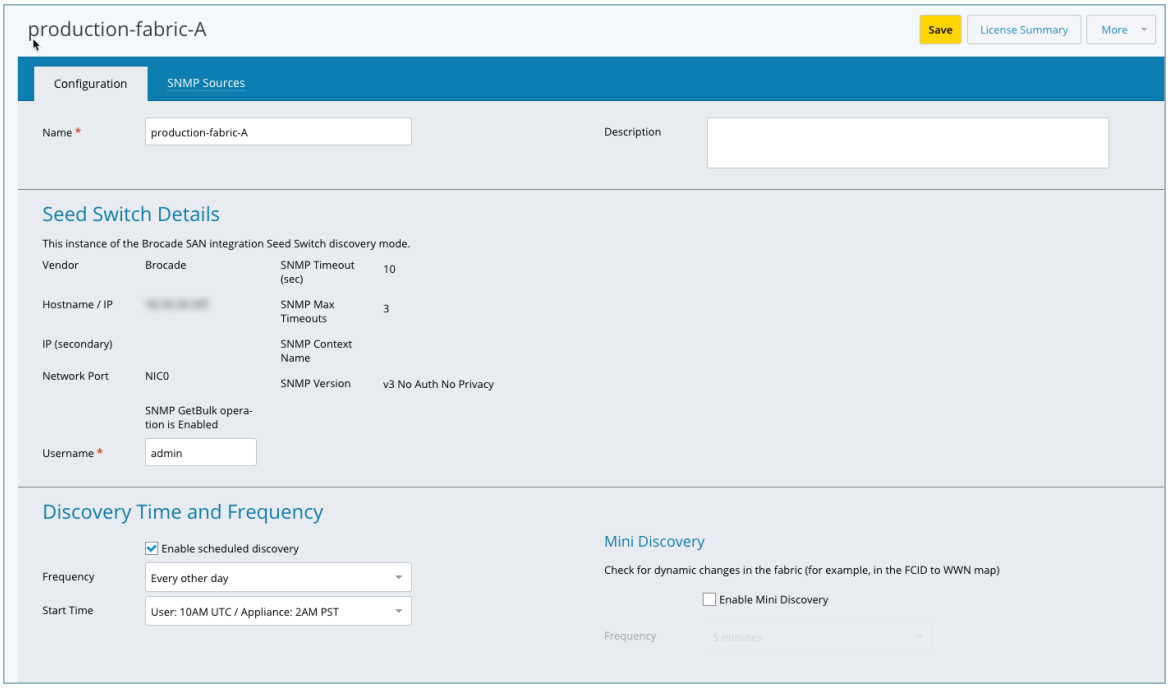
6. Enter the **Seed Switch SSH Credentials**.

Field	Definition
Hostname / IP Address	Hostname or IP address of the switch.
Username	Username of the switch.
Password	Password of the switch.

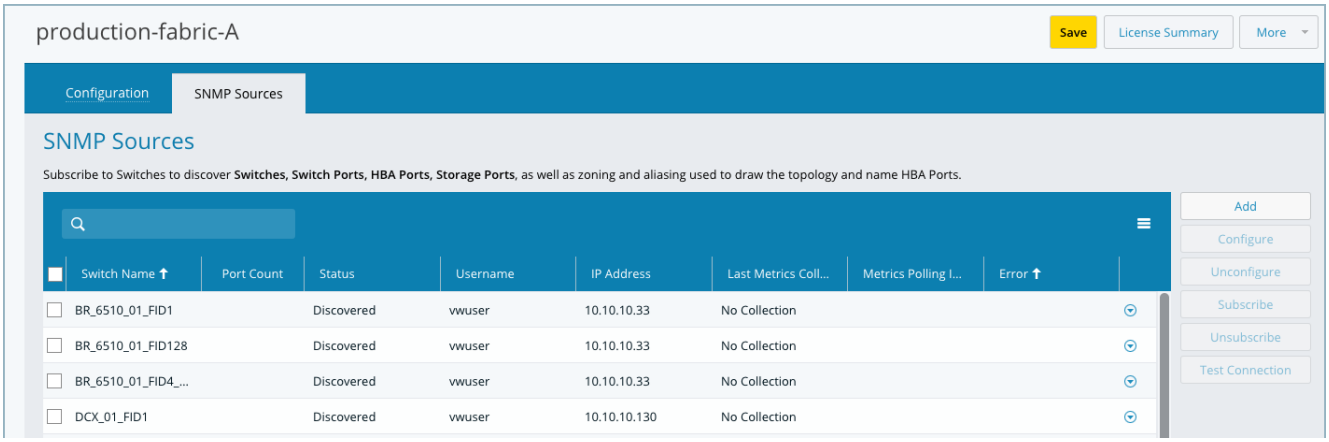
7. Click **Test Connection** to verify that the switch is accessible with provided credentials.
8. Optional: Enter Secondary SSH Credentials and test the connection.
9. Verify or modify the Seed Switch SNMP Settings.

Field	Definition	Comments
SNMP Timeout (sec)	The timeout in seconds between retries 10 is default Accepts an integer from 1 to 1,000	SNMP Timeout multiplied by SNMP Max Timeouts cannot exceed half of the Polling Interval.
SNMP Max Timeouts	Maximum number of retries 3 is default	
SNMP Version	v1 v2c (default) v3 (Auth Privacy, Auth No Privacy, or No Auth No Privacy options)	
Community	Default is *public*	Only applies to v1 and v2c
SNMP Username		Required for all SNMPv3
SNMP Context Name		Optional for all SNMPv3
SNMP Auth Password		Optional for v3 Auth Privacy or No Privacy
SNMP Auth Protocol		Optional for v3 Auth Privacy or No Privacy
SNMP Privacy Password		Optional for v3 Auth Privacy
SNMP Privacy Protocol		Optional for v3 Auth Privacy

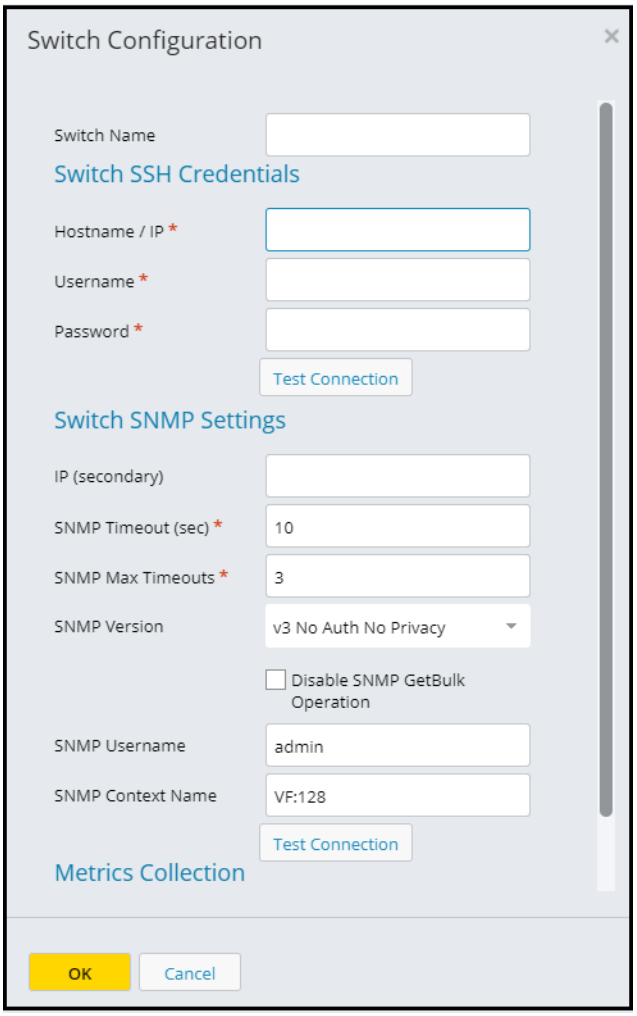
10. Enable or disable the SNMP GetBulk operation.
    This feature is available only for SNMP versions v2c and v3.
    GetBulk is enabled by default, and keeping this option enabled is recommended.
11. Click **Next**.
    Discovery begins for all the switches accessible to the seed switch. This process can take several minutes, depending on the number of switches to be discovered.
    The *New Integration* page opens to display the *Configuration* tab.



12. Enable or disable **Discovery Time and Frequency**.
    By default, regularly scheduled discovery is enabled for integration configurations. If you would like to disable regularly scheduled discovery, uncheck the *Enable scheduled discovery* check box.
    If you would like to have discovery scheduled regularly, keep the box checked and choose a discovery frequency and time of day. By default, the frequency and time of day is every other day and 2am appliance time.
13. Enable or disable **Mini Discovery**.
    This setting is disabled by default.
    Mini Discovery checks for dynamic changes in your fabric.
    If you enable Mini Discovery, you must select a frequency.
14. Click on the **SNMP Sources** tab on the New Integration page.
    Switches that are connected to the seed switch are discovered and listed in the SNMP Sources table.



15. Select the switches you want to use, and then click **Configure**.
    You can configure multiple switches at one time.
    If you selected one switch, the *Switch Configuration* dialog box displays. Proceed to Step 16.
    If you selected more than one switch, the *Bulk Switch Configuration* dialog box displays. Proceed to Step 17.
16. If you select one switch, enter the values in the *Switch Configuration* dialog.



SSH credentials are pre-populated and the Password is encrypted.

Verify the Switch SNMP settings for the switch you intend to configure, and fill in the appropriate details.

When selecting the SNMPv3 provide the SNMP Username.

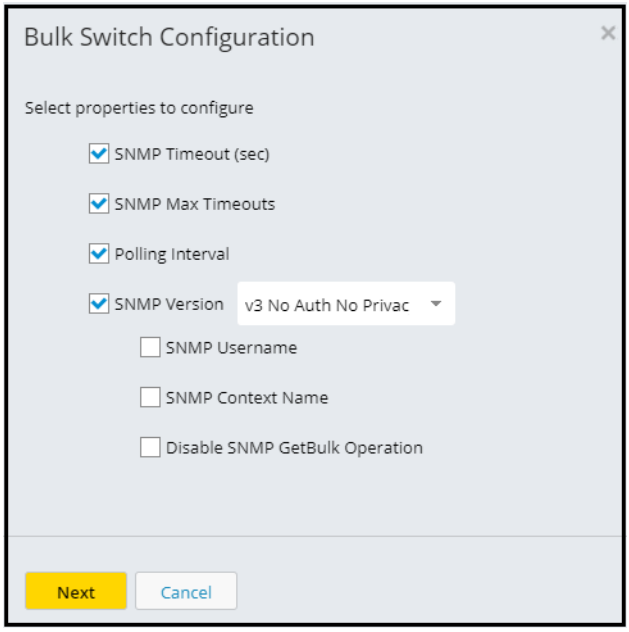
When a single switch is being configured and discovered with a logical fabric, then the SNMP Context Name must be set appropriately. This only configures and discovers the switch with the specified Context Name.

Example: Brocade switch has FID-1 needs to be configured with SNMP Context Name as 'VF:1'.

When multiple switches are being configured and discovered, keeping the SNMP Context Name field blank is recommended, so all switches are discovered.

Proceed to Step 18.

17. If you select two or more switches, select the properties to configure in the *Bulk Switch Configuration* dialog and click Next.



A configuration dialog box displays with configurable fields.

Select the appropriate SNMP version.

- When selecting the SNMPv3, provide the SNMP Username and the SNMP Context Name (optional).
- With SNMP v1, the default username is *public*.

18. Confirm or modify the configuration settings and click OK.
    The status of the switches changes to Configured in the SNMP Sources table.
19. Select the switches for which you want metrics and click **Subscribe**.
    Subscribing to the switches starts the polling for metrics.
    Integration licenses must be available to subscribe.
20. Click **Save** to save all of your changes.
    The Start Discovery dialog box displays so you can initiate a discovery of the integration. VI recommend starting a discovery. Completing the discovery successfully creates the entities.
21. Click **Yes** to start a full discovery.
    After clicking yes, you are returned to the *Brocade SAN* page that lists all configurations, and the integration that you just created has "Discovering..." in its Last Discovery column.
    If you drill down into the configuration again, a banner displays on your screen saying that discovery is taking place. While the discovery is taking place you are in read-only mode. You cannot make any changes to the integration or switch configuration. A message similar to the following displays:
    First-time discovery started at <date> <time>. This could take several hours to complete.

> **NOTE**
> If discovery completes with the error, “Illegal action: attempt to associate archived parent,” re-run discovery on the integration configuration that failed for it to unarchive the port.

22. Check the SNMP Sources list to verify that all switches you want to subscribe are listed and have the status Subscribed.
    If a switch you want does not appear in the table, see Adding Switches to the SNMP Sources List [0].

Brocade SAN Integration Alias and Zone-Based Topology Matrix

Aliases are automatically imported during Brocade SAN Integration discovery if you are using any of the following supported combinations.

Table 11.

Vendor	Alias Type	Alias By	Zoned By	VirtualWisdom Naming*	VirtualWisdom Topology**
Brocade	alias	wwpn	alias	yes	yes
Brocade	alias	wwpn	wwpn	yes	yes
Brocade	alias	wwnn	alias, wwnn	no	no
Brocade	alias	wwnn	wwpn	no	yes
Brocade	alias	port	alias	no	no
Brocade	alias	port	wwpn	no	yes
Brocade	name	wwpn	name	no	no
Brocade	name	wwpn	wwpn	no	yes

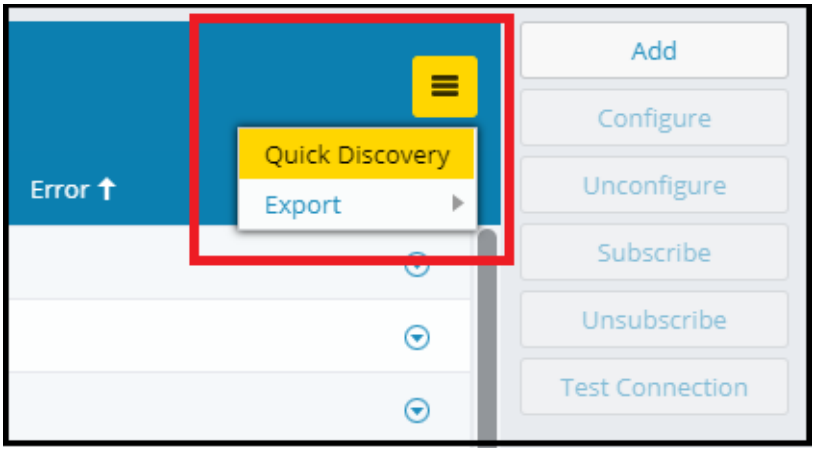
* Retrieves alias definitions from the switches that are used for WWN-to-name resolution

** Retrieves zone information that is used to define the intelligent topology within VirtualWisdom

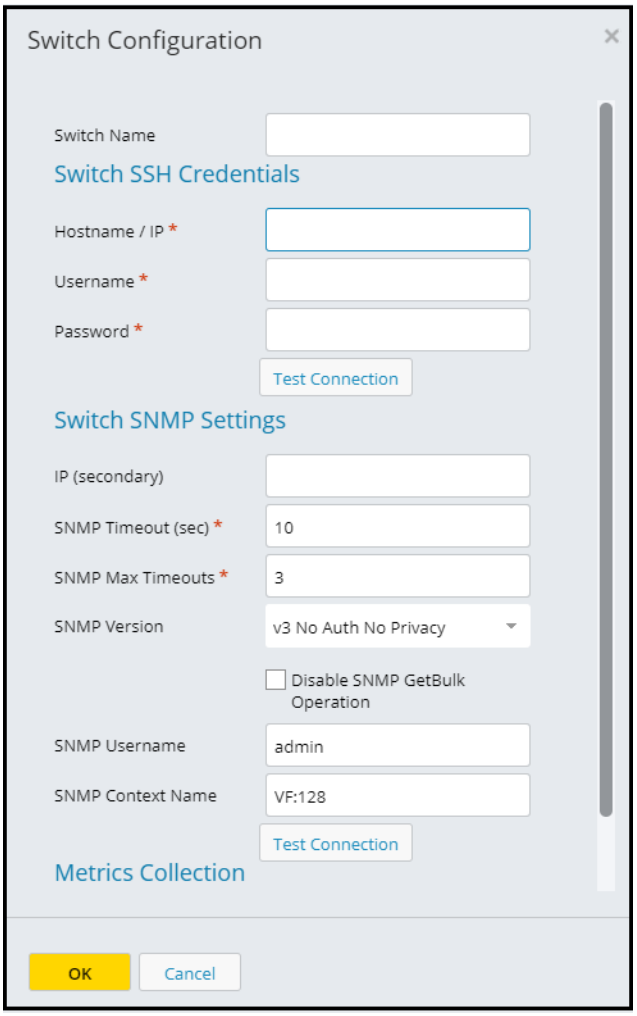
Adding Switches to the SNMP Sources List

You can add switches to the SNMP Sources list either by using Quick Discovery or by using Add. If you add a switch to your infrastructure or a switch you expected to see in the sources list does not appear, you can run Quick Discovery to try to find it. If the switch is still not found, use Add to manually configure the switch.

1. On the SNMP Sources page, click the menu and select **Quick Discovery**.



   If Virtual Wisdom discovers new switches, they are added to the SNMP Sources list.
2. If the switch you want is not discovered, click **Add.**
   The Switch Configuration dialog displays.



3. Enter the configuration settings for the switch and click OK.
   The status of the switch changes to Discovered.
4. Select the switch you added and click **Configure**.
   When the switch is configured without errors, the status changes to Configured,
5. Select the switch you added and click **Subscribe**.
   The status of the switch changes to Subscribed.
6. On the SNMP Sources page, click **Save** to retain your changes.
7. Click **Start Discovery**.
   This begins a discovery of entities associated with the switch you added.
   The status of the switch changes to Discovered.
8. Click **Save** to retain the changes.

Migrating from Brocade BNA to SNMP-SSH Discovery

Follow these guidelines to migrate from Brocade BNA to SNMP-SSH discovery:

1. Before upgrading VirtualWisdom, ensure that one successful discovery has been performed on VirtualWisdom.
2. Upgrade VirtualWisdom and perform a successful discovery on the Brocade BNA integration configuration.

> **NOTE**
> If discovery fails or is unsuccessful, contact Virtana Support.

1. Ensure that there are no duplicate entities in your Brocade BNA integration configuration. If you come across duplicate entities, do not proceed. Contact Virtana Support.
2. Delete the BNA integration configuration and ensure that all the entities are archived. If there is an error deleting the BNA integration, do not proceed. Contact Virtana Support.
3. Click new integration configuration and select *Seed Switch using SNMP-SSH* from the drop-down.
4. Create the SNMP-SSH configuration using the seed switch IP/Hostname. Provide the appropriate SNMP version and username as using your seed switch SNMP settings.
5. Verify that all the switches have been discovered in the *SNMP Sources* tab. If there are any missing switches:
   a. Perform a quick discovery to discover the missing switches.
   b. Add the missing switches using *Add* switch functionality. Provide the SSH and SNMP credentials to add the missing switches.
   c. Repeat the process until all the switches are discovered.
6. Configure and subscribe the discovered switches.
7. Save the configuration and perform a complete successful discovery.
8. Ensure that the expected entities are created and that there no duplicate entities.

Modifying Entity Types for Brocade Switches

There are circumstances under which VirtualWisdom might assign a port as a different type than the one you want. To modify the assigned entity type, see the task, ???.

Content of Integrations Pages

Inventory Table

Table 12. Integrations Inventory Fields

Column Heading	Definition
Name	User-defined name for the integration, often the IP address or the type of integration.
Subscription	Unsubscribed or Subscribed. For Brocade SAN Integration only, if subscribed, shows a ratio of the number of configured switches that are subscribed/the total number of configured switches. For example, 1/5 means that one configured switch is subscribed, out of 5 possible configured switches.
Last Discovery	Date and time that the integration was last discovered, discovering or currently discovering, no discovery, discovery failed, or warned. For Discovery failed or Discovery warned, you can hover over the cell to view the error or warning as a tooltip.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, Metrics collection failed for failed metrics collection, followed by a ratio of the number of failed subscribed switches to total subscribed switches, no collection for no metrics collection, or Warned followed by a timestamp and with no ratio, for a warning. For both failures and warnings, there is no mouse-over tool tip and the user has to drill down and see the failures /warnings in the switch grid. You are notified if an integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification as well as an email notification.

At the end of each row is a down arrow, which, if you click it, provides a short cut to *Configure*, *Test Connection, Start Discovery*, or *Delete* the integration in the associated row.

License Summary Table

The License Summary button displays information on the total number of purchased, used, and remaining licenses.

Table 13. License Summary Fields

Field	Definition
Switch Ports	Number of switch port licenses: Total, used, and remaining
Wire Data Link Credit	Number of wire data link credit licenses: Total, used, and remaining

Switch Ports in the *Brocade SAN License Summary* dialog relates to the number of switch ports that are licensed, even though subscription is done at the switch level. Related to Brocade SAN Integration.

Content of SNMP Sources Pages

The column in the *SNMP Sources* table are defined as follows:

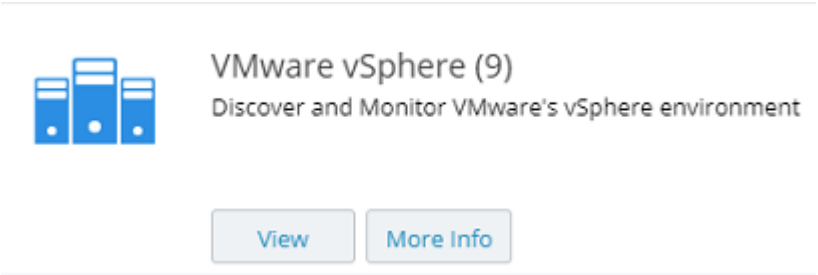
Table 14. SNMP Sources Table Fields

Fields	Definition
Switch Name	Auto-detected name of the switch.
Port Count	Active port count.
Status	Discovered, Configured, Subscribed.
Username	User with permissions on that switch
IP Address	IP address of the switch
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, metrics collection failed, or no collection for no collection. You are notified if an Integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification as well as an email notification.
Metrics Polling Interval	Metrics polling interval set for the switch.
Error	Configuration or subscription errors. Mousing over an error displays a tooltip containing the error text.

From the SNMP Sources page, you can perform the following actions on the switches listed in the table: Add, Configure, Unconfigure, Subscribe, Unsubscribe, and Test Connection.

VMware vSphere Integration

Discover ESX Hosts, VMs, Datastores, and vSAN.



The vCenter integration is an agentless solution that discovers the VMware® estate, and integrates vSphere metrics into the VirtualWisdom platform, optimizing all VM workloads. This integration adds SAN NAS I/O intelligence and operational visibility to VMware deployments, enabling administrators to model and benchmark ESX™/ESXi™ server performance and optimally balance the deployment of virtual machines based on real-time measurements and I/O performance feedback. VirtualWisdom complements vCenter™ by correlating over 100 vCenter metrics in real-time with actual I/O performance data measured by other Virtana probes and integrations.

Prerequisites

For HBA card-HBA port associations to be discovered, the following conditions must be met, in this order:

1. Cisco SAN Integration and Brocade SAN Integration need to be set up to monitor the same environment as Microsoft Hyper-V Integration, IBM PowerVM Integration, and VMware vSphere Integration.
2. A Cisco or Brocade SAN Integration full discovery (either scheduled or manual) must have completed prior to the Microsoft Hyper-V Integration, IBM PowerVM Integration, or VMware vSphere Integration full discovery (either scheduled or manual).

If this order is changed or these conditions are not met, HBA ports are displayed without their HBA card associations.

Configuring VMware vSphere Integration

NOTE

If you want to enable the collection of capacity metrics, follow the steps outlined in `https://kb.vmware.com/s/article/2107096` and disable the two maxQuery limits listed.

1. From the *Settings* page, click **Integrations** in the *Probes and Integrations* section.
   The *Integrations* page is displayed.
2. Click **View**.
   The *VMware vCenter* page is displayed.

Table 15. VMware vSphere Inventory

Field	Definition
Name	User-defined name for the integration, often the IP address or the type of integration. For example, VC_Production or VC_Lab. The name "vcenter" in any combination of case may not be used.
Subscription	Subscription status: Unsubscribed or Subscribed.
Last Discovery	Date and time that the integration was last discovered, discovering for currently discovering, no discovery, Discovery failed, or Warned. For Discovery fail or discovery Warned, you can mouse over the cell shows the error or warning as a tool tip.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, Metrics collection failed for failed metrics collection, no collection for no metrics collection, or Warned followed by a timestamp for a warning. For both failures and warnings, a mouse-over the cell generates a tool tip. You are notified if a software integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification alert as well as an email notification.

At the end of each row is a down arrow, which, if you click it, provides a short cut to *Configure*, *Test Connection*, *Start Discovery*, or *Delete* the integration in the associated row.

3. Click **New**.
   The *Discover New Integration* for VMware vSphere Integration page is displayed.
4. The required *Web Service Port* field in this page is pre-populated. Its value is driven by the use of the SSL check box. If the SSL check box is selected, the port is 443. If the SSL check box is not selected, it is port 80. You can override the pre-populated value if necessary.
   The required *Web Service API* field is also pre-populated.
   Complete the rest of the information as follows:

Field	Definition
Hostname/IP	VCenter host name or IP address. Required.
Username	Username for the VCenter. Required.

Field	Definition
Password	Password for the VCenter. Required.

If the *Use SSL* check box is selected, you must provide the location of your certificate in the *Certificate Location* field. If the **Use SSL** check box is not selected, the *Certificate Location* field is not present.

NOTE

VirtualWisdom requires 1024- or 2048-bit certificates. The SSL certificate can be found on the vCenter server in the following location:

C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\rui.crt

5. Click **Next**.
6. VirtualWisdom tests the connection (hostname and credentials) and tries to find all the ESX servers. This process can take up to five minutes. When the process completes, the next page displays.
   When this process is complete, the *Create New Integration* page displays.
   The *Hostname*, *Web Service API*, *Web Service Port*, *Username*, *Password*, and *Use SSL* (as well as the certificate information if use-SSL was selected) fields are carried forward. The *Metrics Polling Interval* is auto-detected. The *Name* field is user-configurable.
7. Enter the integration *Name*.
   By default, regularly scheduled discovery is enabled for IBM PowerVM, VMware vSphere, and Microsoft Hyper-V Integration configurations. If you would like to disable regularly scheduled discovery, uncheck the *Enable scheduled discovery* check box.
   If you would like to have discovery scheduled regularly, keep the box checked and choose a discovery frequency and time of day. By default, the frequency and time of day for IBM PowerVM, VMware vSphere, and Microsoft Hyper-V Integrations is every day and 1am appliance time.
8. Optionally, click **Test Connection** to test the connection.
9. Use the information in the *ESX Hosts* table to subscribe/unsubscribe specific ESX servers.
   The ESX servers in the *ESX Servers* table on the *Create New VM* window are those ESX servers that were auto-detected.
   The columns headings in the *ESX Hosts* table are defined as follows:

Field	Definition
Server Name	Name of the ESX server
Inventory Path	Path of the ESX Server within the VMware vSphere Integration inventory hierarchy. The last node is the ESX server itself, while first node is the DataCenter, and the intermediate node is the cluster to which ESX server belongs.
Subscription	Subscribed or Unsubscribed

10. Subscribe to an ESX server by selecting the ESX server or ESX servers to which you would like to subscribe and click **Subscribe**.
    All ESX servers are unsubscribed by default.
11. Click **Save** to save all of your changes.
    The *Discovery* dialog box displays, asking if you want the discovery process to start upon saving. Virtana recommends immediate discovery as no metrics are collected into discovery is complete.
12. Click **Yes** to start immediate discovery.

You return to the main grid of integration configurations, and the integration that you just created has "Discovering..." in its last discovery time column.

If you drill down into the integration configuration again, a banner displays on your page saying that discovery is taking place, and might take as much as several hours to complete. While the discovery is taking place you are in read-only mode. You cannot make any changes to the integration or switch configuration.

Configuring for vApp Data Collection

If you intend to have vApp data reported in VirtualWisdom, additional configuration is required.

In VirtualWisdom:

1. Navigate to **Settings > Services Management > ProbeVM for vSphere Proxy > Set Properties**.
2. Add the following property setting:
   Property name: com.vi.vmware.virtualapp.vcenters.queryavailablemetrics
   Value: <the Hostname/IP name of the vSphere server probe>
   Use a comma-separated list for adding multiple vSphere servers.

In vSphere:

1. Navigate to **Statistics Intervals**.
   The path might be similar to *Configuration tab* > *Settings* > *General* > *Statistics*, depending on the version of vSphere you are using.

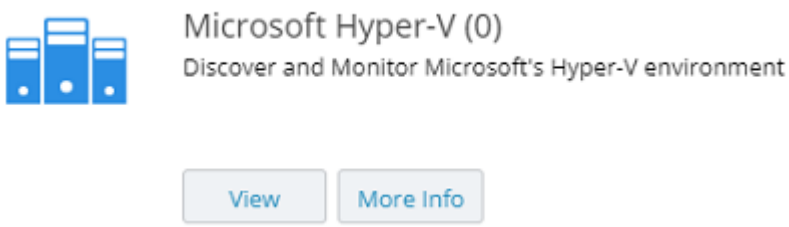
2. Make sure that the statistics intervals field is set to **Level 4** on the vSphere server. This allows for collection of CPU, memory, and network statistics.

VMware vSphere Considerations

When a vMotion is performed on a VM with no guest heartbeat, the VM is not updated until the next discovery.

When an ESX host is moved, the ESX inventory path might not immediately update in VirtualWisdom, because inventory information about ESX clusters only updates with a full discovery. To work around this issue, move the ESX server out of any current cluster before moving it into a new cluster.

Microsoft Hyper-V Integration



The Microsoft Hyper-V Integration is an agentless solution that discovers the Microsoft® Hyper-V environment and provides VM-to-disk LUN visibility.

Advanced analytics enable IT managers to optimize the performance, utilization, and health of their virtualized IT infrastructure running on Hyper-V. This integration offers the ability to correlate Hyper-V CPU and disk metrics with system-wide infrastructure metrics to improve overall application performance. It also enables insight into SAN/NAS I/O intelligence and operational visibility to Hyper-V deployments, which in turn enables administrators to achieve higher performance and better balanced virtual machine deployment based on real-time measurement and analysis of I/O performance.

Supported versions include Windows Server 2012 (R2)/Hyper-V Server 2012 (R2), Windows Server 2016/Hyper-V Server 2016, Windows Server 2019/Hyper-V Server 2019

Configuring Microsoft Hyper-V Integration

1. From the *Settings* screen, click **Integrations** in the *Probes and Integrations* section. The *Integrations* screen is displayed.
2. Click **View** for the software integration. The *Microsoft Hyper-V* screen is displayed.

Table 16. Microsoft Hyper-V Inventory

Column Heading	Definition
Name	User-defined name for the integration, often the integration IP address or the type of integration. For example, Brocade_BNA_27, or seed_switch_1.
Subscription	Unsubscribed or Subscribed. For Cisco SAN Integration and Brocade SAN Integration only, if subscribed, shows a ratio of the number of configured switches that are subscribed/the total number of configured switches. For example, 1/5 means that one configured switch is subscribed, out of 5 possible configured switches.
Last Discovery	Date and time that the integration was last discovered, discovering for currently discovering, no discovery, Discovery failed, or Warned. For Discovery fail or discovery Warned, you can mouse over the cell shows the error or warning as a tool tip.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, Metrics collection failed for failed metrics collection, followed by a ratio of the number of failed subscribed switches to total subscribed switches, no collection for no metrics collection, or Warned followed by a timestamp and with no ratio, for a warning. For both failures and warnings, there is no mouse-over tool tip and the user has to drill down and see the failures /warnings in the switch grid. You are notified if an integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification alert as well as an email notification.

At the end of each row is a down arrow, which, if you click it, provides a short cut to *Configure*, *Test Connection*, *Start Discovery*, or *Delete* the integration in the associated row.

3. Click **New**.
   The *Discover New Integration* for Microsoft Hyper-V screen is displayed.
4. The *Type*, *Frequency*, and *Time of Day* fields on this screen are carried forward from the *Integration Inventory* page. The *Enable scheduled discovery* check box is also checked.
   The *Name* field is user-configurable.
   Enter the *Name*.
   By default, regularly scheduled discovery is enabled for Hyper-V configurations. To disable regularly scheduled discovery, uncheck the *Enable scheduled discovery* check box.

To have discovery scheduled regularly, keep the box checked and choose a discovery frequency and time of day. By default, the frequency and time of day for Hyper-V is every day and 2am Appliance time.

5. Hyper-V Integration hosts can be added individually using the **Add** button. You can add multiple Hyper-V hosts using the **Import** button. To use Import to add multiple Hyper-V hosts, skip to Step 7.
   Click **Add** to add a Hyper-V host one at a time.
   The *Add Host* dialog displays.
6. Complete the information in the *Add Host* dialog as follows:.

Field	Definition
Name	User-defined name for the integration, often the hostname. For example, HYPERV-SC01.
Hostname	Hyper-V host IP address, or a fully-qualified DNS resolvable hostname. For example, hyperv-sc01.lab.company.local.
Domain	Domain of the user account used for polling data from the host.
Username	User name of the user account that is used for polling data from the host.
Password	Password for Username.
Metrics Polling Interval	Frequency of metrics collection. The default is *Every 5 Minutes*.

Click **OK** to add the Hyper-V Integration host.
The *Discover New Integration* screen now shows the host that you added in the *Hosts* list. Proceed to Step 12.

7. Click the **Import** button and follow the steps to import the CSV file.
   Using Import allows you to import multiple Hyper-V Integration hosts at one time. Import requires use of a CSV configuration file that contains Hyper-V hosts and configuration information.
   The CSV configuration file has:
   - One line of text for each host to be imported.
   - Fields in the text line are comma-separated and of the format: *hostname,domain,username, password*

Field	Definition
Hostname	Hyper-V host IP address, or a fully-qualified DNS resolvable hostname. For example, hyperv-sc01.lab.company.local.

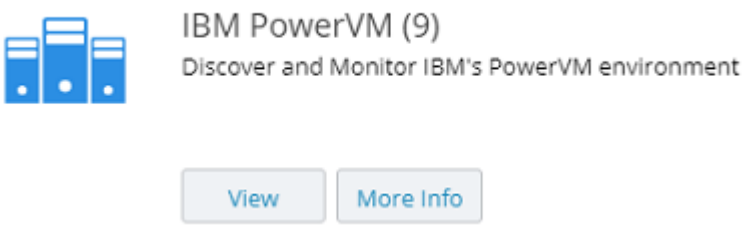
Field	Definition
Domain	Domain of the user account used for polling data from the host.
Username	User name of the user account that is used for polling data from the host.
Password	Password for Username.

A sample CSV file might look like this:
host 2,10.10.56.12,hyperv.dev,vi-services,samplepassword
host 2,10.10.56.12,hyperv.dev,vi-services,samplepassword
and follow the steps to import the CSV file.
After a successful import, the imported hosts appear in the *Hosts* list of the *Discover New Integration* page.

8. Select the Hyper-V Integration hosts that you want to edit from the *Hosts* list and click **Configure**.
   The *Bulk Configuration* dialog box displays.
   a. Select the common fields that you want to change in the selected hosts and click **Next**.
   b. Enter the appropriate information in the *Bulk Configuration* dialog box.
   c. Click OK to apply the changes.
9. Optionally, click **Test Connection** to test the connections (hostname and credentials) for all Hyper-V hosts.
   This process can take up to five minutes. A message will display indicating whether the configuration is correct or if errors were found that you need to correct.
10. Subscribe to the hosts by selecting the host or hosts to which you would like to subscribe and clicking **Subscribe**.
    When you click **Subscribe**, VirtualWisdom also validates that there are sufficient licenses.
11. Click **Save** to save all of your changes.
    The *Discover* dialog box displays, asking if you want the discovery process to start upon saving. Immediate discovery is recommended, as no metrics are collected until discovery is complete.
12. Click **Yes** to start immediate discovery.
    After clicking **Yes**, you return to the main grid of all software integration configurations, and the integration that you just added has “Discovering...” in its last discovery time column.
    If you drill down into the integration configuration again, a banner displays on your screen saying that discovery is taking place. While the discovery is taking place you are in read-only mode. You cannot make any changes to the integration or switch configuration during discovery.

IBM PowerVM Integration

Discover Hosts and VMs.



The IBM PowerVM Integration integration is an agentless solution that discovers the IBM® PowerVM environment and integrates with the VirtualWisdom platform to provide LPAR to disk LUN visibility. This provides IBM PowerVM Integration customers with greater insight into the virtualization stack to enable proper placement and balancing of workloads as well as the intelligence needed to properly size the LPARs. VirtualWisdom along with the IBM PowerVM Integration delivers objective, platform-aware monitoring and problem resolution using real-time, deterministic performance information. This integration also reduces risk in large IT environments by using proactive trend alerts that indicate emergent performance problems.

NOTE
As suggested by IBM, you should configure switches for persistent FCID assignment when possible.

Prerequisites

IBM PowerVM Integration does not currently support redundant HMC configurations. The integration should only be configured for one HMC of a pair that manages the same group of hosts.

For HBA card-HBA port associations to be discovered, the following conditions must be met, in this order:

1. Cisco SAN Integration and Brocade SAN Integration need to be set up to monitor the same environment as Microsoft Hyper-V Integration, IBM PowerVM Integration, and VMware vSphere Integration.

2. A Cisco or Brocade SAN Integration full discovery (either scheduled or manual) must have completed prior to the Microsoft Hyper-V Integration, IBM PowerVM Integration, or VMware vSphere Integration full discovery (either scheduled or manual).

If this order is changed or these conditions are not met, HBA ports are displayed without their HBA card associations.

AIX uses managed system ID instead of managed system name when executing HMC commands. Issues can occur when the ID is not unique.

Configuring IBM PowerVM Integration

1. From the *Settings* tab, click **Integrations** in the *Probes and Integrations* section.
   The *Integrations* page is displayed.
2. Click **View** for the software integration.
   The *IBM PowerVM* page is displayed.

Table 17. IBM PowerVM Inventory

Field	Definition
Name	User-defined name for the integration, often the integration IP address or the type of integration. For example, HMC_1 or HMC_2.
Subscription	Subscription status: Unsubscribed or Subscribed.
Last Discovery	Date and time that the integration was last discovered, discovering for currently discovering, no discovery, Discovery failed, or Warned. For Discovery fail or discovery Warned, you can mouse over the cell shows the error or warning as a tool tip.
Last Metrics Collection	Date and time of last metrics collection, Collecting metrics for metrics collection in progress, Metrics collection failed for failed metrics collection, no collection for no metrics collection, or Warned followed by a timestamp for a warning. For both failures and warnings, a mouse-over the cell generates a tool tip. You are notified if a software integration fails to collect metrics for two hours. The notification takes the form of a VirtualWisdom Health Notification alert as well as an email notification.

At the end of each row is a down arrow, which, if you click it, provides a short cut to *Configure*, *Test Connection*, *Start Discovery*, or *Delete* the integration in the associated row.

3. Click **New**.
   The *Discover New Integration* for IBM PowerVM Integration page displays.
4. Make your selections on the *Discover New Integration* page.

The default method of discovery and metrics collection is using the HMC, with the HMC executing commands against the VIOS. This provides the simplest method of configuration as only a single SSH connection from the Appliance to the HMC is required. The configuration requires “hmcoperator” privileges to execute commands against the VIOS servers using the “viosrvcmd” functionality. Use of “viosrvcmd” has security implications as it allows root level access to the VIOS without additional authentication.

The “enable direct VIOS authentication” check box offers an alternative configuration method. This alternative removes the need for “hmcoperator” privileges for the main HMC user and allows that user to run with “hmcviewer” privileges.

So that the VIOS level information can be discovered (vSCSI disk maps and HBA mappings), an additional service account with view-only privileges is required on each VIOS server to be monitored.

This account should have common credentials across the VIOS servers and can be authenticated by password or SSH key. There should be network connectivity that allows SSH access between the VirtualWisdom Appliance and the VIOS to be monitored.

Complete the information for the *Discover New Integration* page as follows:

Field	Definition
HMC Hostname	HMC host name or IP address. Required.
Username	Username for the HMC. Required.
Password or SSH Key	Password or SSH key for the HMC. Required.
VIOS Username	Username for the VIOS. Only required if VIOS direct authentication is in use.
Password	Password or SSH key for the VIOS. Only required if VIOS direct authentication is in use.

The *Enable direct VIOS authentication check box* enables connection from the Appliance to the VIOS.

5. Click **Next**.

   VirtualWisdom tests the connection (hostname and credentials) and tries to find all the IBM PowerVM Integration hosts. If the VIOS Username and Password are provided, VirtualWisdom also tests connections to the VIOS. This process can take up to five minutes.

   When this process is complete, the *Create New Integration* page displays.

6. The *HMC Hostname*, *Username* and *Password* are carried forward. If the VIOS username and password are provided, they are also carried forward. The *Metrics Polling Interval* is auto-detected. The *Name* field is user-configurable.

Enter the Integration *Name*.

By default, regularly scheduled discovery is enabled for IBM PowerVM Integration configurations. If you would like to disable regularly scheduled discovery, uncheck the *Enable scheduled discovery* check box.

If you would like to have discovery scheduled regularly, keep the box checked and choose a discovery frequency and time of day. By default, the frequency and time of day for IBM PowerVM Integration is every day and 1am appliance time.

7. Optionally, click **Test Connection** to test the connection to the HMC, and VIOS if the VIOS username and password are provided.
8. The IBM PowerVM Integration Hosts in the *IBM PowerVM Integration Hosts* table on the *Create New Integration* for IBM PowerVM Integration window are those IBM PowerVM Integration hosts that were auto-detected.

   Use the information in the *IBM PowerVM Integration Hosts* table to subscribe/unsubscribe specific IBM PowerVM Integration Hosts. The columns headings in the *IBM PowerVM Integration Hosts* table are defined as follows:

Field	Definition
Name	Name of the IBM PowerVM Integration Host.
IP	IP address of the IBM PowerVM Integration Host.
CPU Cores	Number of CPU cores of the IBM PowerVM Integration Host.
Sampling Rate	Sampling rate of IBM PowerVM Integration Host in seconds. Sampling should be enabled on the HMC to allow metric collection to take place. If the sampling rate is shown as disabled, VirtualWisdom is not able to collect metrics from that host.
Subscription	Subscribed or Unsubscribed.

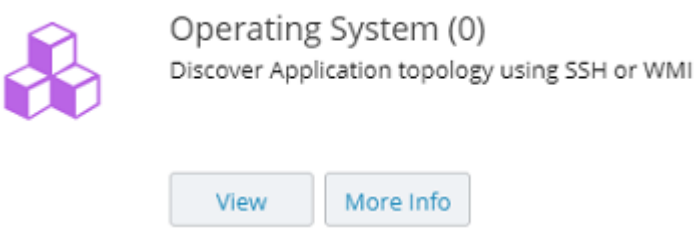
9. All IBM PowerVM Integration Hosts are unsubscribed by default. Subscribe to a IBM PowerVM Integration Host by selecting the IBM PowerVM Integration Host or IBM PowerVM Integration Hosts to which you would like to subscribe and click **Subscribe**.
10. Click **Save** to save all of your changes.

    The *Discovery* dialog box displays, asking if you want the discovery process to start upon saving. Virtana recommends immediate discovery as no metrics are collected into discovery is complete.
11. Click **Yes** to start immediate discovery.

    You return to the main grid of all software integration configurations, and the integration that you just created has "Discovering..." in its last discovery time column.

    If you drill down into the integration configuration again, a banner displays stating that discovery is taking place. While the discovery is taking place you are in read-only mode. You cannot make any changes to the integration or switch configuration.

Operating System Integration



The Operating System Integration interacts with physical and virtual machines for application discovery and operating system monitoring. To these ends, VirtualWisdom communicates directly with the machines to collect information and statistics, using WMI for those running Windows operating systems, and using SSH for those running various flavors of UNIX.

For application discovery, VirtualWisdom collects information from servers about the services (such as database and app servers) that are running on an operating system, its resources, as well as the IP addresses with which it is communicating. Application discovery is not performed on Windows domain controllers.

NOTE
Windows Management Instrumentation (WMI) only identifies physical Network Interfaces for which the MAC address of the Bonded NIC is the same as the MAC address of the physical NIC. This results in physical NICs not being reported as children of a NIC bonded to multiple physical NICs. Therefore, the relationship between a Windows Bonded NIC and its children cannot be reported in VirtualWisdom topology views or entity inventory pages.

The following operating system versions are supported for application discovery:

- Linux
  - Ubuntu (16.0.4.2, 17.0.4)
  - SUSE (11, 12)
  - CentOS (6.8, 7.4)
  - Red Hat Enterprise Linux (6.9)
  - Oracle Linux (6.9)

  - Debian (9)
  - Solaris 10 and 11 (64-bit)
- Windows
  - Windows Server 2019
  - Windows 2016
  - Windows 2012 R2
  - Windows 2008 R2 Standard

For operating system monitoring, VirtualWisdom collects information about the operating system's compute, storage, and networking resources, and collects metrics for these resources.

The following versions of operating systems are supported for operating system monitoring:

- Linux
  - Ubuntu (16.0.4.2, 17.0.4)
  - SUSE (11, 12)
  - CentOS (6.8, 7.4)
  - Red Hat Enterprise Linux (6.9)
  - Oracle Linux (6.9)
  - Debian (9)

LVM implemented on top of multipath devices on Linux is not supported. VirtualWisdom does not discover or collect metrics for operating system instances with this configuration.

- Windows
  - Windows Server 2019
  - Windows 2016
  - Windows 2012 R2
  - Windows 2008 R2 Standard

Configure Operating System Instances

Use the *Configuration* tab to establish Windows (WMI) and Linux (SSH) credential sets for specified hosts. Credential information is supplied by the customer. The credentials needed for VirtualWisdom can be read-only, and do not require admin privileges and root access. In many cases, customers are already using management tools with established credentials, and these can often be leveraged for use with Operating System Integration.

About This Task

There are specific permission/administrator requirements for using the OS Data Collector.

- For Linux systems, a non-root account can be used. The only minor effect of a non-root account is that the “hypervisor type” property is not populated for ESX VMs.
- For Windows 2016 and Windows 2012R2A, a non-administrator account can be used.
  - A non-administrator account can also be used for Windows 2008 R2 Standard, but network and disk entities cannot be discovered from it.
  - When a non-administrator account is used, the account must be in the "Performance Monitor Users Group," and "User Account Control" must be disabled. See https://docs.microsoft.com for a description of the "User Account Control"feature's relationship to WMI.

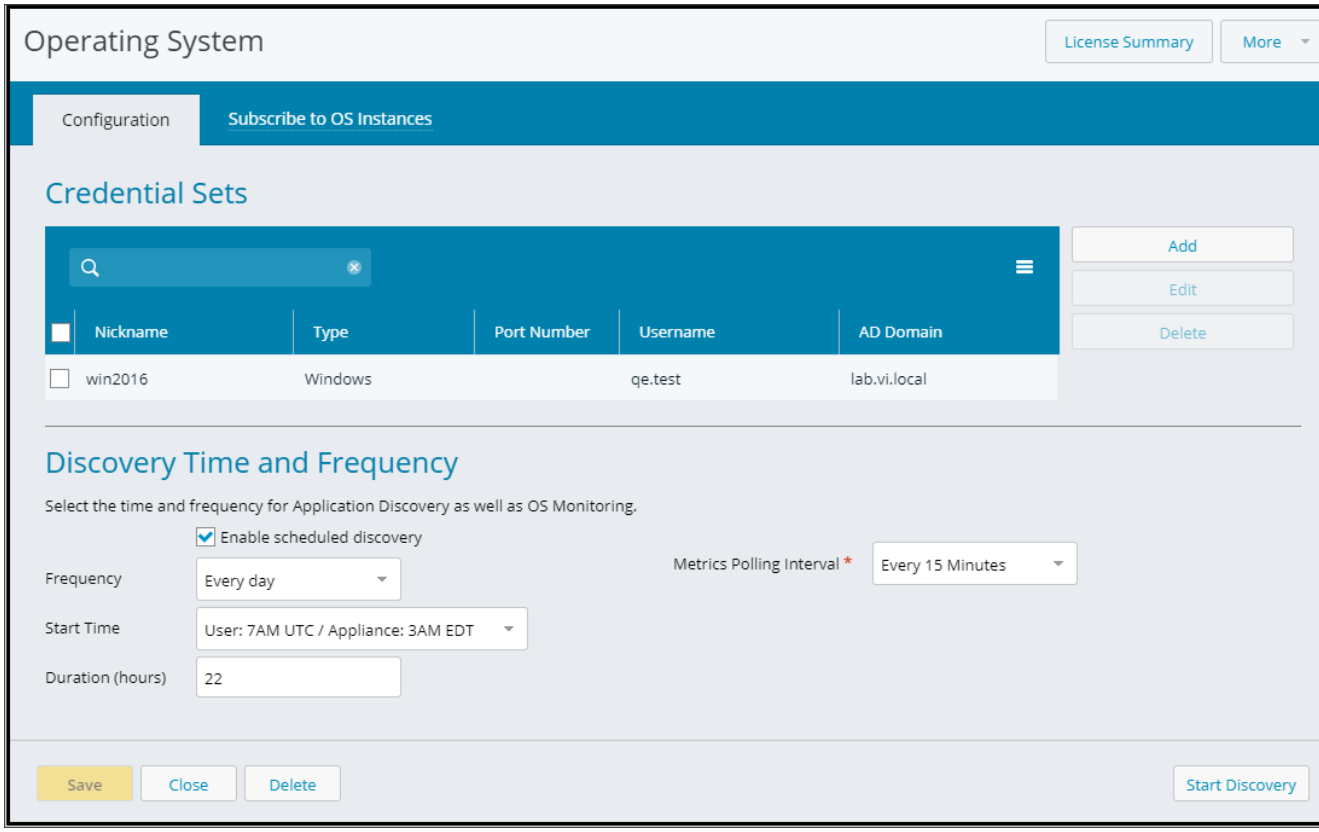
Known Issues

Description	Workaround
On some versions of Linux, the speed of a network interface cannot be obtained from the operating system.	None.
You cannot create a report when the %Network Received Utilization and %Network Transmit Utilization metrics are used with the Application filter.	You can see data for these metrics with the Network Interface filter. Manually add appropriate Network Interface entities to your application.
Upon upgrade to VW 6.1 or later, any existing Logical Volume entities are archived and Logical Volumes re-discovered.	None. Metrics collected prior to VW 6.1 for preexisting Logical Volumes can be accessed by requesting reports on the archived Logical Volumes.

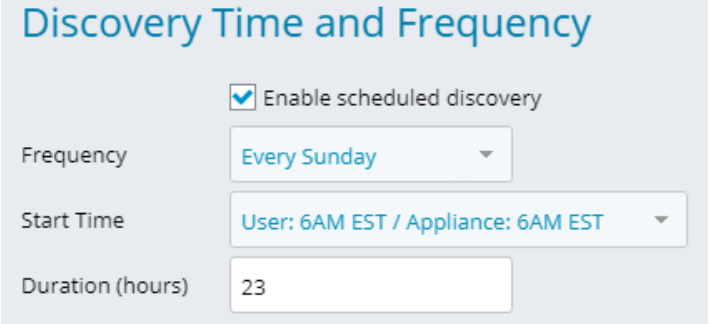
Prerequisites

If you have enabled VMware vSphere Integration or IBM PowerVM Integration, you should have run at least one discovery on those integrations before doing an Operating System Integration discovery. Otherwise, you might see duplicate compute entities in the UI.

1. Click **Settings**, then *Integrations* in the *Probes and Integrations* section, and then the **View** button for *Operating System*.
   The *Operating System* page displays, consisting of two tabs:
   - Configuration
   - Subscribe to OS Instances



2. On the **Configuration** tab, click **Add** to add a credential set.
   The *New Credential Set* dialog box displays.
   There are two variations of the *New Credential Set* dialog box, depending on whether you are adding Linux (SSH) or Windows (WMI) credentials.
   You can use a private key for SSH credentials, but it requires a key file. Passphrase is optional.
   If the host password is changed, the credential set must also be changed. All passwords stored in VirtualWisdom are encrypted.
   For Windows OS monitoring, CIFS Security Mode NTLMv1 and NTLMv2 are both supported.
   Discovery Time and Frequency is, unlike other scheduled discovery processes, bounded by a specified duration in hours. After that amount of time, discovery is paused and bookmarked, and the next scheduled discovery starts at that bookmark. These settings apply to discovery for both application discovery and OS monitoring.



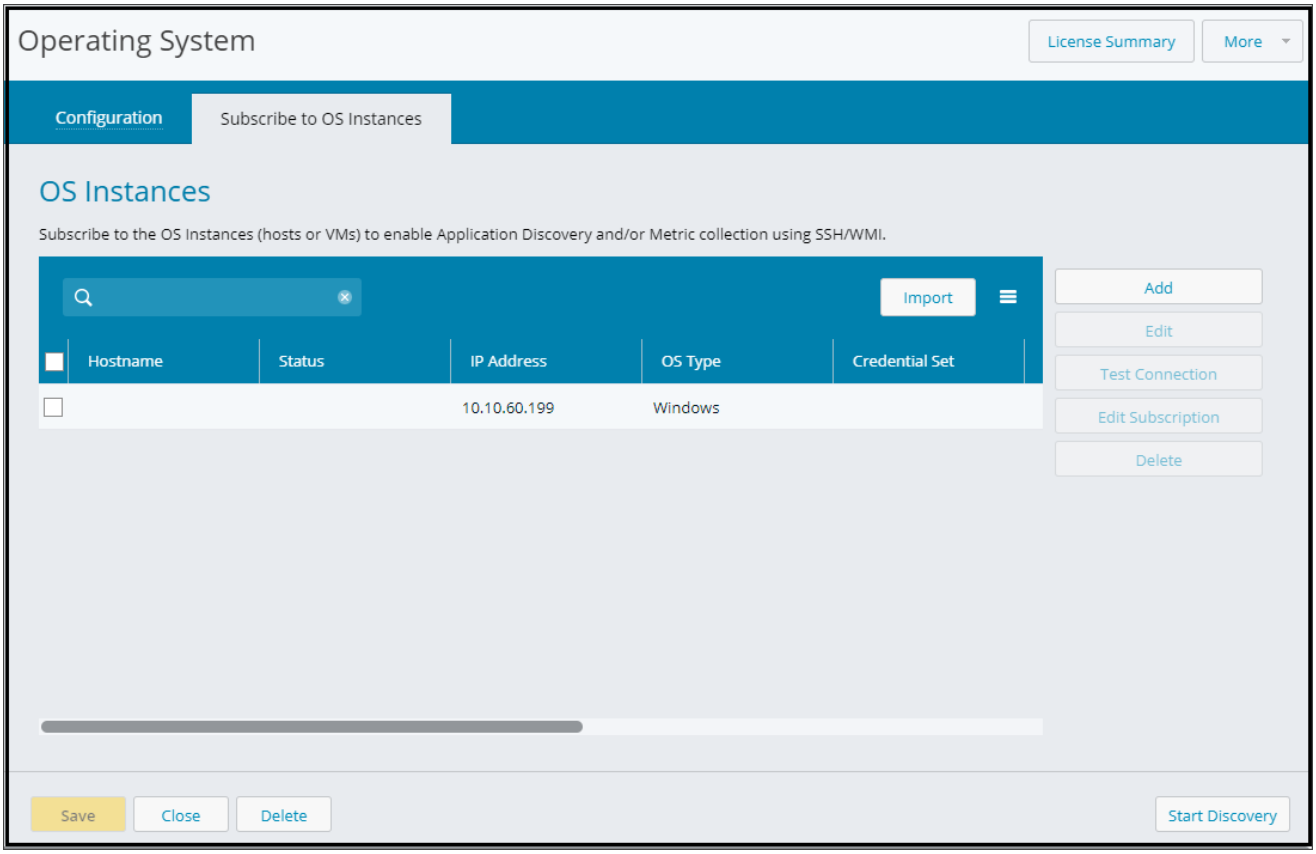
Related Topics

Import File Format [93]

Subscribe to OS Instances

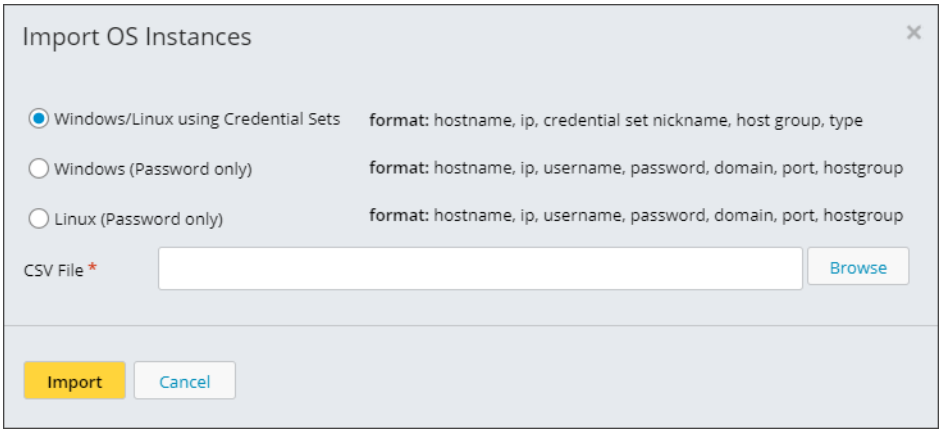
The *Subscribe to OS Instances* tab adds or imports OS Instances and then subscribes to or unsubscribes from them for application discovery and/or OS monitoring. Either an IP address or a hostname is required. If a conflict is found, the IP address takes precedence.

1. Click **Add** to add a host.
   The *New OS Instance* dialog box displays.



There are two variations of the *New OS Instance* dialog box, depending on whether you are adding a Linux or Windows OS instance.

2. Click **Import** to import hosts from a CSV file of a specified format.
3. You can click **Save** on the main OS Instances page at any time to save the current status of the operation.
4. Click **Test Connection** to verify that the specified credentials can be used to connect to the host.
5. Select individual, multiple, or all hosts, and click **Subscribe/Unsubscribe**.
   The *Import OS Instances* dialog box displays.



A discovery audit file contains details of the import.
The *App Discovery* and *OS Monitoring* columns show the subscription status of the host entry for those services.
You can click on the triangle on the right edge of the column to change the subscription status. If the entry has *Subscribed* selected for *App Discovery*, it is included for *App Discovery*. If the entry has *Subscribed* selected for *OS Monitoring*, VirtualWisdom discovers resources within that OS and collect metrics for it.
To change the subscription status for one or more entries at the same time, select individual, multiple, or all hosts, and click **Edit Subscription**. A pop up window displays and from there, you can set the *App Discovery* and *OS Monitoring* subscription states.

6. Click **Save** to save the configuration.
Discovery occurs at the schedule that you have set up in the *Configuration* tab. If you want discovery to occur now, click **Start Discovery**.

> **NOTE**
> OS monitoring metrics collection being for an OS instance only *after* it has been successfully discovered.

The *Status* column indicates the discovery status and metrics collection of the OS instance. The *Last Metrics Collection* column indicates when the last metrics collection was attempted for that OS Instance.

Related Topics

Import File Format [93]

Import File Format

The following format is required for CSV files used to import OS instances.

Hostname: Optional

IP address: Used for the address device on the network

Credential set nickname: Name of the credential set

Host group: Not used, leave blank

Type: SSH or WMI

Example Import file:

In the format hostname:ip:credential nickname:type:

Your Host,10.36.4.41,visvc,,ssh

,10.36.4.42,visvc,,ssh

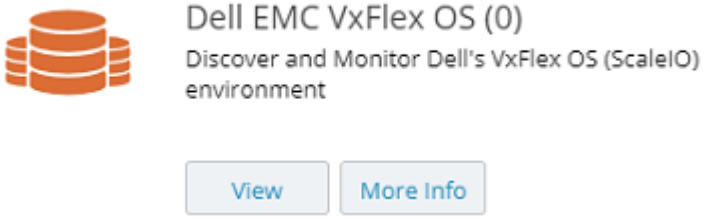
,10.36.4.44,visvc,,ssh

,10.36.4.56,visvc,,ssh

,10.36.4.57,visvc,,ssh

,10.36.4.105, vwuser - Win,,wmi

Dell EMC VxFlex OS Integration



The Dell EMC VxFlex OS Integration captures VxFlex metrics through the VxFlex Gateway and sends them to the VirtualWisdom appliance to apply problem-solving analytics across hundreds of metrics. Use VirtualWisdom to get control over cache and capacity utilization, optimize application performance, and quickly troubleshoot problems.

The VirtualWisdom 10-second infrastructure summaries are derived from over 400 VxFlex-specific metrics including:

VxFlex OS Cache Usage

- Cache Entry Eviction Count
- Cache Big Bloc Eviction Count
- Cache No Eviction Count

SDS Capacity

- Capacity Used

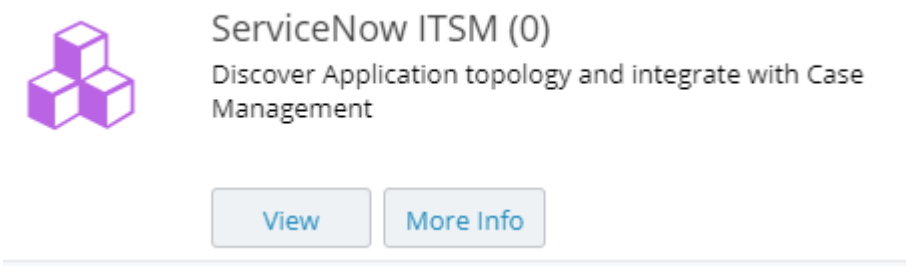
SDS Latency

- DOM Client Avg Read latency
- DOM Client Avg Write Latency
- DOM CompMgr Avg Read Latency
- DOM CompMgr Avg Rec Write Latency
- DOM CompMgr Avg Write Latency

Configuring Dell EMC VxFlex OS Integration

1. From the Settings tab, click **Integrations** in the Probes and Integrations section, and then click the **View** button for *Dell EMC VxFlex OS*.
   The *Dell EMC VxFlex OS* page is displayed, with information about existing VxFlex integrations.
2. To create a new Dell EMC VxFlex OS Integration, click **New**.
   The *New Dell EMC VxFlex OS* page is displayed.
3. Complete the following fields:
   Name
   Hostname/IP
   Username
   Password
   Port
   All fields are required.
   The *Use SSL* checkbox is on by default.
4. Click **Browse** to select a *Certificate File*.
5. You can click **Save** at any time to save the current status of the operation.
6. Click **Save** and then **Start Discovery**.

ServiceNow ITSM Integration



The VirtualWisdom AppDynamics APM Integration, ServiceNow, and Dynatrace APM functions all discover running applications in those products and add them to VirtualWisdom. VirtualWisdom uses the applications discovered by the first-executed function (AppDynamics APM Integration, ServiceNow, or Dynatrace APM), and, after the other function executes, conflict resolution and manual reconciliation of differences as seen by VirtualWisdom might be required.

ServiceNow integrates with VirtualWisdom alarms, enhanced REST API access to reports, analytics, and case management CMDB. It also enables discovery/importation of applications directly from ServiceNow. It provides the ability to configure Tier Mapping to associate business criticality to VirtualWisdom tiers. VirtualWisdom can import application descriptions, business service, and the set of all hosts that support that business service. VirtualWisdom alarm thresholds are automatically associated with each tier. The application and the entire supporting infrastructure are included in this tiering setup.

The bi-directional integration between VirtualWisdom and ServiceNow enables Incidents to be automatically created, updated and closed within ServiceNow. Case updates in VirtualWisdom cause Incident updates in ServiceNow, and Incident closure in ServiceNow closes the corresponding case in VirtualWisdom.

Configuring a ServiceNow Instance

VirtualWisdom discovers/imports applications directly from both local and cloud instances of ServiceNow Business Service, Manual Service, and Technical Services.

VirtualWisdom creates applications only from existing Hosts, VMs, Microsoft Hyper-V VMs, and PowerVM Partitions that have been discovered by other VirtualWisdom integrations.

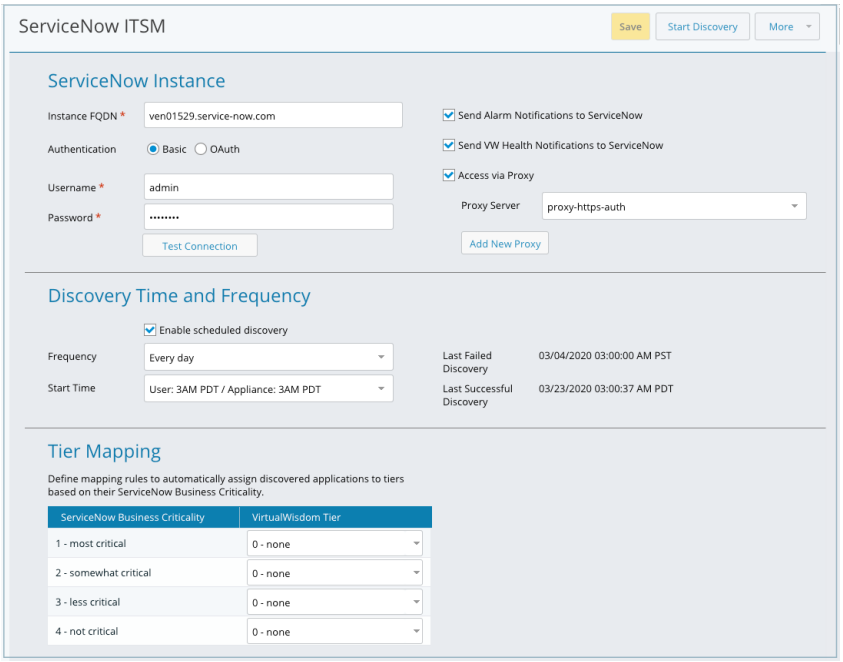
Prerequisites

VirtualWisdom requires read access to the following ServiceNow database tables via the assigned ServiceNow user with the sm_user role.

- cmdb_ci_service
- cmdb_rel_ci
- svc_ci_assoc
- cmdb_ci_hardware
- cmdb_ci_server
- cmdb_ci_vmware_instance (if applicable)
- cmdb_ci_hyper_v_instance (if applicable)

In order for VirtualWisdom to integrate with ServiceNow's incident infrastructure, the configured ServiceNow user must also have the itil role assigned to it.

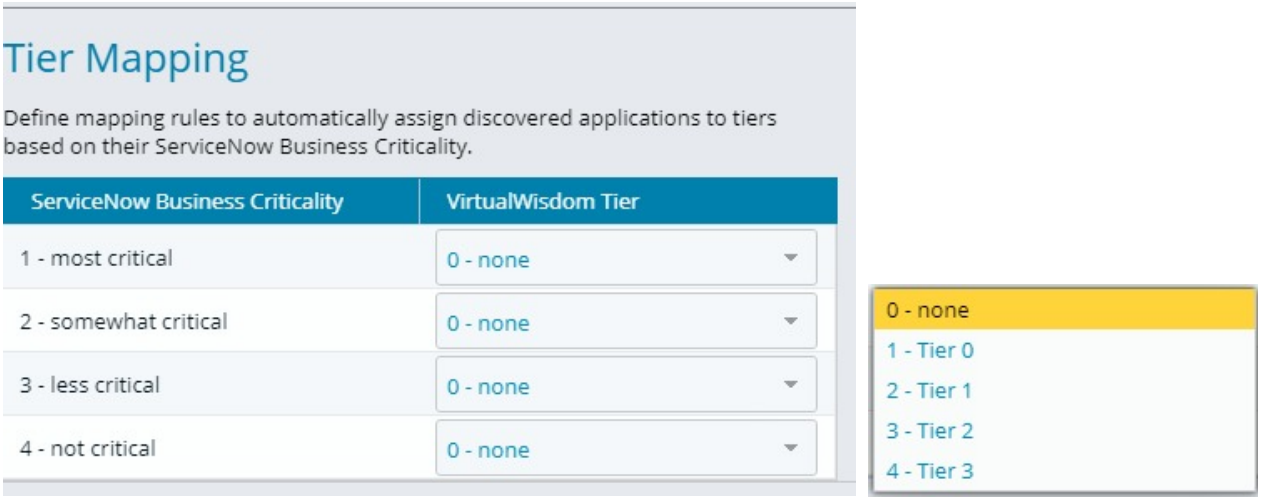
1. Select an instance of a ServiceNow application (cloud or on-premise), and copy the URL.
2. Navigate to the Settings page and click **Integrations** in the *Probes and Integrations* section, and then click the **View** button for *ServiceNow*.
   The *ServiceNow* page is displayed.



3. Paste the copied ServiceNow URL into the *Instance FQDN* field, and type your credentials in the *Username* and *Password* fields.
4. Select any optional items you want to configure for the instance.
   If you select *OAuth Authentication*, you need to specify additional client information. The *Client Secret* key is displayed only at the time the OAuth token is generated.

You can also select the following: *Send Alarm Notifications to ServiceNow* and *Send VirtualWisdom Health Notifications to ServiceNow*.

5. Click **Test Connection** to verify that the specified URL and API Token can connect to the site successfully using the provided credentials.
6. Optional: Select **Access via Proxy** if your environment requires access to the internet through a proxy server.
   You can select an existing proxy server or add a new proxy server.
7. Optional: Select **Enable Scheduled Discovery** and select the frequency and start time.
8. Optional: Assign a ServiceNow-discovered application to one or more VirtualWisdom tiers based on the *ServiceNow Business Criticality* ranking.



   The default setting (*none*) does not map the ServiceNow levels to any tier, and you can select one or more tiers from the VirtualWisdom defaults or create your own tiers. For more information, see the following section, *Create Application-Assigned Tiers*.
9. Click **Save** and **Start Discovery**.
   The specified ServiceNow application is discovered and optionally assigned to VirtualWisdom tier(s). If scheduled discovery was specified (defaults to *Enable*), it begins as specified in the *Discovery Time and Frequency* section, similar to existing integrations.
   Changes in ServiceNow are updated in VirtualWisdom at manual discovery or the next scheduled discovery.
   In a ServiceNow instance, when you discover virtual machine entities, it does not show the IP Address and FQDN in the VM entity, even though the IP address is linked under Network Adapter tab for that entity, VirtualWisdom is not addressing that table for its IP address. You can provide the IP manually in the IP address field and perform a discovery, in which case, the application is discovered.
   After you create an application, you can drill down into it to see topology, application components, and FC conversations.
   VirtualWisdom automatically pushes case information to ServiceNow.

Adding a Proxy Server

If your corporate security requirements include using proxies for internet access, you can add proxy servers to your integration configuration. Currently, ServiceNow is the only VirtualWisdom integration that supports proxy servers.

When configuring a new proxy server, clicking Test Connection confirms that the proxy server is listening on the port provided. If the proxy server uses basic authentication, the correct user and password must also be provided for the test connection to pass. If the proxy server does not require authentication, the user and password are ignored.

About This Task

- You can select only one proxy server per integration.
- Only Basic Auth is currently supported as an authentication method.
- If you create an invalid proxy server, it will still display in ServiceNow.
  If you select the invalid proxy, there is no indication it is invalid and that it will not connect. Ensure you use Test Connection when you create a proxy to verify the server is accessible.
- If you delete or update a proxy server, ServiceNow is refreshed with the new configuration.

Prerequisites

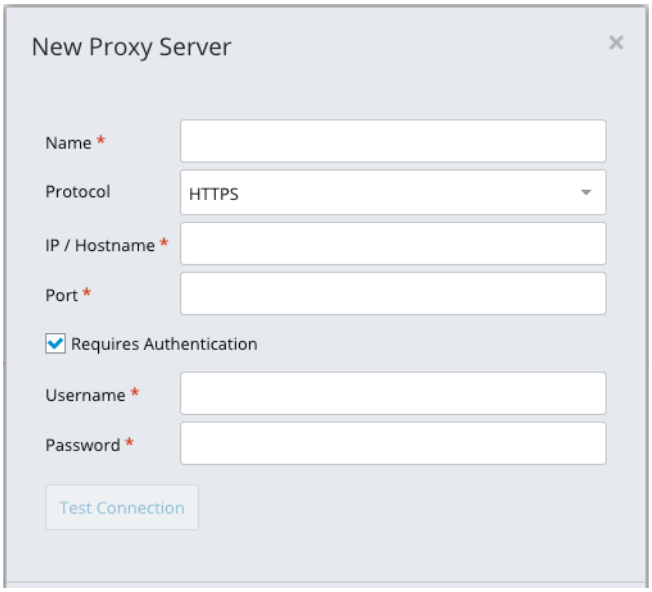
To complete this task, you need the following information for the proxy server:

- Server name
- Protocol type: HTTPS or HTTP
- IP address or hostname
- Server port number
- If the protocol is HTTPS, authentication is required so you must provide the username and password to access the server

Steps

1. You can access the proxy server configuration from the **Settings** page in either of two ways.
   - On the **Probes and Integrations** panel, click **Integrations**, then select **View** for ServiceNow ITSM.
   - In the ServiceNow Instance area, select **Access via Proxy**.
2. Click **Add New Proxy**.
3. On the **Administration** panel, click **Proxy Servers**.
   - Click **New Proxy Server**.
     The New Proxy Server page displays.

4. Complete the configuration for the proxy server.



   Only Basic Auth is currently supported for authentication.
5. Click **Test connection** to verify the proxy settings are correct and the server can be accessed.
   Clicking Test Connection confirms that the proxy server is listening on the port provided and the integration can successfully communicate with the ServiceNow instance via the selected proxy server. If the proxy server uses basic authentication, the correct user and password must also be provided for the test connection to pass. If the proxy server does not require authentication, the user and password are ignored.

If you create an invalid proxy server, it will still display in ServiceNow.

TIP

If the proxy server cannot be accessed, the configuration can still be saved so that you can modify it later. However, there is no indication that a proxy is invalid. Therefore, ensure you use Test Connection when you create or modify a proxy to verify the server is accessible.

VirtualWisdom Incidents in ServiceNow

When a VirtualWisdom Health Notification is opened, an incident is created in ServiceNow. When the incident is closed in ServiceNow, the VirtualWisdom Health Notification is ***not*** closed.

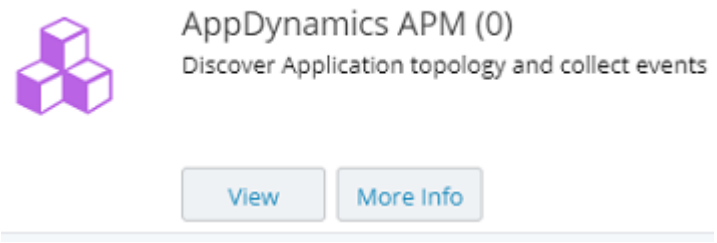
When VirtualWisdom clears a health alert, the corresponding ServiceNow incident state is changed to *closed*. Health Notifications cannot be closed by a user, but they are cleared by the system when it detects that the issue no longer persists.

Table 18. ServiceNow/VirtualWisdom Parameter Comparison

ServiceNow Parameters	VirtualWisdom Parameters	Description
short-description	VirtualWisdom, Device Name, Failed Part	Set the short description to: VirtualWisdom-<Device Name>-<Failed Part>
severity	Severity	ServiceNow: 1 - Critical 2 - High 3 - Moderate 4 - Low 5 - Nondisruptive VirtualWisdom equivalent: FATAL (Critical) WARNING (Moderate) INFO (Nondisruptive)

ServiceNow Parameters	VirtualWisdom Parameters	Description
description	HostName Case ID Case Name Case Description Case Type Device Name Failed Part Additional Details Threshold Values Open Time	The details of the case are stored in the description.

AppDynamics APM Integration



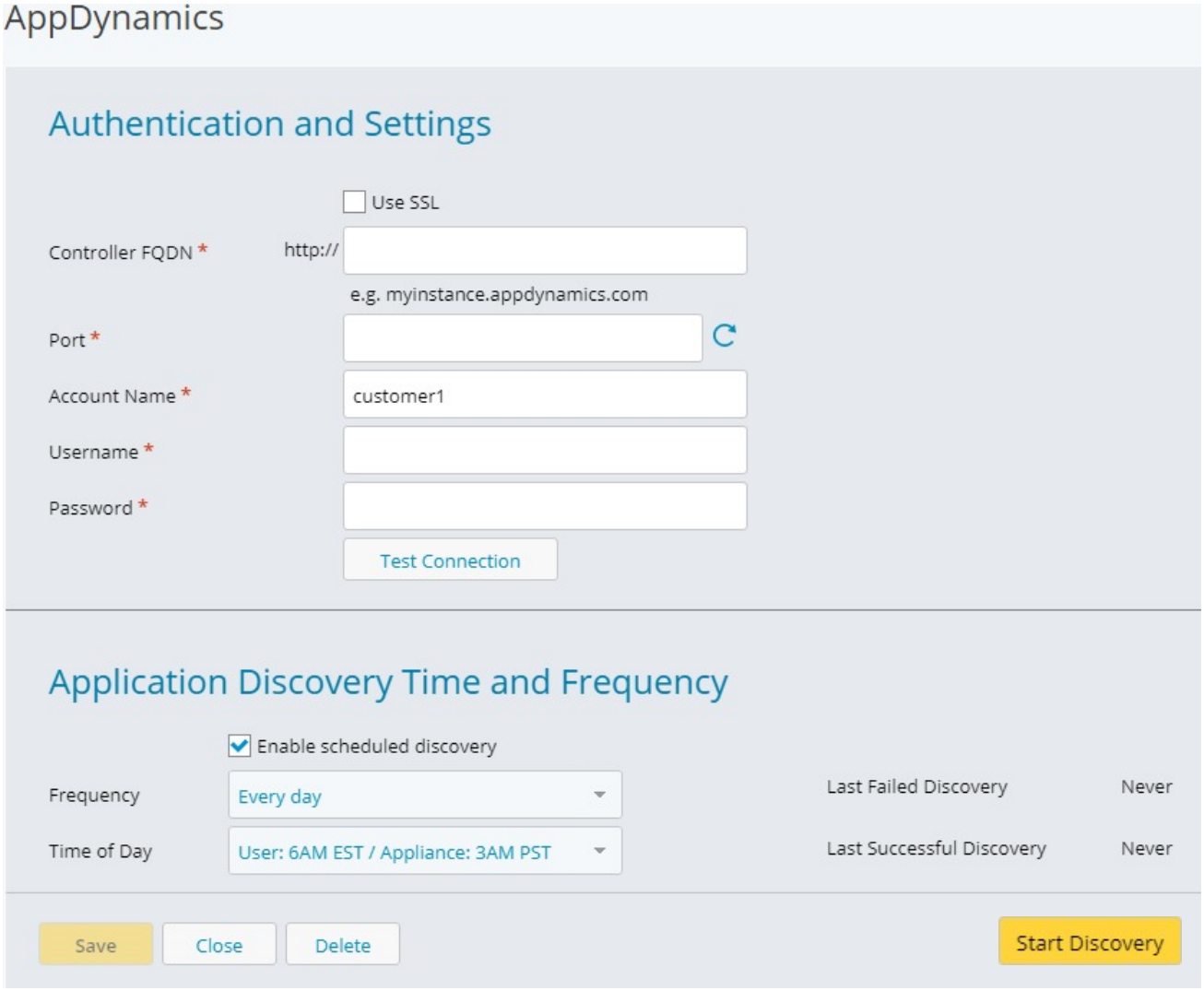
The VirtualWisdom AppDynamics APM Integration, ServiceNow, and Dynatrace APM functions all discover running applications in those products and add them to VirtualWisdom. VirtualWisdom uses the applications discovered by the first-executed function (AppDynamics APM Integration, ServiceNow, or Dynatrace APM), and, after the other function executes, conflict resolution and manual reconciliation of differences as seen by VirtualWisdom might be required.

Configuring AppDynamics APM Integration

VirtualWisdom discovers/imports applications directly from both local and cloud instances of the AppDynamics controller, and creates applications only from existing Hosts, VMs, Microsoft Hyper-V VMs, and PowerVM Partitions that have been discovered by other VirtualWisdom integrations.

Steps

1. Select an instance of a AppDynamics app (cloud or on-premise), and copy the URL.
2. From the Settings tab, click *Integrations* in the *Probes and Integrations* section, and then click the **View** button for *AppDynamics APM Integration*.
   The *AppDynamics APM Integration* page is displayed.

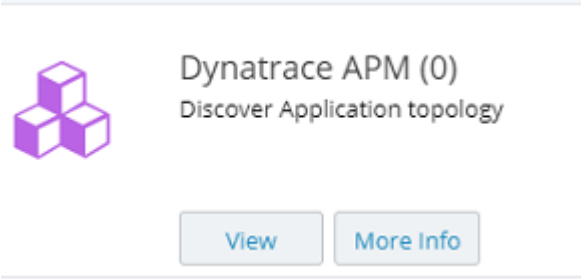


3. To specify a secure connection, click the *Use SSL* checkbox.
   If SSL is selected, the port defaults to 443. Otherwise, the default port is 8090.
4. Paste the copied URL into the *Controller FQDN* field, specify *Port* (if overriding the default) and *Account Name* (to override the default *customer1*), and type your credentials in the *Username* and *Password* fields.
5. Optional: Assign an AppDynamics APM Integration-discovered application to one or more VirtualWisdom tiers.

VirtualWisdom Health notifications are not imported for any Server that is not a part of Tier/Node of an application in AppDynamics.

6. Click **Test Connection** to verify that the specified URL and API Token can connect to the site successfully.
7. Click **Save** and then **Start Discovery**.
   You can click Save at any time to save the current status of the operation.
   The specified AppDynamics APM Integration application is discovered. If scheduled discovery was specified (defaults to *Enable*), it begins as specified in the *Discovery Time and Frequency* section, similar to existing integrations.
   After you create an application, you can drill down into it to see topology, application components, and FC conversations.

Dynatrace APM Integration



The VirtualWisdom AppDynamics APM Integration, ServiceNow, and Dynatrace APM functions all discover running applications in those products and add them to VirtualWisdom. VirtualWisdom uses the applications discovered by the first-executed function (AppDynamics APM Integration, ServiceNow, or Dynatrace APM), and, after the other function executes, conflict resolution and manual reconciliation of differences as seen by VirtualWisdom might be required.

Unmonitored hosts from an application in a Dynatrace instance, continue to be shown in VirtualWisdom. After 72 hours and with the next discovery of the Dynatrace Integration, it re-imports this application. For the host which is marked unmonitored, the Dynatrace API still returns that host, which is the same as it was before it was marked unmonitored.

If a Dynatrace Integration imports two or more applications (A and B) consisting of the same or similar nodes, when integrations such as ServiceNow, Operating System, etc. perform application discovery and provide suggestions, the integrations suggest only for one application (A), not the other similar application (B). When changes are made in Dynatrace for Application(A) and Dynatrace reimports Application(A) (with changes), the suggestions from the integrations are shown on Application(B).

Configuring Dynatrace APM Integration

VirtualWisdom discovers/imports applications directly from either the local or cloud instance of the Dynatrace APM controller, and creates applications only from existing Hosts, VMs, Microsoft Hyper-V VMs, and PowerVM Partitions that have been discovered by other VirtualWisdom integrations.

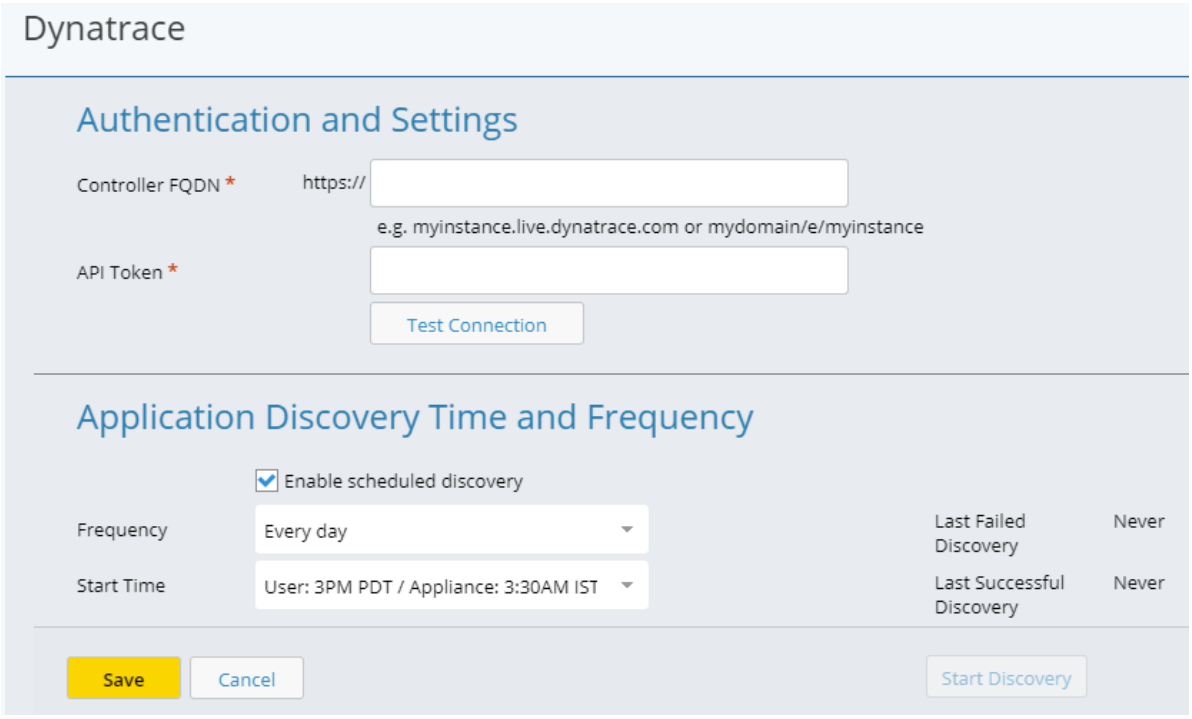
Prerequisites

You must have defined Application patterns in their Dynatrace instance to discover different applications in Dynatrace. This is a prerequisite for the Dynatrace Integration to discover the applications correctly.

You must have disabled Real User Monitoring (RUM) for monitoring with the Dynatrace Integration.

Steps

1. Select an instance of a Dynatrace app (cloud or on-premise) and copy the main Dynatrace URL.
2. From the Settings tab, click **Integrations** in the *Probes and Integrations* section, and then click the **View** button for *Dynatrace APM*.
   The *Dynatrace APM* page is displayed.

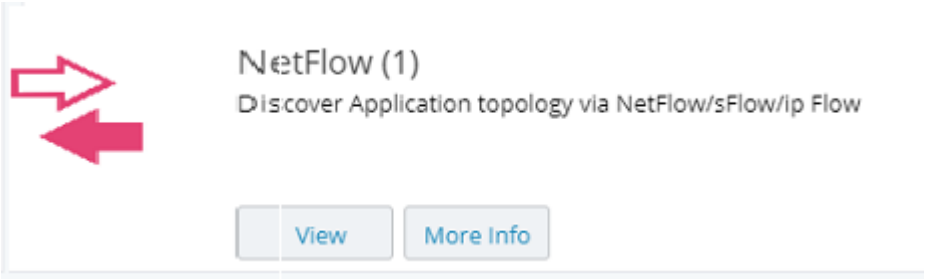


3. Copy and past the main Dynatrace URL into the *Controller FQDN* field.

4. Copy the API Token from Dynatrace site and paste it into API Tokenfield.
   For additional information, see https://www.dynatrace.com.
5. Click **Test Connection** to verify that the specified URL and API Token can connect to the Dynatrace site successfully.
6. Click **Save** and then **Start Discovery**.
   You can click Save at any time to save the current status of the operation.
   The specified Dynatrace application is discovered. If scheduled discovery was specified (defaults to *Enable*), it begins as specified in the *Discovery Time and Frequency* section.

After you create an application, you can drill down into it to see topology, application components, and FC conversations.

NetFlow Integration



The NetFlow Integration captures flow records from NetFlow, sFlow, Jflow, and IPFIX and sends them to the VirtualWisdom appliance.

Use VirtualWisdom to control bandwidth utilization, optimize application performance, and troubleshoot problems. Typical use cases include:

- What bandwidth is being consumed by a particular IP node?
- Who/What is congesting the network? Or, what is the bandwidth usage of specific applications?
- Who is talking to whom?
- Who is using a particular network service?
- What are the top talkers in a subnet?
- Which network services are being used?
- Detects network anomalies (DDoS, SPAM, BotNets, abnormal downloads/uploads, ...)
- Detects impact of hosts on other hosts and correlates to affected applications and storage, via contention analysis
- Predict, prevent, and remediate performance problems via correlation with other data sources, such as the Dell EMC VxFlex OS Integration and NetApp integrations, combined with analytic

An IP flow record provides a summary of the interaction between two IP addresses. The application discovery process uses *Network Conversations* to find/suggest possible applications, and uses a *likely-kind* heuristic analysis to determine possible roles of network endpoints. It provides information to determine:

- How much bandwidth is consumed by a specific IP?
- Who is a network hog?
- Who is talking to whom?
- Who is using a specific network service?
- Who are the top talkers in a subnet?
- Which network services are being used?

Duplicate flows, from redundant sources, can misrepresent the actual amount of traffic reported. Flow deduplication:

- Identifies possible home links for subnets and IPs, collecting information from subscribed routers about their subnets and interfaces, and from vCenter about the virtual distributed switches, their ports and associated IP addresses.
- Monitors live traffic to identify *active* home links for both source and destination IPs
- Requires a *warm-up* period to identify *active* home links.
- Accepts or filters flows based on active home link information
- Reports errors if conflicts are detected (for example, two different routers with the same active home link subnets).

VirtualWisdom Health Notifications are generated, the feature is disabled, and an error is shown on the *Probes and Integrations* page when:

- Errors prevent the feature from being enabled
- The proxy detects an issue
- SNMP credentials are incorrect
- Router inaccessible (direct connectivity between router and VirtualWisdom is required)
- VDS does not have associated vCenter configured in VMware vSphere Integration
- Conflicting home link information
- When issue detected
- Health alert generated
- Feature automatically disabled
- Error shown in Probes and Integrations page

Correct the problem and re-enable feature.

Caveats:

- Feature works only when network topology is relatively static. The network being monitored does **not** use dynamic routing.

- VDS must be associated with a vCenter already configured in VirtualWisdom
- VDS updates linked to VMware vSphere Integration scheduled discovery (not discovery updates)
- Data collected from Level 2 switches is necessarily limited because switch data is routed via MAC address rather than IP address
- Deduplication caveats
  - Recommend configuring VMware vSphere Integration *before* enabling duplication detection
  - Deduplication is all or nothing: All VDS and all router source types must be properly configured in NetFlow and vCenter or deduplication fails
  - The source type (router or VDS) must be correctly set and subscribed in VirtualWisdom
  - Each subscribed "Router" type flow source must have router SNMP configured; each subscribed "VDS" type flow source must be configured in vCenter
  - The IP addresses in NetFlow and vCenter for VDS must match. If not, the VDS shows up as “not found” under the VDS vCenter column in the NetFlow integration and deduplication fails

Sampling rate determination:

Global Sampling Rate should be set as low as possible, as long as flow data can still be processed in a timely manner.

- If the rate is set too low, flow processing might not be able to keep up, too high a load might be generated on the box, and some data might get dropped. Increase the rate, and NetFlow Integration looks for indications that the flow processor is struggling to keep up. If detected, a health alert is generated, recommending a specific global sampling rate increase.
- If the rate is set too high, sampling requires NetFlow Integration to fill in the gaps, and accuracy might suffer. Decrease the rate, and NetFlow Integration tracks incoming flow rates versus expected flow processing capacity. If the Global Sampling Rate can be safely lowered, a health alert is generated, recommending a specific global sampling rate decrease.

You can create a Network Usage Rate alarm rule with specific thresholds described by:

- Incoming and/or Outgoing traffic
- Bitrate or Packetrate

The rule applies to entity types with NetFlow metrics, and the case shows trend chart of specified metrics and corresponding thresholds.

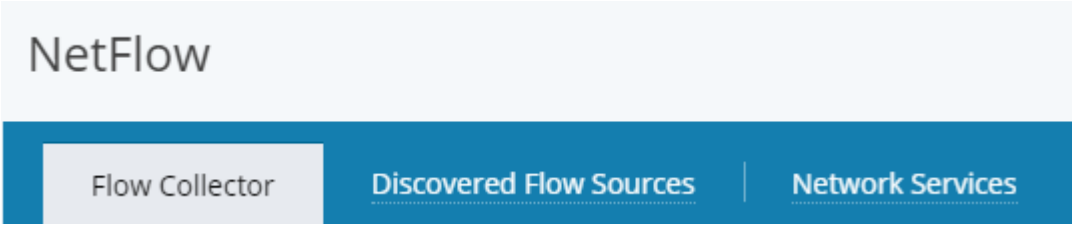
- Click **Settings**, then *Integrations* in the *Probes and Integrations* section, and then the **View** button for *NetFlow Integration*.

The *NetFlow Integration* page is displayed, consisting of three tabs:

- Flow Collector
- Discovered Flow Sources
- Network Services

Flow Collector

This tab specifies the IP address and port number, scheduled discovery, and limits the scope of flow source discovery.



1. Specify an *Interface* (IP address) and *Port* number.
   Flow source discovery time/frequency are enabled by default.
2. To specify in the *Discovering Entities* area which subnets to *Monitor* and *Not Monitor*, click **Add** to enter the IP address and mask for each subnet.
3. In the *Entity Discovery Thresholds* section, enter the minimum numbers of Packets/Second and Bits/Second for *Network Conversations* entity discovery.
4. Click **Save** and then **Start Discovery**.
   You can click Save at any time to save the current status of the operation.
5. Select individual or multiple subnets and click **Subscribe/Unsubscribe**.

Discovered Flow Sources

This tab subscribes to flow sources to discover *IP Addresses*, *Network Services*, and *Network Conversations*. If the Sampling Rate is not displayed, specify a rate based on the flow source configuration. The default global sampling rate is 1.

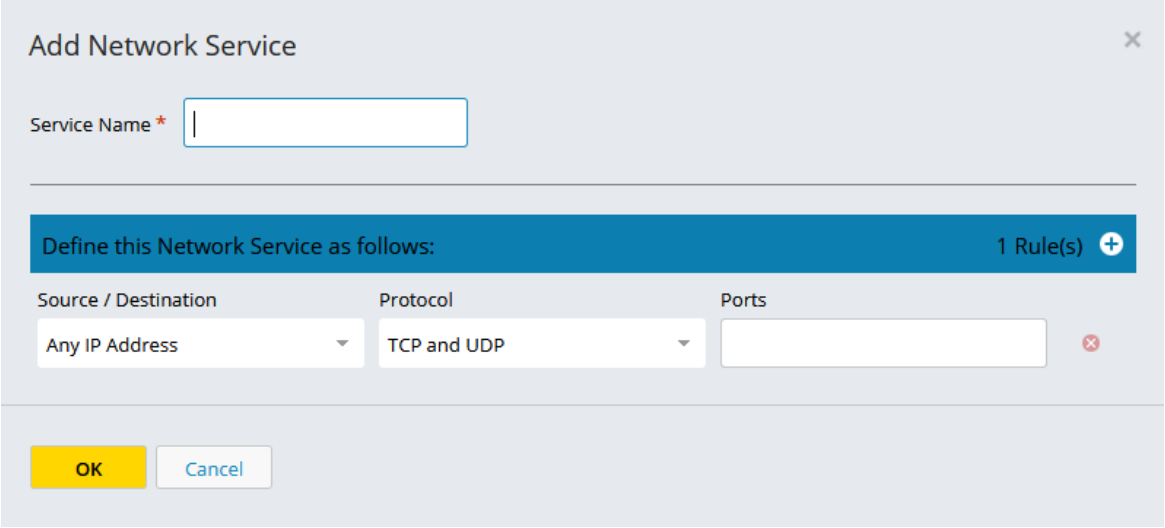
1. Select one or more source IP addresses.
2. To *Detect Duplicate Flows*, click the checkbox (off by default).
   Duplicate flows, from redundant sources, can misrepresent the actual amount of traffic reported. Deduplication requires SNMP access to all subscribed routers, and all subscribed vDSs must be linked to a vCenter via the vCenter Integration.
3. You can click **Save** at any time to save the current status of the operation.
4. Click **Save** and then **Start Discovery**.
   You can click Save at any time to save the current status of the operation.

5. Select individual, multiple, or all source IP addresses and click **Subscribe/Unsubscribe**.

Network Services

This tab lists network services.

1. Click **Add** to add a network service.
   Add Network Service displays.



2. Specify *Service Name*, *Source/Destination*, *Protocol*, and *Ports*.
3. Click **OK**.
4. Click the **+** to create additional rules, specify the new information, and click **OK**.
5. Click **Save** and then **Start Discovery**.
   You can click Save at any time to save the current status of the operation.
6. Select individual, multiple, or all network services and click **Subscribe/Unsubscribe**.

Virtana Platform Connectivity

The VirtualWisdom Migration Analysis analytic has the ability to connect directly to Virtana Platform in order to transfer data.

To establish access between VirtualWisdom and Virtana Platform, you must have the Client ID and Client Secret for the organization in Virtana Platform to which you are connecting. After generating a set of unique credentials in Virtana Platform, you must enter the credentials in VirtualWisdom.

OAuth credentials are generated for the Virtana Platform organization under which you logged in and are unique to that organization.

Prerequisites

You must have *administrator privileges* in both Virtana Platform and VirtualWisdom to perform this task.

Your Virtana Platform account must be configured with a supported cloud provider instance.

The organization to which you want to upload the VirtualWisdom metrics must already exist in Virtana Platform.

Steps

1. In *Virtana Platform*, ensure you are logged in to the organization you want to connect to.
2. Navigate to **Settings > Integrations > Virtana Platform API**.
3. Click **Generate OAuth Client Credentials**.
   Unique credentials are displayed for your organization.
   You must copy these credentials and enter them in VirtualWisdom.
4. In *VirtualWisdom*, navigate to **Settings > Probes and Integrations > Connect to Virtana Platform** and do one of the following:
   - If no connection yet exists to a Virtana Platform organization:
     a. Provide the OAuth 2.0 **Client ID** and **Client Secret** for the target organization in Virtana Platform.
     b. Click **Validate & Connect**.
        A confirmation message displays when the connection succeeds.
   - If a connection already exists to a Virtana Platform organization:
     a. Click **Connect to a different organization**.
     b. Provide the OAuth 2.0 **Client ID** and **Client Secret** for the target organization in Virtana Platform.
     c. Click **Validate & Connect**.
        A confirmation message displays when the connection succeeds.
5. To revoke credentials, return to the Virtana Platform API tab and click **Revoke Credentials**l.

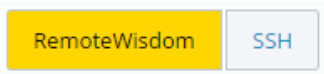
Chapter 2

Remote Access

Remote access to VirtualWisdom allows Virtana Support personnel to troubleshoot issues with VirtualWisdom hardware and software.

There are two methods of accessing VirtualWisdom remotely: RemoteWisdom and Secure Shell (SSH) access. Both are enabled by default.

Configuring RemoteWisdom



RemoteWisdom enhances the ability of Virtana Support personnel to diagnose and solve issues with VirtualWisdom hardware and software. RemoteWisdom is enabled by default, and Virtana recommends that you leave it enabled.

NOTE

RemoteWisdom is enabled by default and starts working when the Appliance boots. If you have security concerns regarding RemoteWisdom, you can disable RemoteWisdom using the Configuration Wizard or the Settings tab from the VirtualWisdom UI.

NOTE

For RemoteWisdom connectivity to succeed, the VirtualWisdom Appliance will need to be able to communicate with virtualinstruments.axeda.com and at least one of the other external IP addresses shown below.

Hostname	IP Address
virtualinstruments.axeda.com	40.121.152.116
ghuk2.axeda.com	52.56.106.12
ghuk3.axeda.com	52.56.113.192
ghsj1.axeda.com	52.8.82.253
ghsom1.axeda.com	209.202.157.179

Configuring RemoteWisdom

1. From the *Settings* tab, click **Remote Access**.
   The **RemoteWisdom** page is displayed.
2. RemoteWisdom is enabled by default and is indicated by a check in the **Enable RemoteWisdom feature** for this product check box. If this check box is checked, you can optionally specify the HTTP proxy or SOCKS host information on the page.
   Also optionally, verify your login credentials.
   By default, RemoteWisdom users are given access to the VirtualWisdom UI. To disable this feature, uncheck the Enable RemoteWisdom access to the VirtualWisdom UI.
   To disable RemoteWisdom, deselect the **Enable RemoteWisdom feature for this product** check box.

3. Click **Test Connection** to verify your RemoteWisdom connection. Assuming that you have entered valid information, the *Info* dialog box displays.
4. Click **Ok** to return to the RemoteWisdom page.
5. Click **Save.**
   You receive a message that the **Remote proxy settings have saved successfully**.
6. Click **OK** to return to the RemoteWisdom page.
7. Click **Close** to return to the Settings tab.

Disabling SSH

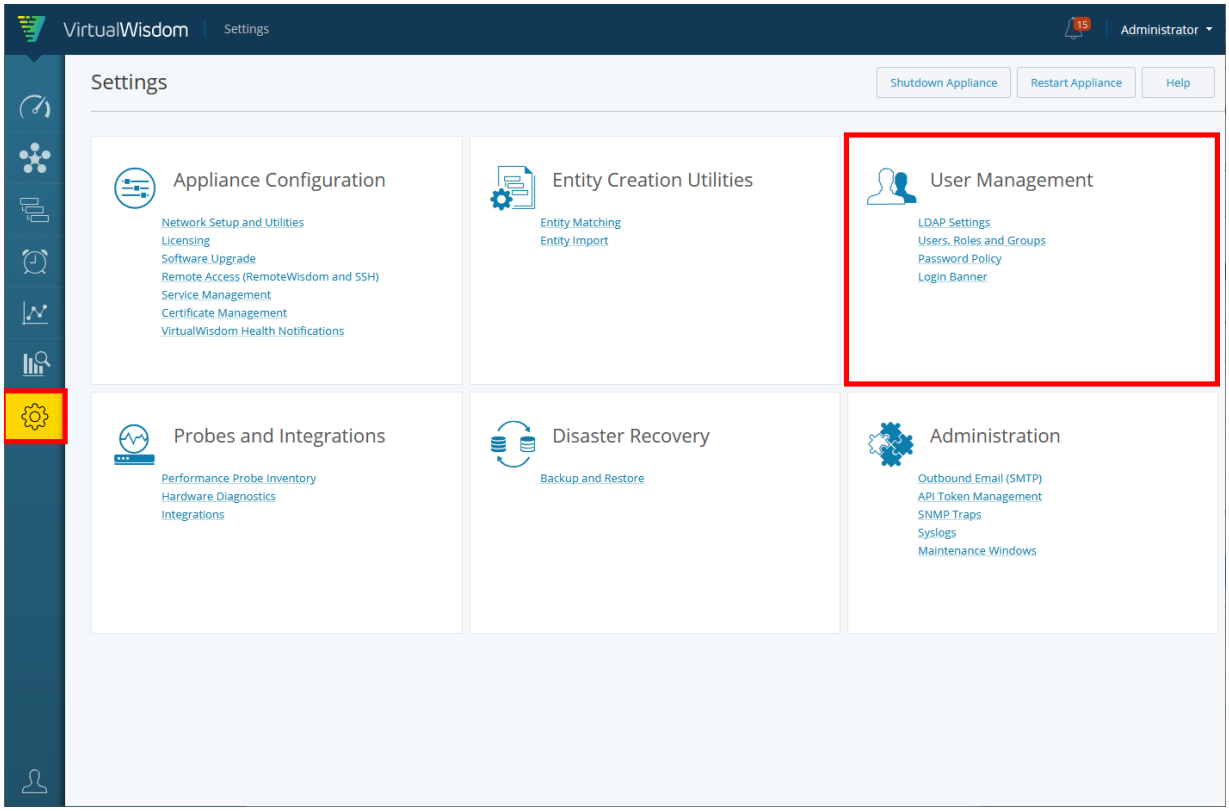
The Appliance supports Secure Shell (SSH) access for use by authorized Virtana personnel when troubleshooting issues. Support for SSH is enabled by default, but you can disable SSH if you prefer.

1. From the **Settings** tab, click **Remote Access**.
   The RemoteWisdom page is displayed.
2. Click **SSH** to access the SSH page.
3. Uncheck the **Enable SSH Access** check box.
4. Click **Save**.
   A confirmation dialog displays.
5. Click **OK** to confirm and return to the *SSH* page.

Chapter 3

User Management

The User Management function is found on the **Settings** tab.



From this page, you can configure **LDAP settings [116]** , manage **Users, Roles and Groups**, configure the **Password Policy [129]** for the portal, and change the **banner [203]** displayed on the portal's login page.

LDAP Settings

VirtualWisdom supports LDAP and local users. Before an LDAP user can access VirtualWisdom, you first need to configure the LDAP server settings.

Configure LDAP Server Settings

1. From the **Settings** page, click **LDAP Settings** to access the LDAP Settings page. The LDAP Settings page is displayed.
2. Edit the following information in the LDAP Setting page:

Table 19. LDAP Settings Parameters

Settings	Parameter	Definition
Connection	Name	User-defined name for the LDAP server. Required.
	Hostname	IP address or hostname of the LDAP server. If digest-MD5 or cram-MD5 is being used, Hostname has to be a DNS name, not IP address. Required.
	Port	LDAP port number, this field is automatically completed when the *Auth Method* is selected. You can override the default port after selecting the *Auth Method*. Required.
	Search Base	Starting point for the LDAP search in the directory tree. Required.
	Auth Method	Choose one of the following LDAP authentication methods: none, simple, digest-MD5, and cram-MD5. Required.
	Realm	Realm is required when both MD5 and multiple domains are used. Otherwise, leave field blank. Only one realm is supported.
	Username	Username, that has suitable permissions to query the LDAP server.
	Password	Password for *Username*.
	Use SSL Check box	Use SSL when this check box is checked.
	Certificate File	Upload a certificate in Base64 encoding for LDAP using standard upload procedure.
Template	Template	Choose Active Directory, Generic LDAP Server, or Posix.
User Mapping	Base DN	Base DN that contains user entries. Base DN is concatenated to prefix of Search Base, for example, if Base DN "ou=people" and Search Base is "dc=vi,dc=com", the application tries to find user under "ou=people,dc=vi,dc=com".
	Object Class	Default value depends on what template user selects: For Active Directory: “sAMAccountName”, for Generic LDAP Server : “inetOrgPerson” and for Posix : “posixAccount”.
	User ID Attribute	Supplies the User ID.
	Real Name Attribute	Supplies the real name of the user.

Settings	Parameter	Definition
	Email Attribute	Supplies the email address of the user.
Group Mapping	Base DN	Base DN that contains group entries. Base DN is concatenated to prefix of Search Base, for example, if Base DN "ou=people" and Search Base is "dc=vi,dc=com", the application tries to find group under "ou=people,dc=vi,dc=com".
	Object Class	Default value depends on what template user selects: for Active Directory : “group”, for generic LDAP Server : “organizationalUnit”, for Posix : “posixGroup”.
	Real Name Attribute	Supplies the real name of the group.
Membership Schema	Group Membership Attribute	Attribute name of the group entity of the LDAP server that defines the users belong to it. The default value is "memberUid" for Posix, and "member" for all others.
	User Membership Attribute	Attribute name of the user entity of the LDAP server that defines the groups to which it belongs. The default value is "memberOf".

3. Use the **Authenticate** button to verify the test settings.
4. Click the **Save** button to verify and save the settings.
   You are returned to the Settings page.

User Roles and Privileges

VirtualWisdom users role-based access control. Every user is assigned a specified role when their account is created.

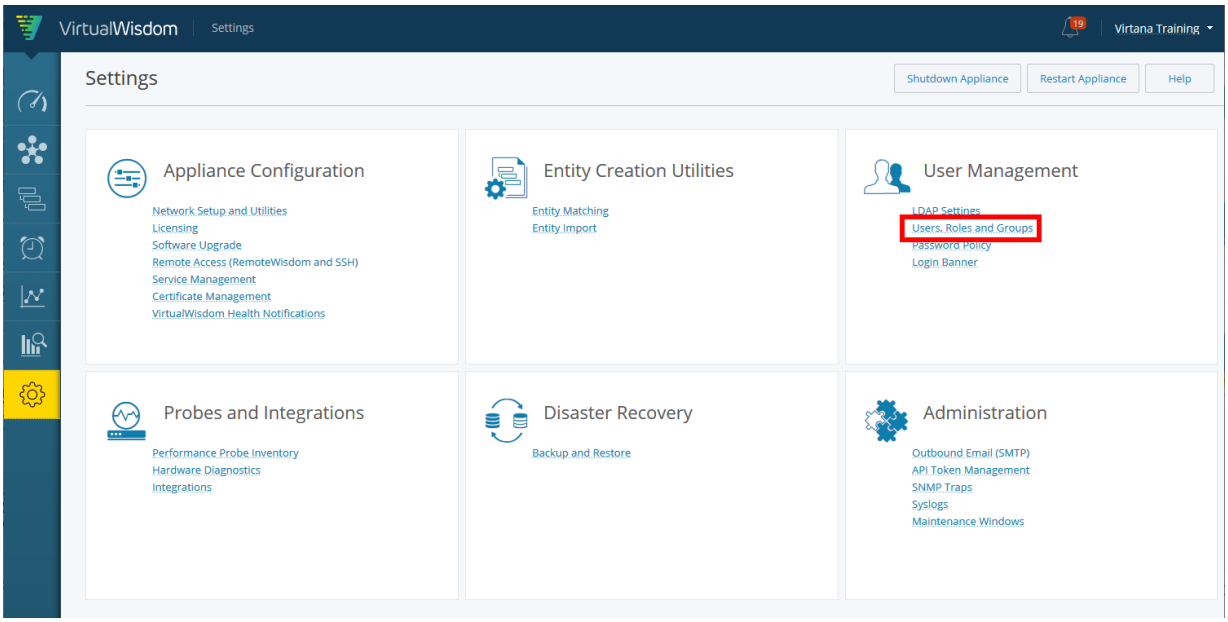
Table 20. Default VirtualWisdom Roles

Role	Definition
vw-admin	Provides full access to the VirtualWisdom user interface, including tasks on the Settings tab.
vw-user	Provides access to the VirtualWisdom UI, excluding access to tasks on the Settings tab. All individual reports must be shared with the vw-user role user by an administrator.

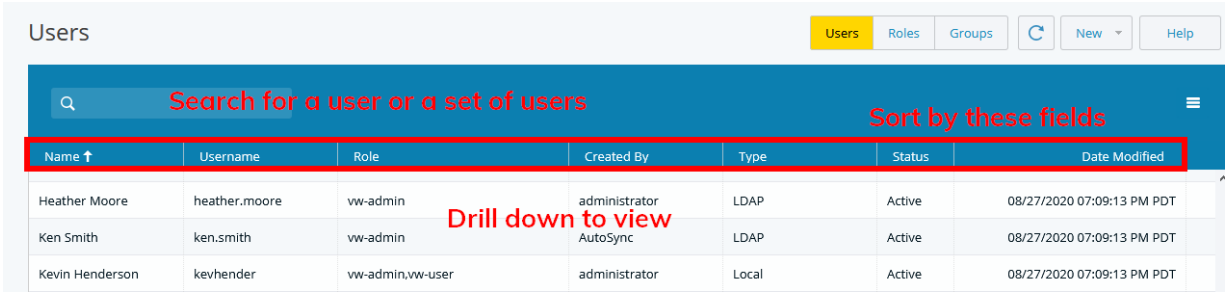
Role	Definition
vw-readonly	Provides the same access to the VirtualWisdom user interface as the vw-user role, but with read-only access. A user assigned the vw-readonly role can view and interact with a topology, but cannot create a report or chart. If a report was shared with them, they are able to view it but not modify it.

User Account Management

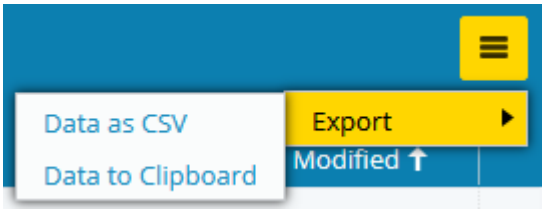
To view and manage user accounts, select Users, Roles and Groups from the **User Management** section on the **Settings** page.



A list of users is displayed using a list view. You can use the search field to find a user or a set of users. You can also sort by any column.



To export the user list, click on the hamburger icon, then select **Export**. You can download the user list as a CSV file or copy the data to the clipboard.

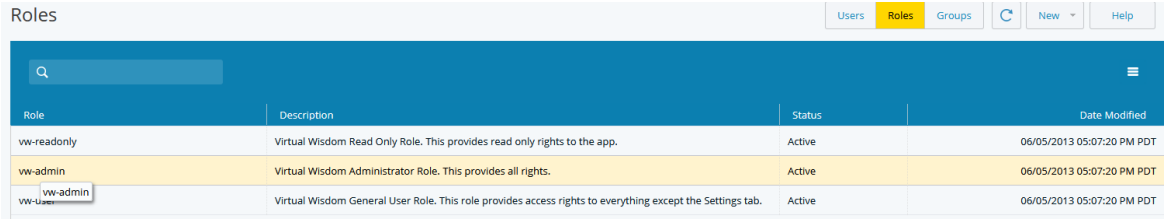


View Users by Roles

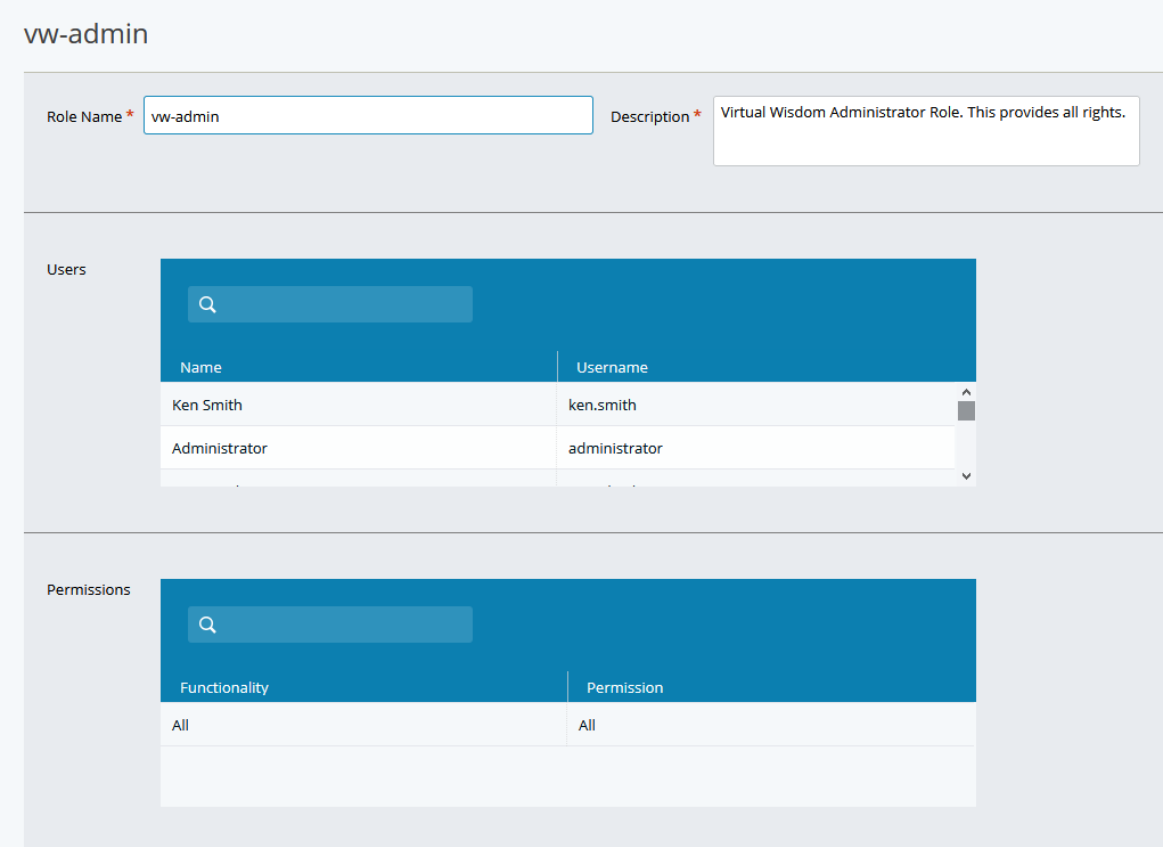
Follow these steps to view the users associated with a specific VirtualWisdom role:

1. From the **Settings** screen, click **User Management** to access the **User Management** screen.
   The **Users** list displays.
2. Click the **Roles** button.

   The **Roles** page displays. This page contains a list of the VirtualWisdom roles: `vw-user`, `vw-readonly`, and `vw-admin`, as well as the associated Description, Status, and Date Modified for each role.



3. Click the role that you want to view.
   A window with information regarding the selected role, including the Role Name, Description, Users, and Permissions. The Role Name, Description, and Permissions are not modifiable.
   The information reflected in the Users field shows the Name and Username of all users with the selected role.

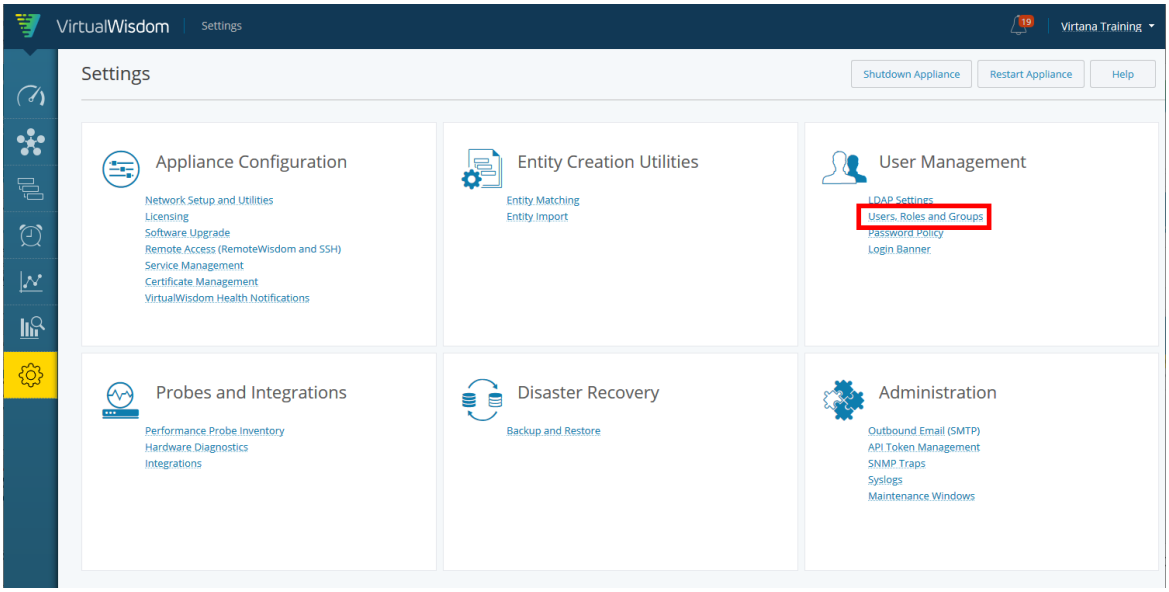


Create a User

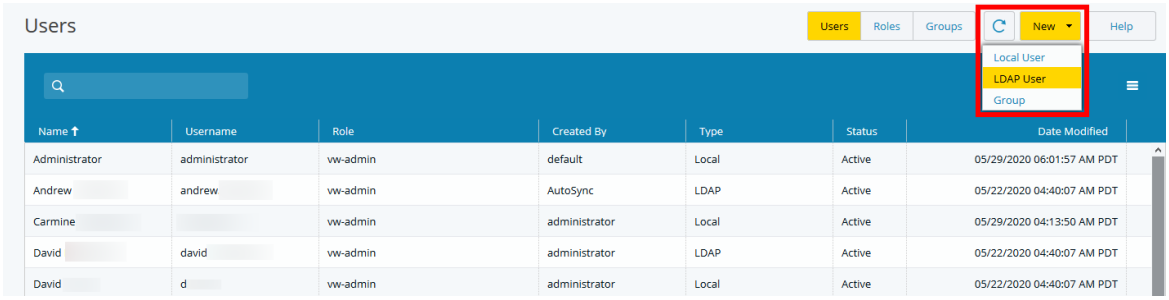
You can create local or LDAP user accounts.

Creating a New Local or LDAP User Account

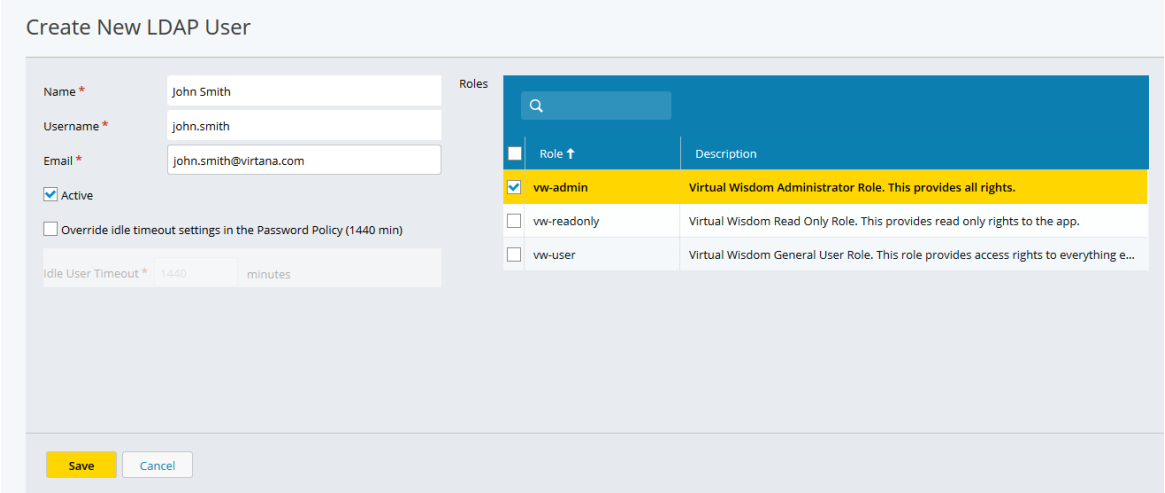
1. From the Settings page, select **User Management**, then **User Roles and Groups**.



2. Select **New**, and then select **Local User** or **LDAP User** from the drop-down menu. Depending on your selection the **Create New Local User** or the **Create New LDAP User** page is displayed.



3. Enter the user's information, select a role, then click Save.
LDAP user information is auto-populated from the client's LDAP account as soon as you start to enter the name, email, or username of the LDAP user.



NOTE
Usernames are case-sensitive.

By selecting “Override idle timeout settings...”, an administrator can override the Idle User Timeout value that is set in the Password Policy.

Verifying the New Local or LDAP User

1. Click the arrow where the current logged-in username is displayed and select Sign Out (from the drop-down menu) to log out of the Administrator account.
   You are returned to the login page.
2. Use the newly created username and password for the account that you just created.
   You are now logged in as the new user.

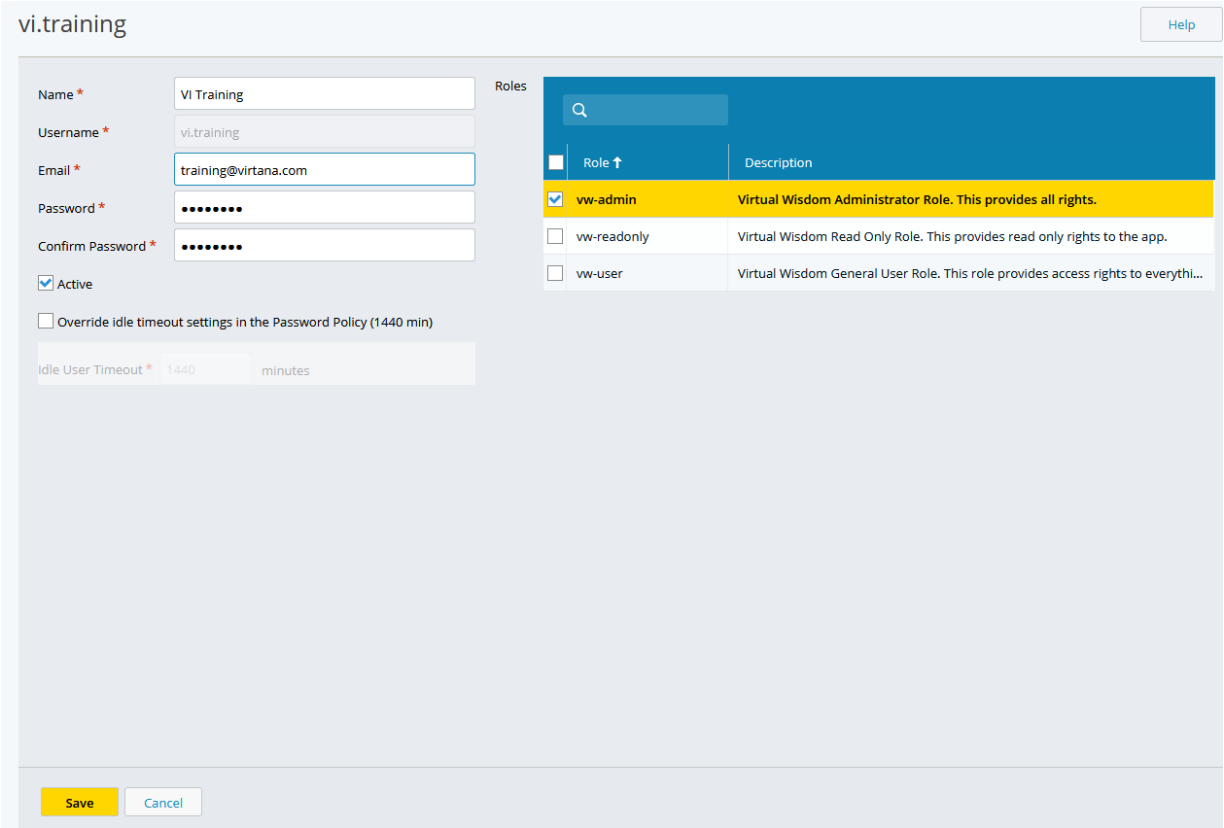
NOTE
If you attempt to log in to VirtualWisdom three times with incorrect login/password credentials, you need to complete a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) challenge-response test to log in to VirtualWisdom.

Edit, Deactivate, or Delete a User

Use the **User** page to edit, deactivate, or delete a user's account.

Editing a User's Account

You can change the user's name, email address, password, idle timeout settings, and role. Make your changes then click **Save**.

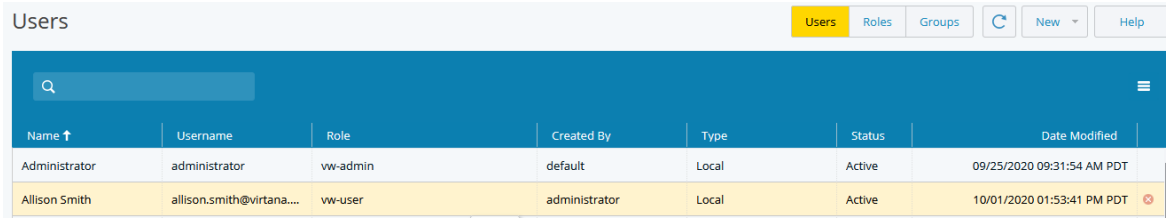


NOTE
The **username** cannot be edited.

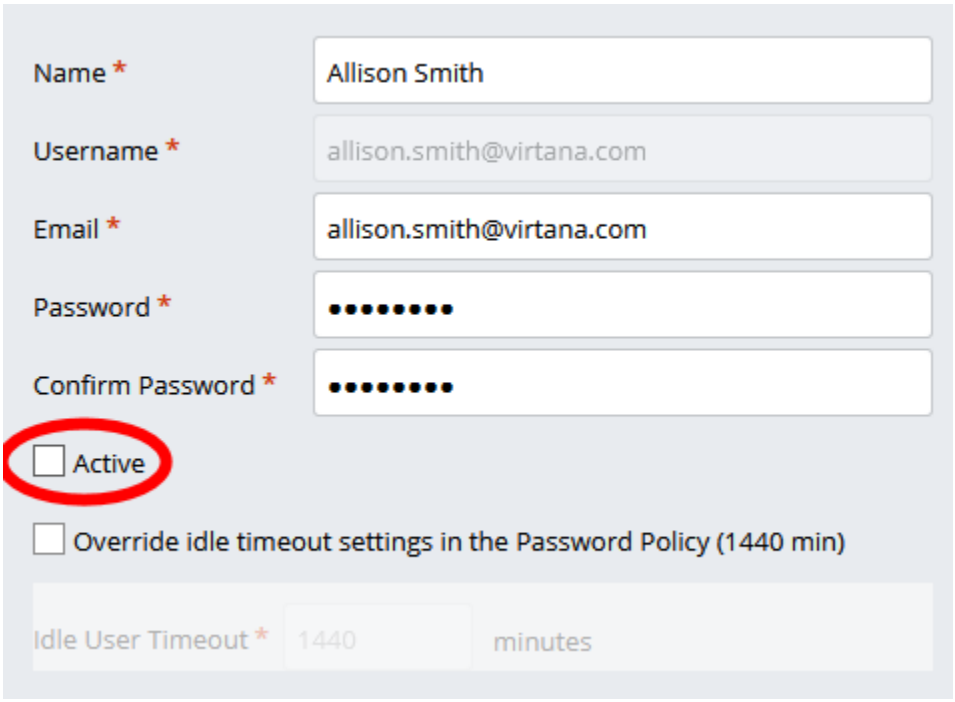
Deactivating a User

You can deactivate a user's account while retaining it in the portal's account list. This can be used to temporarily restrict access by a user.

1. From **Settings** > **User Management**, select **Users, Roles and Groups**.
2. From the list, click on the user account you want to deactivate.



3. Uncheck the **Active** box and click **Save**.

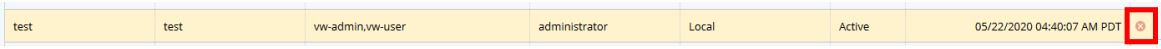


The user account is deactivated and the user is no longer allowed to log in to the portal.

Deleting a User

In some cases, you may want to delete a user's account completely.

- From Users page, select a user from the list and click the x to delete their account.



The user account is deleted from the portal.

User Groups

A User Group (Group) is a collection of LDAP and/or Local users, and LDAP groups.

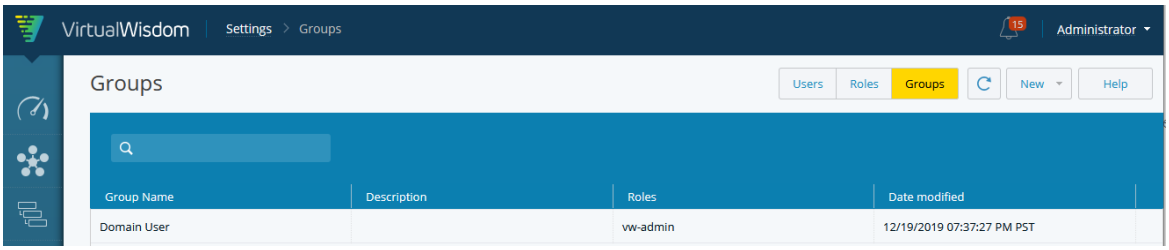
Groups specify special VirtualWisdom access for users in the group, such as the ability to login or the ability to share reports, analytics, and topology. Groups have roles, as users do. An advantage of using groups is that you can create a Group (consisting of multiple users and LDAP groups), rather than creating each user separately.

Local users and LDAP groups/users are displayed in separate lists, each list has its own search, and the complete list of groups/users is displayed. You can customize the filter string by defining your own wildcards. The filter string minimum for LDAP Groups (default value = 0):

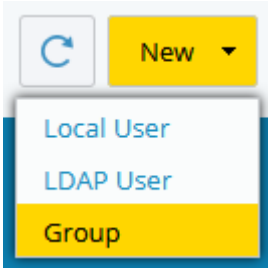
com.vi.service.security.min_group_pattern_length

User Group Creation, Editing, and Deletion

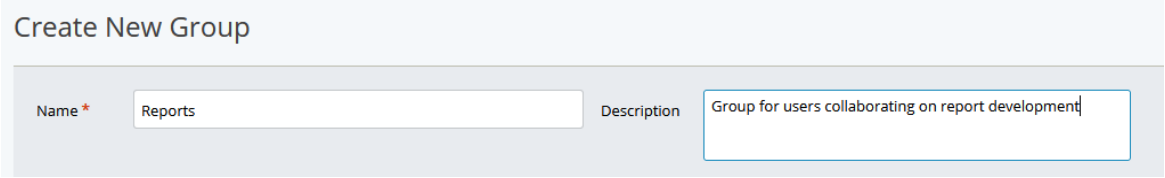
1. From the **Settings** tab, click **User Management** to access the **Users** page.
   The **Users** list displays.
2. Click **Groups**.
   The **Groups** page displays the names of all configured VirtualWisdom Groups, their associated description, roles, and the date and time that the group was created or last modified.



3. Click **New**, and select **Group** from the drop-down menu.

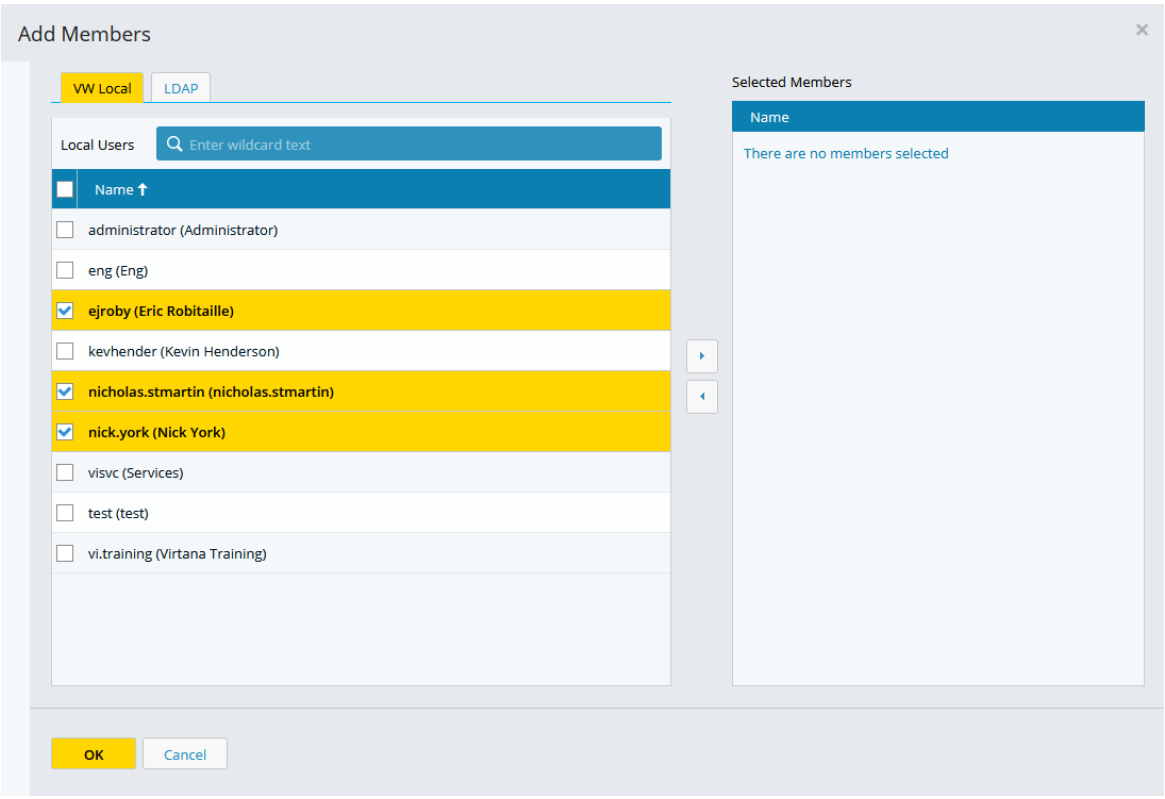


   The **Create New Group** page displays.
4. Enter values for the Group Name and Description.

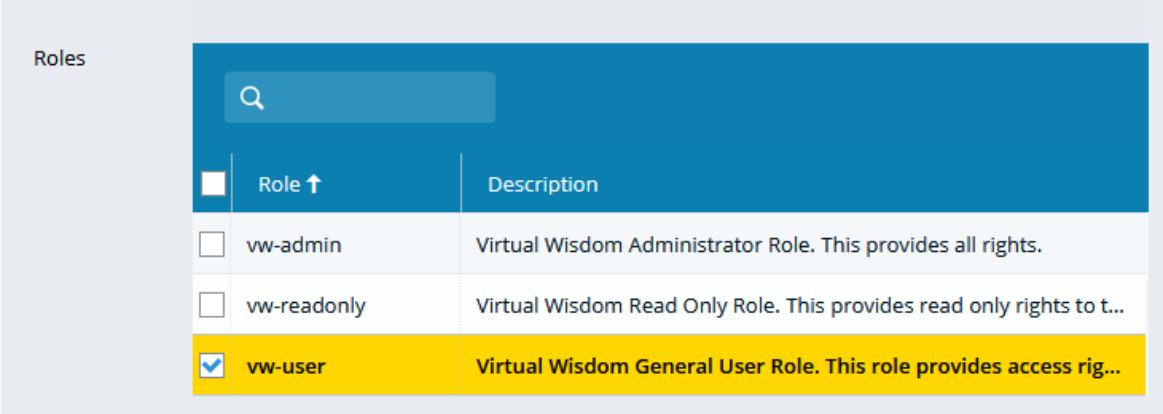


Field	Definition
Name	User-defined name of the Group.Group names are case sensitive.
Description	User-defined description of the Group.

5. Click **Add** to add members to the Group.
   The **Add Members** dialog displays with a tab for VW Local and a tab for LDAP.
6. Select the checkboxes for the users in the **Name** column and move the users to the **Selected Members** column.
   The specified users are grayed out in the source box.



7. Click **OK**.
   You return to the **Create New Group** page.
8. Choose a role for the Group by checking the appropriate check box.



The roles definitions are as follows:

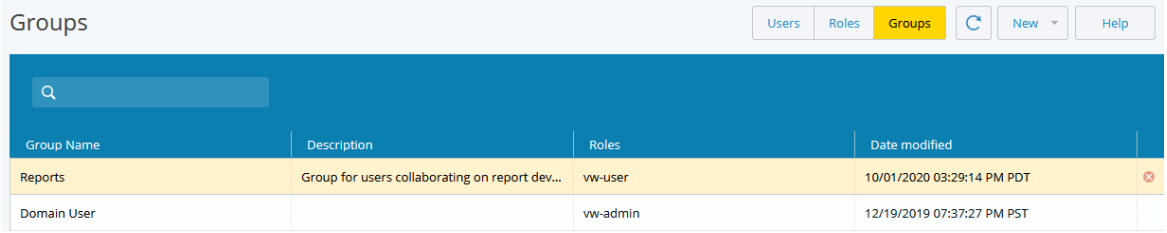
Table 21. Default VirtualWisdom Roles

Role	Definition
vw-admin	Provides full access to the VirtualWisdom user interface, including tasks on the Settings tab.
vw-user	Provides access to the VirtualWisdom UI, excluding access to tasks on the Settings tab. All individual reports must be shared with the vw-user role user by an administrator.
vw-readonly	Provides the same access to the VirtualWisdom user interface as the vw-user role, but with read-only access. A user assigned the vw-readonly role can view and interact with a topology, but cannot create a report or chart. If a report was shared with them, they are able to view it but not modify it.

9. Add one or more email addresses in the **Email To Group** field.

TIP
Enter addresses as a comma- or space-separated list.

10. Click **Save**.
You return to the **User Management Groups** page, and your newly created group is now listed in the **Groups** list.

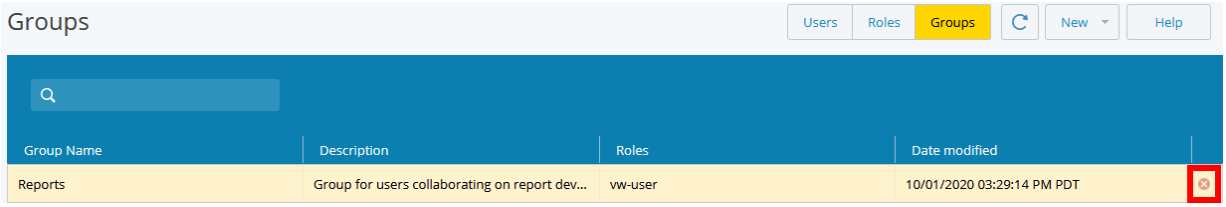


Edit a User Group

You can return to the **User Group** page to edit a user group, and remove or add members.

Delete a User Group

To delete a user group, click the x in the user group's row on the **User Groups** page. This removes the group from the portal. Any permissions that were set up using the group are removed.



Password Policy

VirtualWisdom provides parameters to control your password policy. You can choose from the following options:

Table 22. Password Policy Settings

Setting	Description
Password length	Minimum password length: 1 - 15 characters
Password repetition	Whether passwords must be different from previous passwords: 1-5 previous passwords
Require uppercase letter	Whether at least one uppercase character is required
Require lowercase letter	Whether at least one lowercase character is required
Require numeric character	Whether at least one numeric character is required

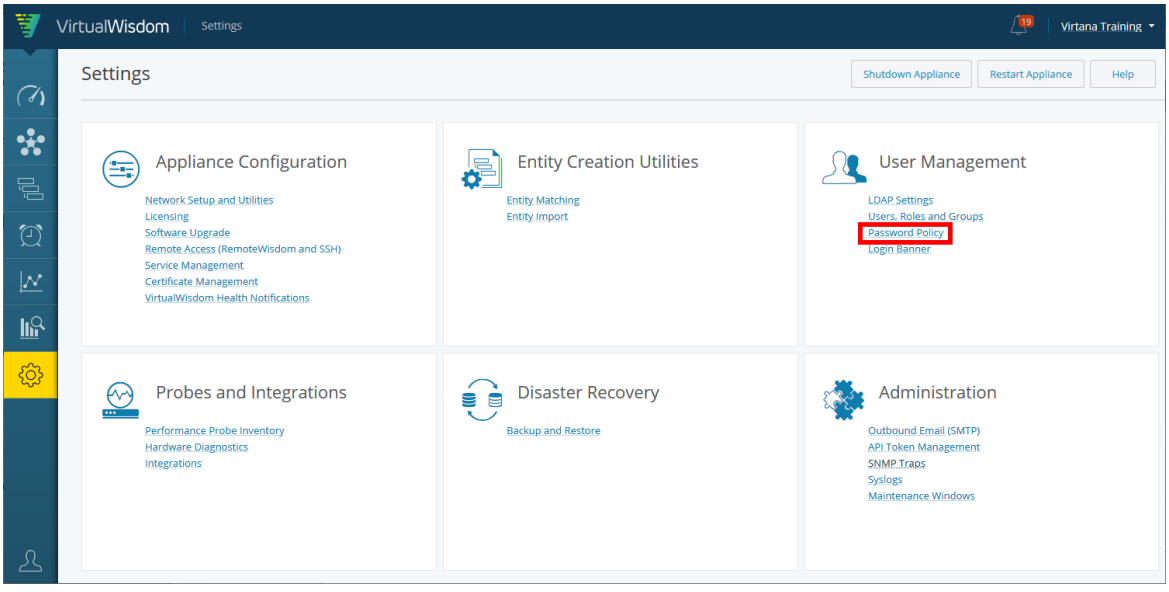
Setting	Description
Require special character	Whether at least one special character is required
Password expiry	Password expiration: 1-24 months
Limit failed login attempts	Limit number of failed login attempts: 2-5 attempts
Idle User Timeout	Inactivity logout time (idle user timeout): 6-1440 min An administrator can override this setting for any user from Settings > User Management > Users, Roles and Groups.

NOTE

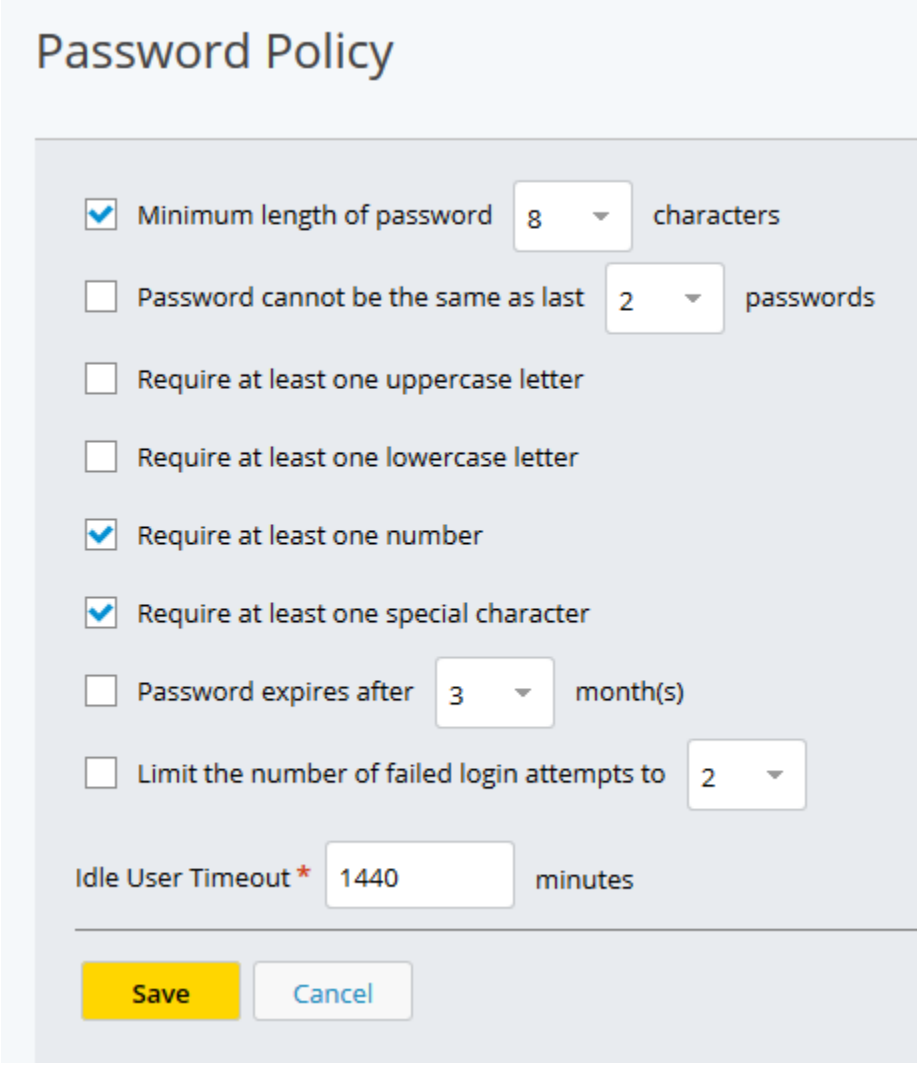
VirtualWisdom Password Policy configuration can be lost after a restore operation. This can cause the Management UI to fail to authenticate and display a blank gray screen. After performing a restore, reconfigure the Password Policy from the VirtualWisdom Settings screen. Be sure to save it, even if it already looks correct.

Specify a Password Policy

1. From the Settings tab, click **Password Policy** under the User Management section.



2. Choose your preferred settings and click **Save**.

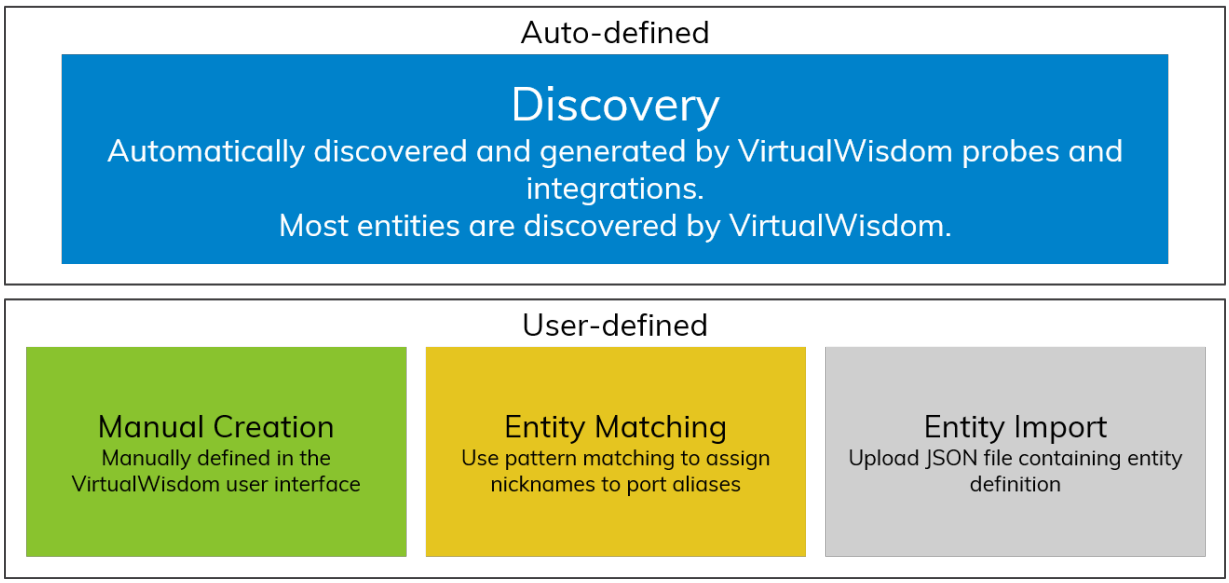

Password Policy
Minimum length of password 8 characters
Password cannot be the same as last 2 passwords
Require at least one uppercase letter
Require at least one lowercase letter
Require at least one number
Require at least one special character
Password expires after 3 month(s)
Limit the number of failed login attempts to 2
Idle User Timeout * 1440 minutes
Save
Cancel

Chapter 4

Entity Creation

How are entities created?

Most entities are automatically created by VirtualWisdom when new infrastructure is discovered by VirtualWisdom's probes and integrations. This is called auto-defined or auto-discovery entity creation.



Entities can also be defined manually through the VirtualWisdom user interface using one of three methods:

1. **Manual Creation:** The user creates each entity with the entity management feature in the VirtualWisdom user interface. User Defined Entities allow the VirtualWisdom user to organize their environment and the collected metrics in a fashion that is familiar to them, for example, by Host, Application, or Storage Array.
2. **Entity Matching:** Entity Matching is a feature that allows the user to assign a meaningful nickname to discovered port Entities. Pattern matching is applied against port alias values based on a nickname scheme to streamline what would otherwise be a tedious process.
3. **Entity Import:** Entities can also be imported using a JavaScript Object Notation (JSON) file. JSON is an open standard format that uses human-readable text to transmit data between a server and a web application.

IMPORTANT

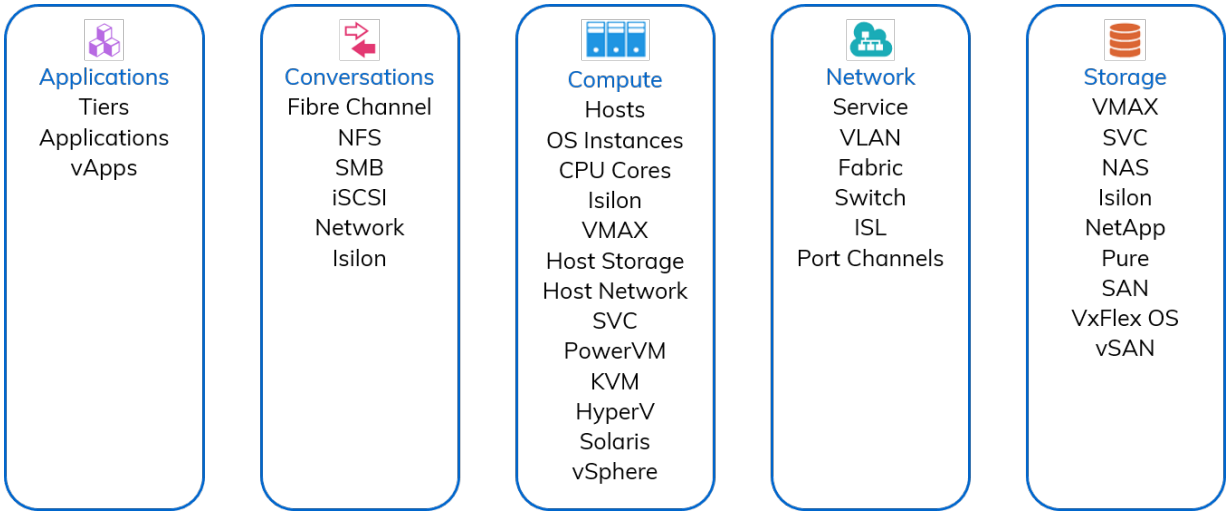
Beginning in VirtualWisdom 6.7, a limit has been placed on the number of conversation entities that VirtualWisdom stores for ProbeFC, ProbeNAS, and NetFlow.

If the system limit of the number of conversations is reached, the least-recently-seen conversations are automatically deleted.

Deletion of these entities is intended to increase performance and reliability for long-running deployments. If you wish to modify or disable this feature, contact VirtualWisdom Support.

Entity Overview

What is an entity?



The entity is the fundamental and most atomic element in VirtualWisdom. Entities allow VirtualWisdom to group resources based on their function, correlation, and inter-dependencies. Entities are logical groupings of the physical and virtual components of your infrastructure and include all the infrastructure components monitored by VirtualWisdom.

Entities can be linked to other entities. The VirtualWisdom user can build groups of entities to display the end-to-end infrastructure of an application in a meaningful fashion in the VirtualWisdom software.

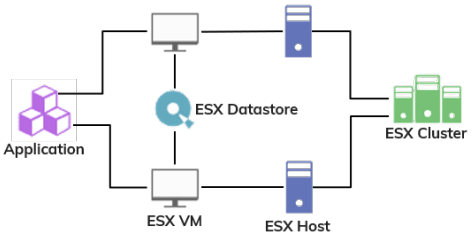
All entities have associated metrics with built-in aggregation rules for each metric type. The metrics, which measure the data flow in the environment, are collected, accessed and analyzed through Entities. Data can be viewed in the context of hosts, arrays and applications, for example, the top 10 hosts in an application.

The VirtualWisdom software is entity-centric. Entities are used to view topology, set alarm rules, create reports, and run analytics.

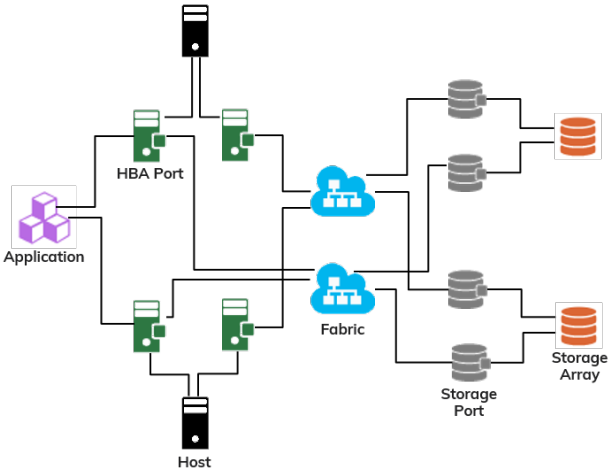
The Value of Entities

Entities provide visibility into the end-to-end infrastructure supporting your application. In the image below, we see two application-centric views of the infrastructure supporting an application: the VMware infrastructure and the fibre channel infrastructure.

Application – VMware Infrastructure

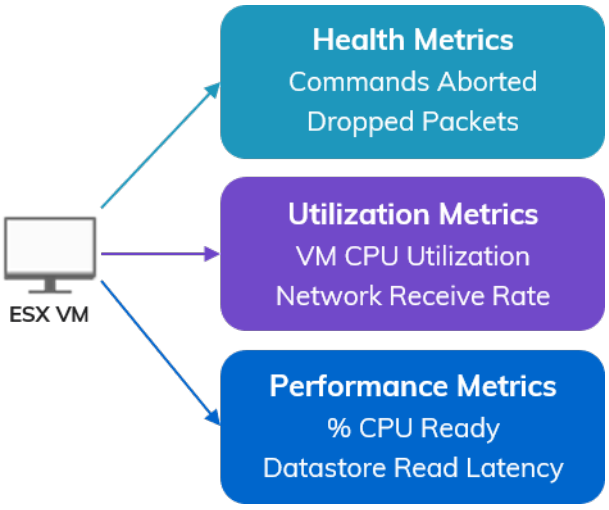


Application – Fibre Channel Infrastructure



Entities are also associated with collected metrics and use built-in aggregation rules to enable:

- Reporting - "What are the top 10 ESX VMs by VM CPU Utilization for an ESX cluster?"
- Alerting - "Alert me when VM CPU Utilization exceeds 95% for the VMs on an ESX cluster?"
- Troubleshooting - "Display events from the last 24 hours where the VM CPU Utilization was high on an ESX cluster."



Entity Types by Category

The Entity Types page displays tables of entity types and their properties. All entity types include the name, tags, and created on properties, plus various additional entity-specific properties.

The following tables list entity types that are included with a standard VirtualWisdom Basic License. Entity types for optional (non-core) integrations are detailed in the relevant Integration User Guide.

Application

Table 23. Entity Types - Applications

Entity Type	Icon	Properties	Created By
Tier		• Application • Application Count • Created On • Discovered Name • Entity Type • External ID • Name • Rank • Tags • Tier Key • VW UID	User or Discovery
Application		• Conflict Key • Created On • Entity Type • Name • Number of Hosts not Imported • Tags • Tier • Tier Id • Unread • VW UID	User or Discovery

Entity Type	Icon	Properties	Created By
vApp		• Annotation • Child vApps • Created On • Discovered Name • Entity Type • Inventory Path • Name • Overall Status • Owner • Parent vApp • Tags • VW UID • Virtual Machines	Discovery

Compute

Table 24. Entity Types - Compute

Sub-Category	Entity Type	Icon	Properties	Created By
Hosts	All Host Types		• Created On • Entity Type • Name • Tags • VW UID	
Hosts	Host		• Components • Created On • Domain Name • Entity Type • Last Discovered Role • Name • OS Version • Role • Role Updated By • Tags • VW UID	User or Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Hosts	OS Instance		• Created On • Domain Name • Entity Type • Hypervisor Type • Name • OS Release • OS Type • OS Version • State • Tags • UUID • VW UID	Discovery
Hosts	CPU Core		• Core ID • Created On • Entity Type • Model • Name • OS Instance • Speed (MHz) • Tags • VW UID	Discovery
Host Storage	Volume Group		• Capacity (KB) • Created On • Device Name • Entity Type • Name • OS Instance • Tags • VW UID	Discovery
Host Storage	Logical Volume		• Capacity (KB) • Created On • Device Name • Entity Type • Logical Device Name • Name • OS Instance • Tags • VW UID • Volume Group	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Host Storage	Physical Volume		• Capacity (KB) • Created On • Device Name • Entity Type • Created On • Device Name • Entity Type • Logical Device Name • Name • OS Instance • Storage Device • Tags • VW UID	Discovery
Host Storage	Storage Device		• Capacity(KB) • Created On • Device Name • Entity Type • Logical Device Name • Name • OS Instance • Tags • VW UID	Discovery
Network	HBA Card		• Created On • Driver • ESX Host • Entity Type • Host • Model • Name • Node WWN • Tags • VW UID	User or Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Network	HBA Port		• Attached Ports • Created On • Device Type • Discovered Name • Entity Type • FCID • HBA Card • Host • Is Virtual • Logical Fabric • Name • Nickname • Port Speed • Proxy FC Port • Proxy FCID • Proxy Fabric Name • Tags • VW UID • WWN	Discovery
Network	Virtual Ethernet Port		• Created On • Discovered Name • ESX Host • ESX VM • Entity Type • IP Address • Name • Role • Tags • VW UID	Discovery
Network	Source Ethernet Port		• Created On • DHCPv4 Enabled • DCPv6 Enabled • Device Type • Entity Type • MAC Address • Name • Storage Array • Storage Controller • Storage I/O Module • Tags • VW UID	

Sub-Category	Entity Type	Icon	Properties	Created By
Network	IP Address		• Bonded Network Interface • Created On • Device Type • Domain Name • Entity Type • Ethernet Port • Host • IPv4 Long Value • Name • Network Interface • Prefix Length • Tags • VLAN • VW UID • Value • Version	Discovery
Network	Source IP Address		• Bonded Network Interface • Created On • Device Type • Domain Name • Entity Type • Ethernet Port • Host • IPv4 Long Value • Name • Network Interface • Prefix Length • Tags • VLAN • VW UID • Value • Version	
Network	Network Interface		• Bonded Network Interface • Created On • Entity Type • IP Address • Interface Name • MAC Address • Name • OS Instance • Speed (Mbps) • Status • Tags • VW UID	• Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Network	Bonded Network Interface		• Bonding Mode • Created On • Entity Type • IP Address • Interface Name • MAC Address • Name • OS Instance • Speed (Mbps) • Status • Tags • VW UID	Discovery
IBM PowerVM	PowerVM Host		• Actual Cores • Actual Memory GB • Created On • Current Available Cores • Current Available Memory GB • Deconfigured Cores • Deconfigured Memory GB • Dedicated Cores • Entity Type • Firmware Memory GB • Model • Name • Pending Available Cores • Pending Available Memory GB • Pool Size • Sample Rate • Serial • Status • Tags • Total Cores • Total Memory GB • VW UID • Virtual Processors	Discover

Sub-Category	Entity Type	Icon	Properties	Created By
IBM PowerVM	PowerVM Partition		• Active Memory Expansion Factor • CPU Mode • CPU Pool Maximum • CPU Pool Name • CPU Pool Reserved • CPU Sharing Mode • CPU Uncapped Weight • Components • Created On • Current CPU • Current Memory GB • Current Paging VIOS • Domain Name • Entity Type • IP Address • LPAR Env • Last Discovered Role • Mac address • Maximum CPU • Maximum CPU Entitled Capacity • Maximum Memory GB • Memory Mode • Memory Weight • Minimum CPU • Minimum CPU Entitled Capacity • Minimum Memory GB • Name • OS version • Power VM Host Name • Primary Paging VIOS • Processor Compatibility Mode • RMC state • Role • Role Updated By • Secondary Paging VIOS • Status • Tags • Using NPIV • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
IBM PowerVM	PowerVM VIOS Partition		• Active Memory Expansion Factor • CPU Mode • CPU Pool Maximum • CPU Pool Name • CPU Pool Reserved • CPU Sharing Mode • CPU Uncapped Weight • Created On • Current CPU • Current Memory GB • Current Paging VIOS • Entity Type • IP Address • LPAR Env • Mac address • Maximum CPU • Maximum CPU Entitled Capacity • Maximum Memory GB • Memory Mode • Memory Weight • Minimum CPU • Minimum CPU Entitled Capacity • Minimum Memory GB • Name • OS version • Power VM Host Name • Primary Paging VIOS • Processor Compatibility Mode • RMC state • Secondary Paging VIOS • Status • Tags • VW UID	Discovery
Microsoft Hyper-V	Hyper-V Cluster		• Created On • Discovered Name • Domain Name • Entity Type • Hyper-V Hosts • Name • Tags • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Microsoft Hyper-V	Hyper-V Host		• Created On • Discovered Name • Domain Name • Entity Type • HBA Cards • Hyper Visor Present • Hyper-V Cluster • Hyper-V VMs • Inventory Path • Logical Processors • Name • Power State • Public IP Address • Tags • Total Physical Memory (GB) • VW UID • Version • Windows GUID	Discovery
Microsoft Hyper-V	Hyper-V VM		• Components • Created On • Discovered Name • Domain Name • Entity Type • FC Ports • Hyper-V Host • Inventory Path • Last Discovered Role • Name • OS Version • Power State • Role • Role Updated By • Tags • Total Memory (GB) • VW UID • Virtual CPUs • Windows GUID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Microsoft Hyper-V	Hyper-V VHD		• Created On • Discovered Name • Entity Type • Filename • Hyper-V VM • Name • Tags • VW UID	Discovery
VMware vCenter	ESX Cluster		• Created On • Discovered Name • ESX Hosts • Entity Type • Inventory Path • Name • Tags • VW UID	Discovery
VMware vCenter	ESX Datastore		• CIFS User • Created On • Data Store Type • Discovered Name • Disk Groups • Entity Type • Inventory Path • Is Accessible • NAS Host • NAS Host IP • NAS Mount Path • Name • Overall Status • Tags • VW UID • Virtual Machines	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
VMware vCenter	ESX Host		• CPUMhz • Cache Disks • Capacity Disks • Connection State • Created On • Discovered Name • Disk Groups • ESX Cluster • ESX Datastores • Entity Type • Ethernet Ports • HBA Cards • Hyper-Threading Enabled • Inventory Path • Is Supported Version • Logical Processors • MemorySize • Mounted File Systems • Name • Number of CPU Packages • Overall Status • Power State • Tags • VW UID • Version • Virtual Ethernet Ports • Virtual Machines	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
VMware vCenter	ESX VM		• Capacity • Components • Connection State • Created On • Datastores • Discovered Name • Domain Name • ESX Host • Entity Type • Ethernet Ports • FC Ports • Free Space • Inventory Path • Last Discovered Role • MemorySizeMB • Name • OS Version • Overall Status • Power State • Role • Role Updated By • Tags • VW UID • Virtual CPUs	Discovery

Conversations

NOTE

If you are working on a software VirtualWisdom Edition then only Network Conversations and Isilon Conversations* can be viewed in Inventory. To view other conversation types (FC, NFS, SMB, iSCSI) the VirtualWisdom hardware probes must be installed.

*Requires the Isilon integration to be installed and configured. See the Isilon Integration User Guide for a list of Isilon entities.

Contact Virtana Sales for more information.

Table 25. Entity Types - Conversations

Entity Type	Icon	Properties	Created By
FC Conversation		• Created On • Entity Type • Initiator FCID • Initiator Name • Initiator WWN • LUN • Name • Tags • Target FCID • Target Name • Target WWN • VW UID • initiatorId • targetId	Discovery
NFS Conversation		• Created On • Destination • Entity Type • FSID • Name • Source • Tags • VLANID • VW UID	Discovery

Entity Type	Icon	Properties	Created By
SMB Conversation		• Created On • Destination • Entity Type • Name • Share Name • Source • Tags • VLANID • VW UID	Discovery
ISCSI Conversation		• Created On • Destination • Entity Type • LUN • Name • Source • Tags • VLANID • VW UID	Discovery
Network Conversation		• Created On • Discovered Name • Entity Type • Name • Tags • VW UID	Discovery

Network

Table 26. Entity Types - Network

Sub-Category	Entity Type	Icon	Properties	Created By
IP Network	Ethernet Port		• Created On • DHCPv4 Enabled • DHCPv6 Enabled • Device Type • Entity Type • MAC Address • Name • Storage Array • Storage Controller • Storage I/O Module • Tags • VW UID	
IP Network	Network Service		• Created On • Discovered Name • Entity Type • Name • Tags • VW UID • Version	Discovery
IP Network	VLAN		• Created On • Entity Type • ID • Name • Tags • VW UID	Discovery
Storage Network	Physical Fabric		• Created On • Discovered Name • Entity Type • Name • Tags • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Storage Network	SAN Switch		• Created On • Discovered Name • Entity Type • IP Address • Manufacturer • Model • Name • Physical Fabrics • Serial Number • Tags • VW UID • Version • WWN	Discovery
Storage Network	Switch Blade		• Created On • Discovered Name • Entity Type • Module Number • Name • SAN Switch • Tags • VW UID	Discovery
Storage Network	Switch Port		• Attached ISL Port • Attached Ports • Created On • Device Type • Discovered Name • Entity Type • FCID • Is Virtual • Logical Fabric • Logical Switch • Name • Nickname • Port Speed • Port Type • SAN Switch • Switch Blade • Tags • VW UID • WWN	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
Storage Network	Inter-Switch Link		• Attached Ports • Created On • Discovered Name • Entity Type • Name • Tags • VW UID	Discovery
Storage Network	LAN		• Created On • Entity Type • Name • Tags • VLAN • VW UID	
Logical Network	Logical Fabric		• Created On • Discovered Name • Entity Type • Fabric ID • Name • Physical Fabrics • Tags • VW UID	Discovery
Logical Network	Logical Switch		• Created On • Discovered Name • Entity Type • Fabric ID • Logical Fabric • Name • SAN Switch • Tags • VW UID • WWN	Discovery
Logical Network	Port Channel		• Attached ISLs • Created On • Entity Type • Is Virtual • Name • Port Speed • Tags • VW UID • WWNs	Discovery

Storage

Table 27. Entity Types - Storage

Sub-Category	Entity Type	Icon	Properties	Created By
NAS>File System	NFS File System		• Created On • Entity Type • Ethernet Port • FSID • NAS File System Key • NFS Conversation • Name • Storage Array • Tags • VW UID	Discovery
NAS>File System	SMB File System		• Created On • Entity Type • Ethernet Port • Name • SMB Conversation • SMB File System Key • Share Name • Storage Array • Tags • VW UID	Discovery
NAS>File System	Link Aggregation Group		• Created On • Entity Type • LAG Key • LAG Number • Name • Tags • VW UID	Discovery
NAS>File System	Monitored Link		• Created On • Entity Type • Link Aggregation Group • NAS Probe Port Key • Name • Port Number • Tags • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
NAS>File System	Destination Ethernet Port		• Created On • DHCPv4 Enabled • DHCPv6 Enabled • Device Type • Entity Type • IP Addresses • MAC Address • Name • Storage Array • Storage Controller • Storage I/O Module • Tags • VW UID	Discovery
NAS>File System	Destination IP Address		• Bonded Network Interface • Created On • Device Type • Domain Name • Entity Type • Ethernet Port • Host • IPv4 Long Value • Name • Network Interface • Prefix Length • Tags • VLAN • VW UID • Value • Version	Discovery
NAS>NetApp	NetApp Cluster		• Cluster Location • Created On • Discovered Name • Entity Type • Manufacturer • Model • Name • Serial Number • Tags • UUID • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
NAS>NetApp	NetApp Storage Node		• Asset Tag • Created On • Discovered Name • Entity Type • Manufacturer • Model • Name • NetAppCluster DisplayLabel • NetAppCluster UUID • Node Location • Serial Number • Tags • UUID • VW UID • Version	Discovery
NAS>NetApp	NetApp SVM		• Created On • Discovered Name • Entity Type • Name • NetAppCluster DisplayLabel • NetAppCluster UUID • Tags • UUID • VServer Type • VW UID	Discovery
NAS>NetApp	NetApp LIF		• Created On • Discovered Name • Entity Type • IP Address • Name • NetApp SVM • Role • Tags • VW UID	Discovery
SAN	Storage Array		• Created On • Entity Type • Name • Tags • VW UID	User or Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
SAN	Storage Controller		• Created On • Entity Type • Name • Storage Array • Tags • VW UID	User or Discovery
SAN	Storage I/O Module		• Created On • Entity Type • Name • Storage Controller • Tags • VW UID	User or Discovery
SAN	Storage Port		• Attached Ports • Created On • Device Type • Discovered Name • Entity Type • FCID • Is Virtual • Logical Fabric • Name • Nickname • Port Speed • Proxy FC Port • Proxy FCID • Proxy Fabric Name • Storage Array • Storage Controller • Storage I/O Module • Tags • VW UID • WWN	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
SDS>VxFlex OS	VxFlex OS System		• Cluster Mode • Cluster State • Created On • Entity Type • Good Nodes Num • Good Replicas Num • Name • Perf Profile • VxFlex OS System Key • System Version Name • Tags • VW UID	Discovery
SDS>VxFlex OS	VxFlex OS Metadata Manager		• Created On • Entity Type • Name • Role • VxFlex OS Mdm Node Key • VxFlex OS Mdm Node Name • Status • Tags • VW UID • Version	Discovery
SDS>VxFlex OS	VxFlex OS Protection Domain		• Created On • Entity Type • Name • VxFlex OS Protection Domain Key • VxFlex OS Protection Domain Name • State • Tags • VW UID	Discovery
SDS>VxFlex OS	VxFlex OS Storage Pool		• Created On • Entity Type • Name • VxFlex OS Storage Pool Key • VxFlex OS Storage Pool Name • Tags • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
SDS>VxFlex OS	VxFlex OS Data Server		• Created On • Entity Type • Maintenance State • Mdm Connection State • Membership State • Name • Perf Profile • Rmcache Size In Kb • VxFlex OS Data Server Key • VxFlex OS Data Server Name • State • Tags • Use Rmcache • VW UID • Version	Discovery
SDS>VxFlex OS	VxFlex OS Network Interface		• Created On • Entity Type • IP Address • Name • Role • Tags • VW UID	Discovery
SDS>VxFlex OS	VxFlex OS Device		• Capacity Limit In Kb • Created On • Device State • Entity Type • Error State • Max Capacity In Kb • Name • Path Name • VxFlex OS Device Key • VxFlex OS Device Name • Tags • VW UID	Discovery
SDS>VxFlex OS	VxFlex OS Volume Tree		• Created On • Entity Type • Name • VxFlex OS Volume Tree Key • VxFlex OS Volume Tree Name • Tags • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
SDS>VxFlex OS	VxFlex OS Volume		• Capacity In KB • Created On • Entity Type • Name • VxFlex OS Volume Key • VxFlex OS Volume Name • Tags • Use Rmcache • VW UID • Volume Type	Discovery
SDS>VxFlex OS	VxFlex OS Fault Set		• Created On • Entity Type • Name • Role • VxFlex OS Fault Set Key • VxFlex OS Fault Set Name • Status • Tags • VW UID • Version	Discovery
SDS>VxFlex OS	VxFlex OS Data Client		• Created On • Entity Type • Mdm Connection State • Name • Perf Profile • VxFlex OS Data Client IP • VxFlex OS Data Client Key • VxFlex OS Data Client Name • Tags • VW UID • Version	Discovery
vSAN	Disk Group		• Cache Disks • Capacity Disks • Created On • Disk Group Key • ESX Datastore • ESX Host • Entity Type • Name • Node UUID • Tags • UUID • VW UID	Discovery

Sub-Category	Entity Type	Icon	Properties	Created By
vSAN	Cache vSAN Disk		• Created On • Device Type • Discovered Name • Disk Group • Entity Type • LUN • Name • PowerVM Partition • Tags • VW UID	Discovery
vSAN	Capacity vSAN Disk		• Created On • Device Type • Discovered Name • Disk Group • Entity Type • LUN • Name • PowerVM Partition • Tags • VW UID	Discovery
vSAN	SCSI Disk		• Created On • Device Type • Discovered Name • Disk Group • Entity Type • LUN • Name • PowerVM Partition • Tags • VW UID	Discovery

Entity Matching

The Entity Matching utility creates entities based on pattern matches using discovered port information, e.g., WWN and nickname (alias).

NOTE

Entity Matching works really well when your organization uses a highly regimented approach to providing aliases (human-readable nicknames for HBA and storage port WWNs) for their devices. Here are some examples:

Host	HBA Ports
SJPEXWIN23	SJPEXWIN23_HBA0 SJPEXWIN23_HBA1

This name breaks down as follows: SJ = San Jose, P = Production, EX = an abbreviation of the primary application (Microsoft Exchange), WIN = Windows, 23 = the 23rd of its kind.

This host has one or more HBA ports. A common naming convention of these ports is shown above.

With this kind of convention in place, using Entity Matching to create the Host entity (SJPEXWIN23) is a trivial exercise.

Storage Array	Storage Ports
VMAX0589	VMAX0589_10E0 VMAX0589_10F0 VMAX0589_10G0 VMAX0589_10HO VMAX0589_9E0 VMAX0589_9F0 VMAX0589_9G0 VMAX0589_9H0

This name breaks down as follows: VMAX = storage array model, 0589 = last four digits of the array's serial number.

This storage array has a number of storage ports associated with it, with names as shown above.

Using Entity Matching to create the storage array entity is very simply done.

The Entity Matcher uses parse rules to group discovered port-level entities into higher level entities like hosts and storage arrays. Parse rules are regular expressions: sequences of characters that form search patterns.

You can use the REGEX tester at this link to test your pattern matches before using the Entity Matching Utility: https://regex101.com/#pcre

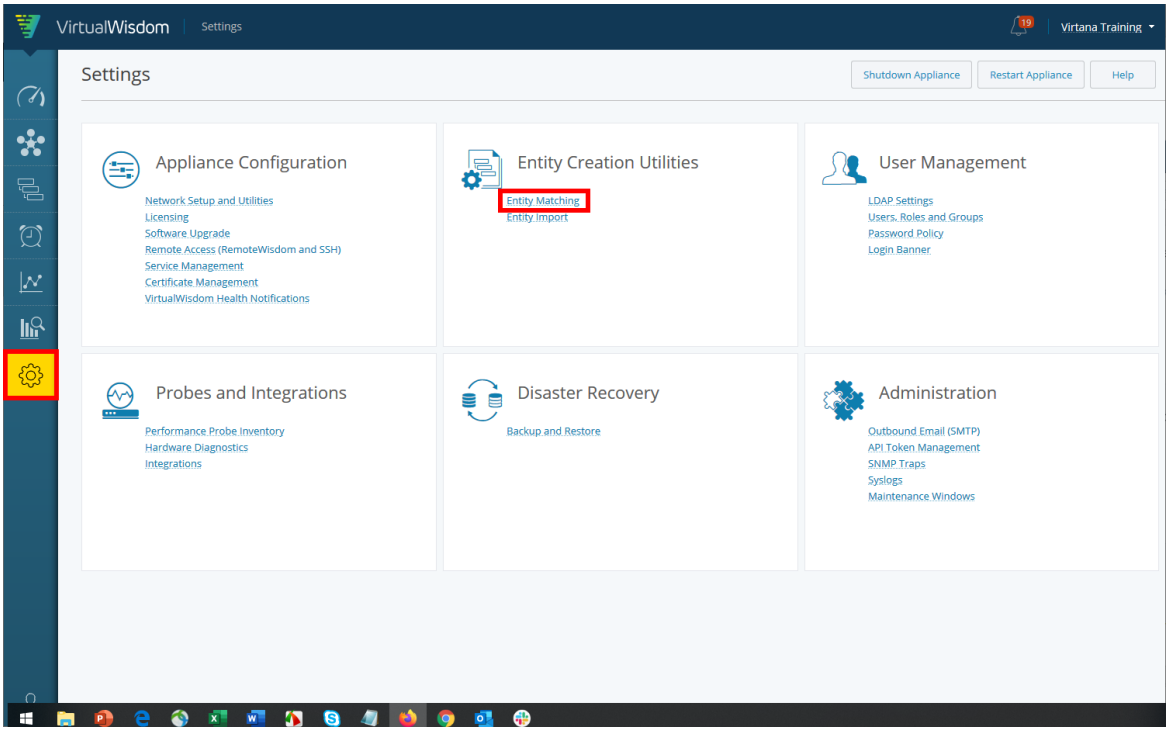
If your organization uses a consistent naming strategy for hosts, storage arrays, and ports, using the Entity Matching Utility is straightforward.

If your organization does not use a consistent naming strategy (this is common in companies that have undergone mergers), you can request assistance from Virtana Services to design parse rules and assist you with using the Entity Matching Utility.

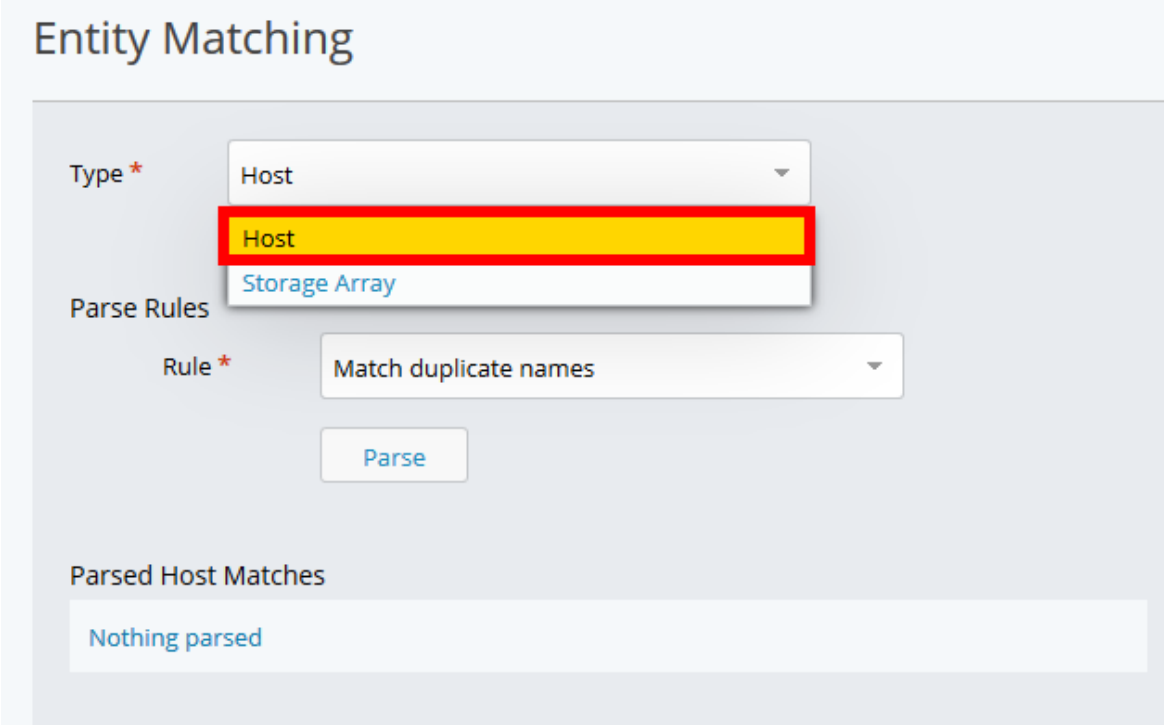
Using the Entity Matching Utility

NOTE
This task is available only to users with the VirtualWisdom Administrator (**vw-admin**) role.

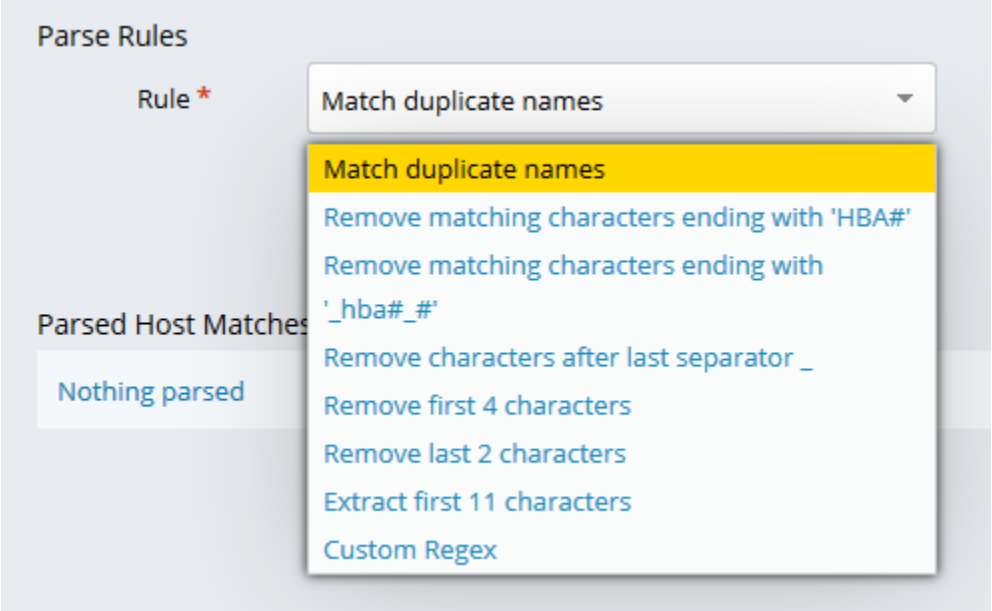
1. To use the utility, navigate to Settings > Entity Matching.



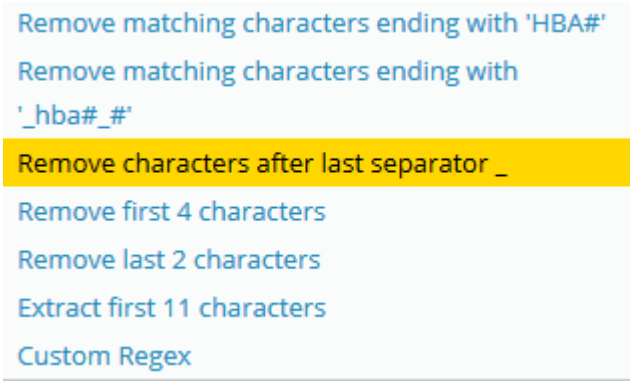
2. You can create hosts or storage arrays using the utility.



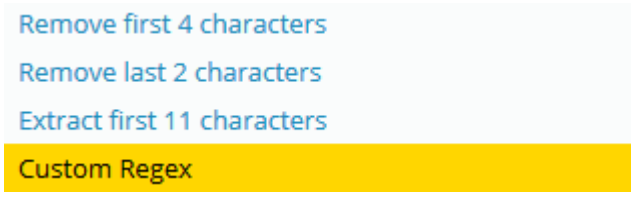
3. Select a parse rule to match the entities' aliases. You can use any of the existing parse rules or create your own custom regex.



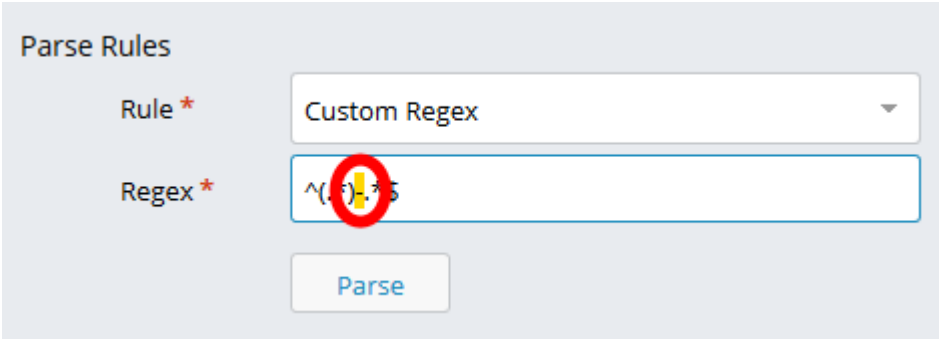
4. Use these recommended parse rules to perform entity matching.



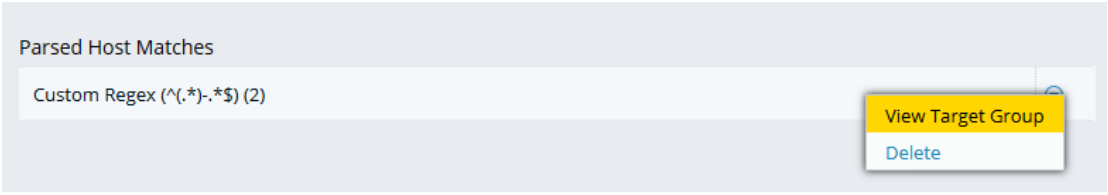
a. **Remove characters after last separator (_)**
This parse rule will remove all characters from the alias after the last separator. The base rule uses an underscore, _, as the separator but you can create a custom rule to change the separator.
After selecting the standard "last separator" rule, select the Custom Regex rule.



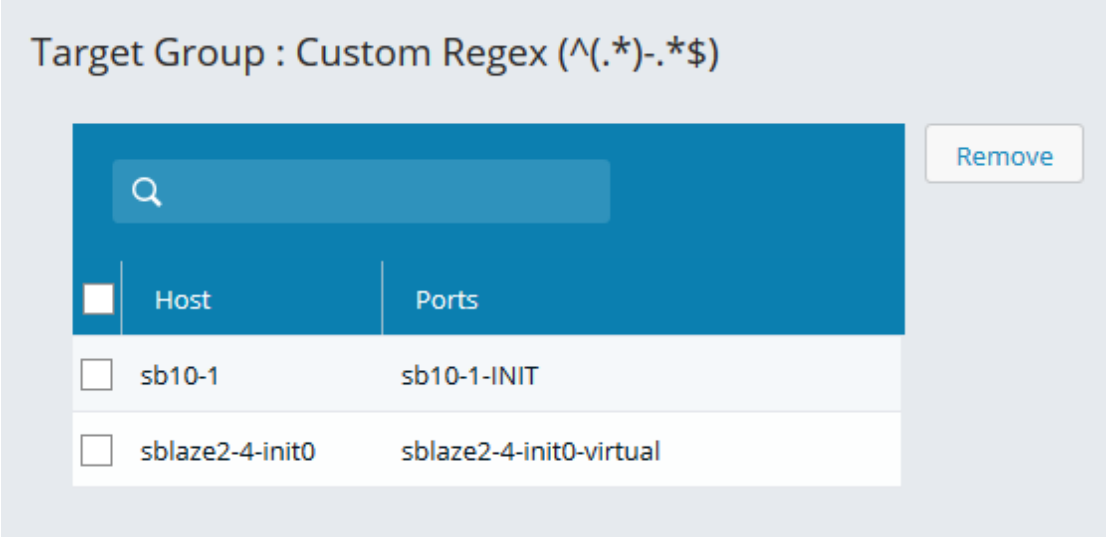
Change the underscore to any other symbol you want to use for matching. Click Parse to view the matches.



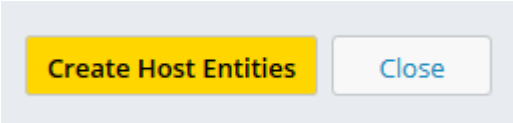
The utility returns the number of matches found. Click the down arrow next to the rule to view all matches in the target group.



All entities matching the rule are displayed. Hover over the matched ports to see the complete list of target hosts. You can remove any entities you do not wish to include in the creation process.



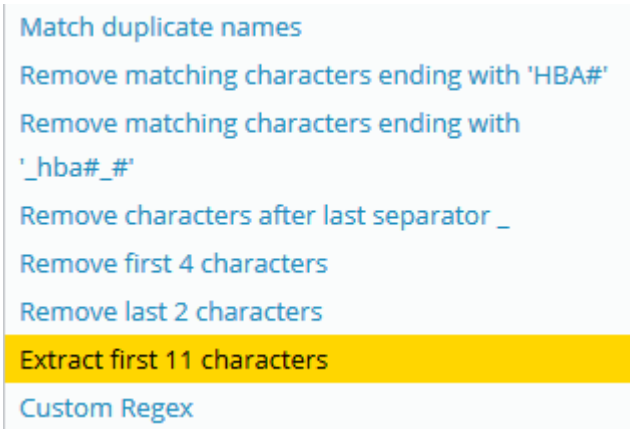
Once you are satisfied with the target group, select Create (Host) Entities to create the entities.



b. **Extract first 11 characters**

Another useful parse rule is the "Extract first 11 characters" rule. Using the same process that was outlined above, you can create a custom regex to change the number of characters to extract.

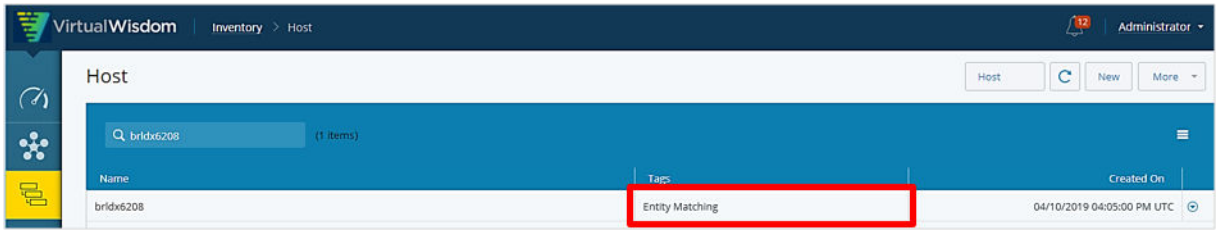
We recommend that you start the the longest port names first.



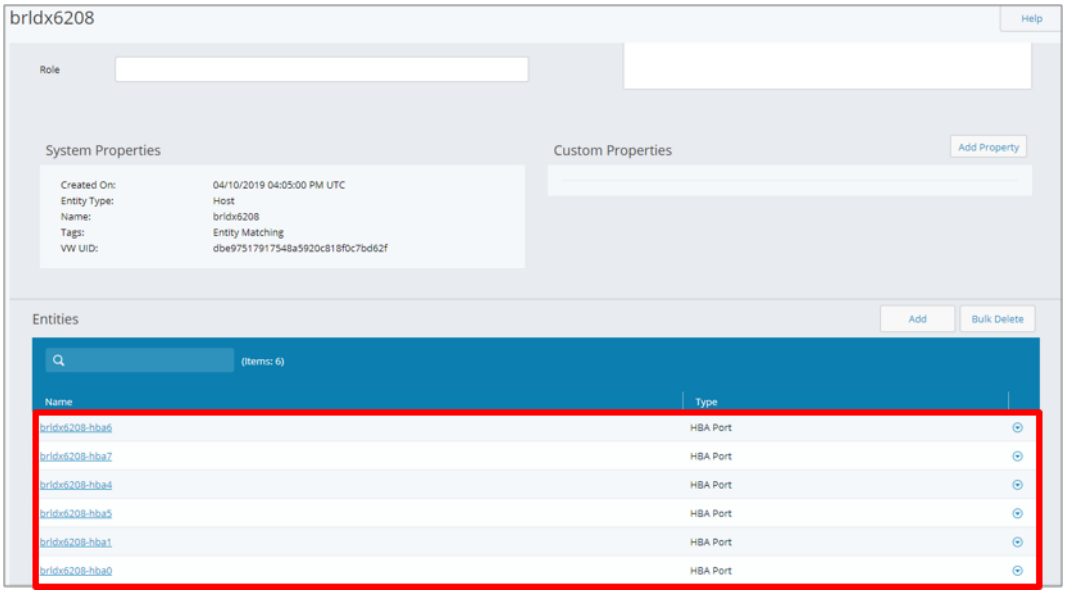
Confirming Entity Creation Using Inventory

Use the Inventory module to confirm entity creation.

The entity is tagged with "Entity Matching" as part of its system properties.

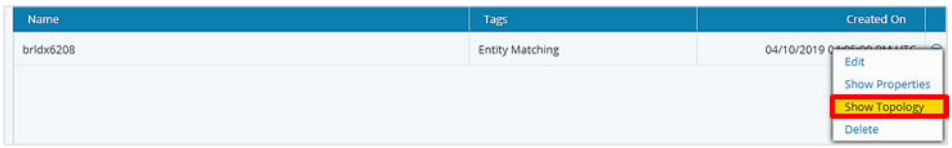


The sub-entities used to create the entity are displayed on the entity's inventory page.

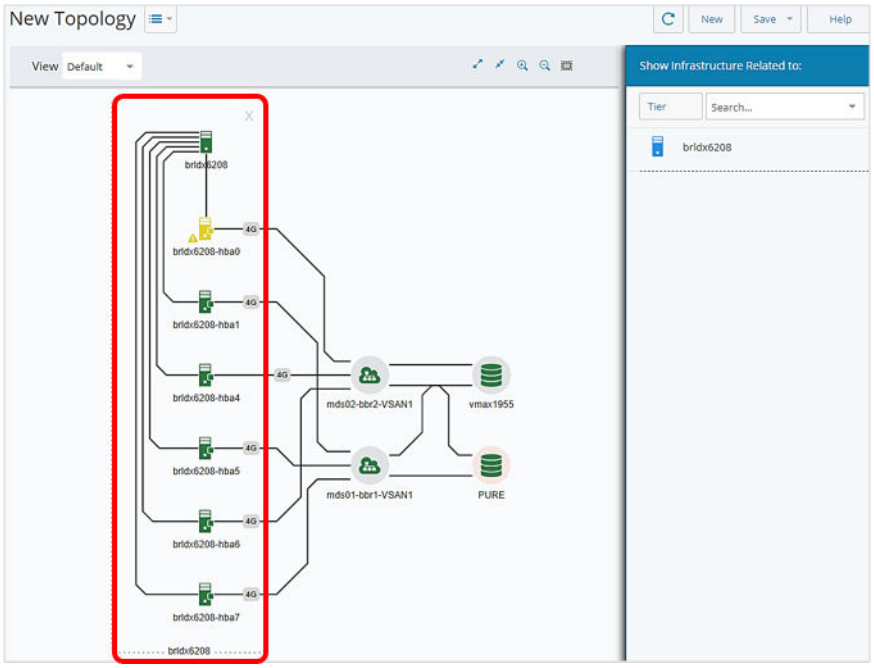


Confirming Entity Creation Using Topology

You can also use the Topology module to confirm entity creation, and to view the entity's relationships within the infrastructure.



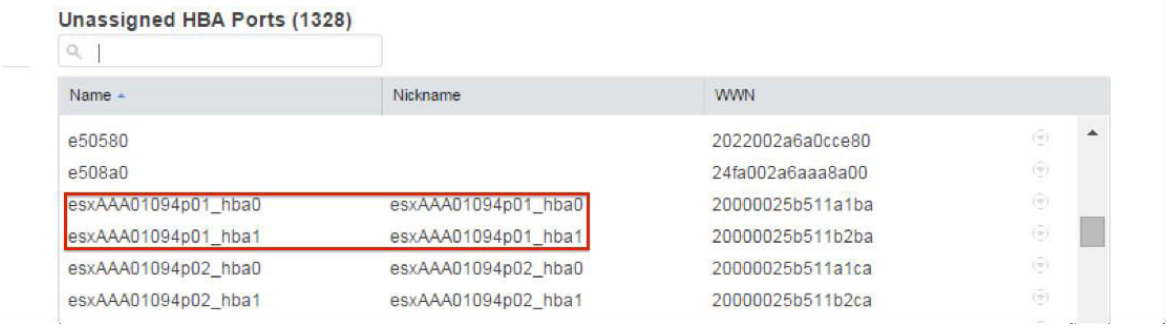
Expand the host's topology to view the HBA ports and the relationships within the infrastructure.



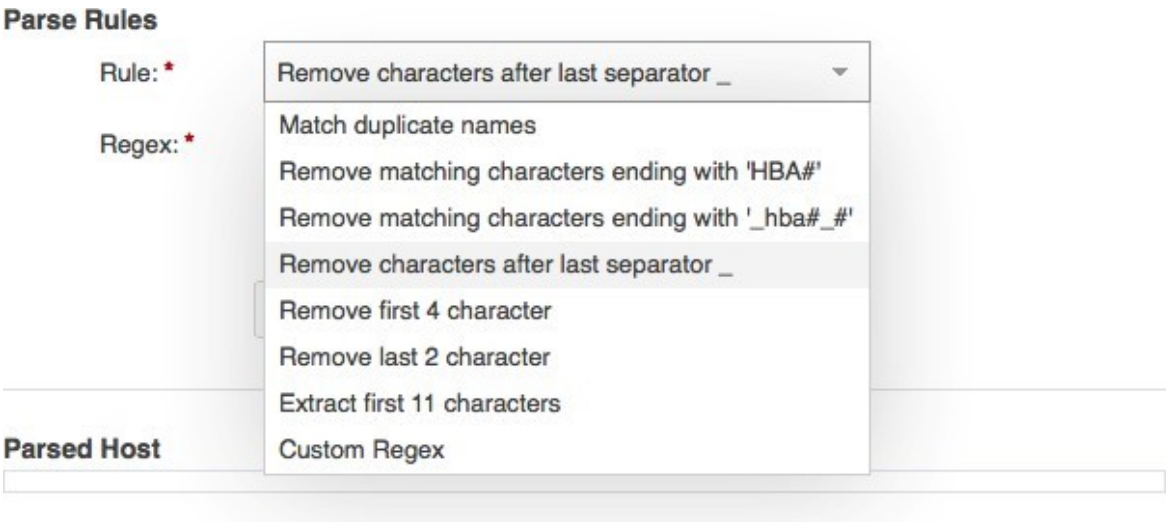
Entity Matching Example

Here's an example of how the Entity Matching utility was used to create a host from HBA port aliases.

1. The Entity Matcher displays a list of unassigned HBA ports. Let's focus on the two HBA ports highlighted in the image below.

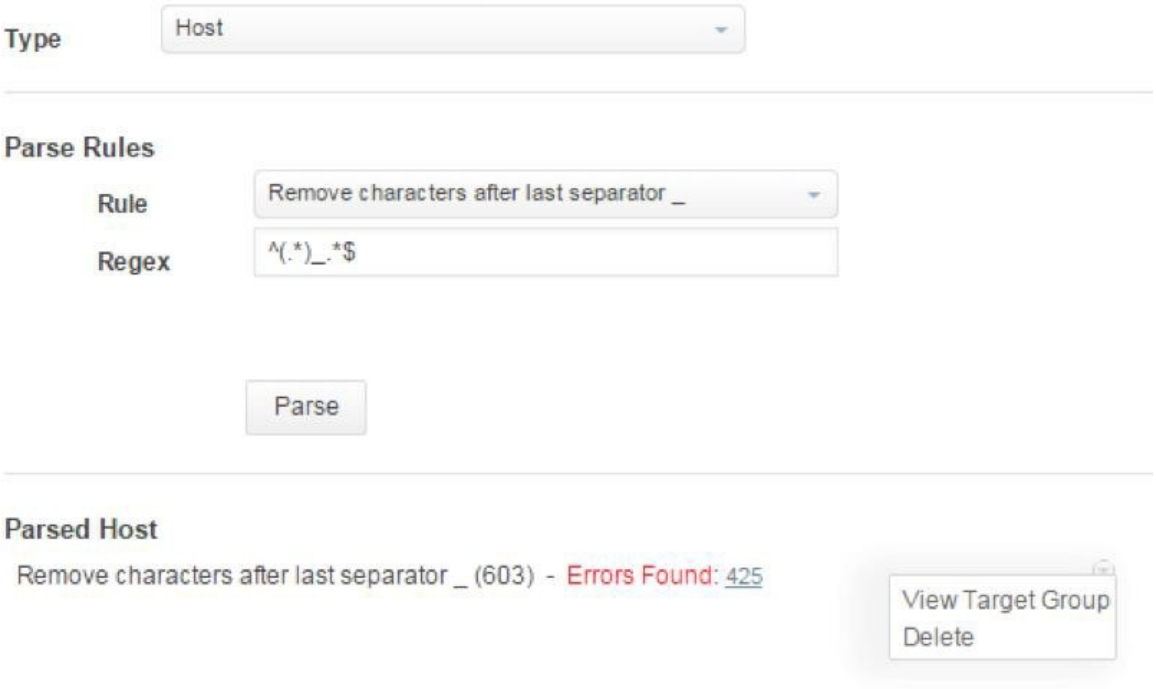


2. It's clear from the naming conventions used that these HBA ports belong to a service named **esxAAA0109p01**. The objective is to use the provided parse rules to select these two HBAs to create the parsed Host name. Luckily, there's a rule that does just that. Select the rule called "**Remove characters after last separator _**" from the Rule pull-down as shown below.

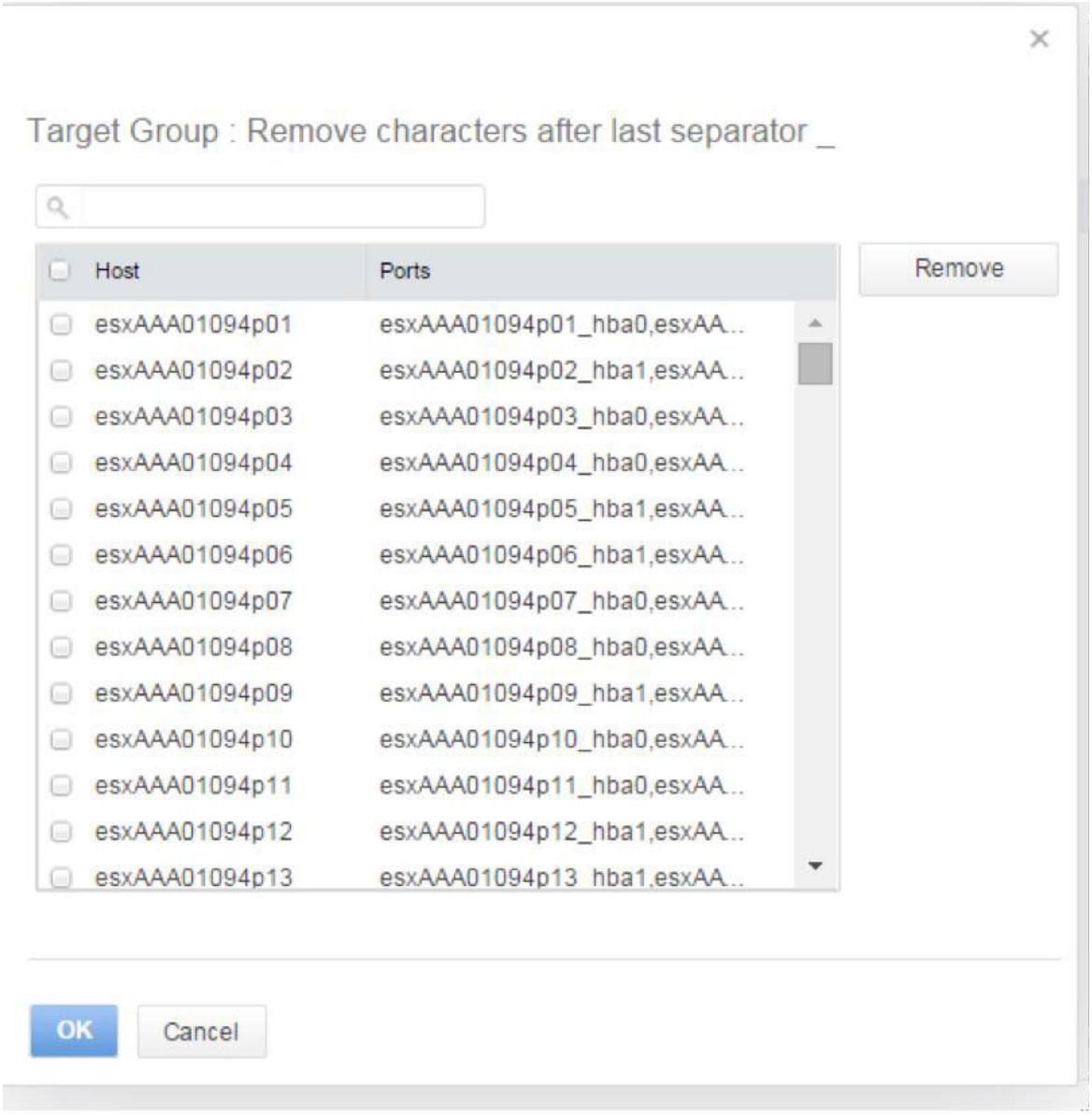


Choosing this rule results in the regular expression (abbreviated Regex in VW):
^(.*)_.*$
Let's translate this rule:
^ Starting from the beginning of the line
(.*) Match any arbitrary sequence of characters: . matches any single character, * matches zero or more of what precedes
Until an underscore character is found
.* Followed by any abritrary sequence of characters
$ Until end of line is encountered

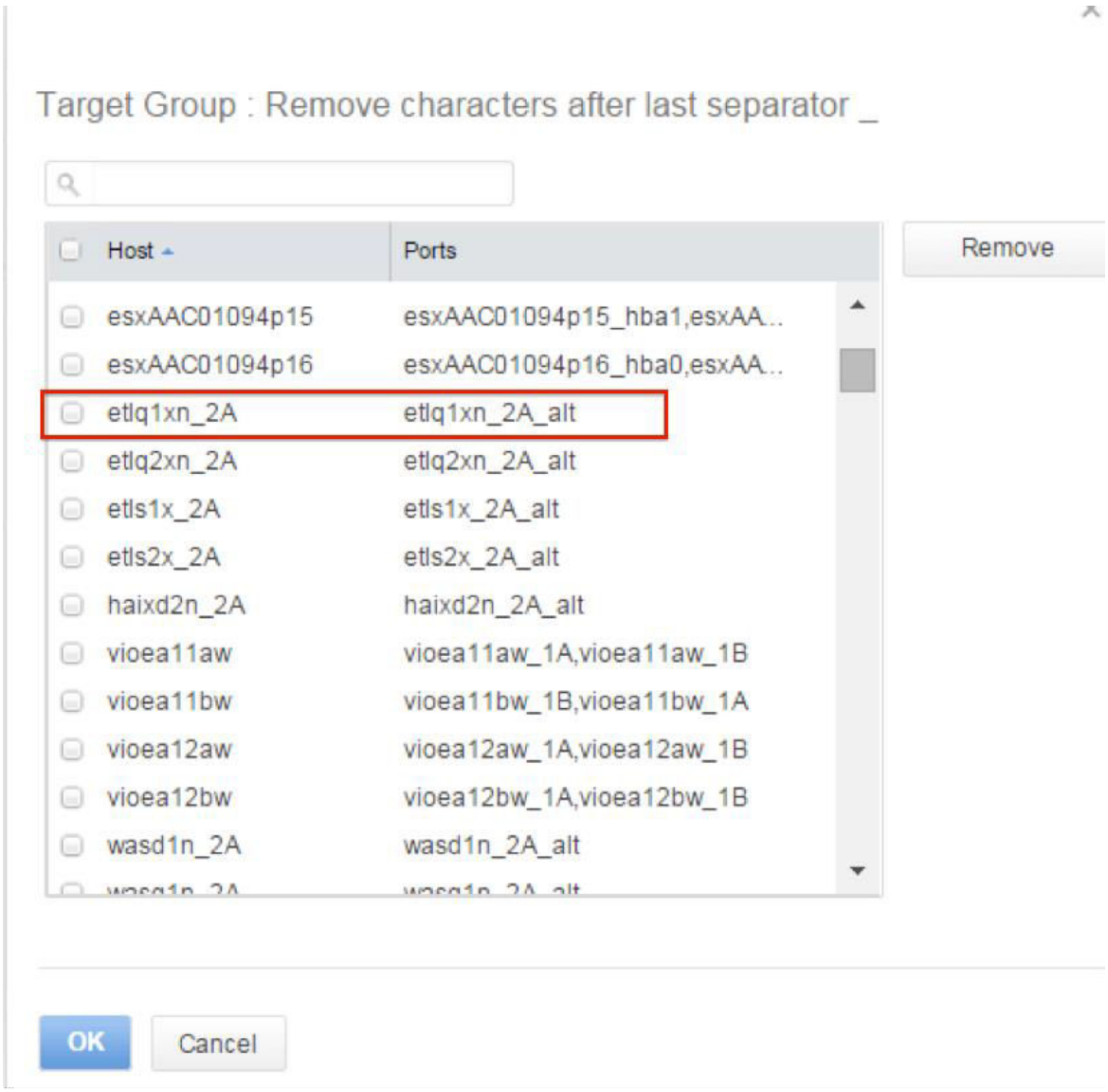
3. After clicking on the **Parse** button, the rule is added to the **Parsed Host** list under the **Parse Rule** selector area. Click on the **View Target Group** to expand the group.



4. A list consisting of Host entity names, each with a list of HBA ports that the entity will contain, is displayed.



5. Review the generated list and confirm that each entry is correct. It's likely that there may be a few host entities that were constructed incorrectly, usually resulting from inconsistent nicknaming. If you go ahead and click OK without reviewing, there may be a set of host entities created that are not correct and that will have to be removed. Here's an example: look at the host entity named **etlq1xn_2A** highlighted in the image below.



It contains a single HBA nicknamed **etlq1xn_2A_alt** which is odd. It's unlikely that any host in this day and age has only a single HBA port in it. There are numerous reasons why VirtualWisdom may not have discovered a second port:

- It didn't have a nickname so it appears in the list as an FCID
- It isn't connected to anything; hence VirtualWisdom couldn't discover it

This line should be excluded until you can resolve the anomaly. Remove the line by clicking on the checkbox next to the name.

6. Once you've finished reviewing the list, you click the **Remove** button to remove suspicious entries. Now you can click the **OK** button and then the **Create Host Entities** button and all of the host entities in the target group(s) will be created.

Custom Regular Expressions

If your organization uses a less rigorous approach to naming your ports, you will have to work a bit harder to use Entity Matching to create Host or Storage entities. Here's an example of two HBA ports belonging to the same virtual server:

Sto_sjctxesx1_PROD-fc-HBA-1-lab_HBA0_New Sto_sjctxesx1_PROD-fc-HBA-1-lab_HBA1_New

The rule we used above won't work here. It would create two hosts named **Sto_sjctxesx1_PROD-fc-HBA-1-lab_HBA0** and **Sto_sjctxesx1_PROD-fc-HBA-1-lab_HBA1**, each with a single port, which is not correct. We want a single host called **Sto_sjctxesx1_PROD-fc-HBA-1-lab** with two HBA ports (**...HBA0_New** and **...HBA1_New**) in it.

What we need to do is modify the Regex for that rule.

1. Start by selected the rule as before, but instead ofapplying it to the list of unassigned HBA ports, simply copy the Regex field into your edit buffer (ctrl-c or cmd-c).
2. Select Custom Regex and paste inthe copied Regex.
3. Edit as shown below and the rule will now match the HBA ports.

Entity Import

Entity import enables you to perform entity creation or modification in bulk by importing CSV or JSON files. You can use import to do several things:

- Create an entity hierarchy from discovered entities.
- (JSON Only) Add or modify device nicknames (alias mappings) for discovered port-level entities

- Modify tags and custom properties for any entity type
- Modify children of container entities. For example, add or remove Host entities from an Application entity

When new entities are added to VirtualWisdom, previously collected metric data for child entities is aligned with the new container entities. This is useful in reports and charts because you can see the historical metrics of the child entities after the creation of the parent.

Related Topics

For information about entities, see Data and Entities.

Entity Hierarchy

VW entities consist of two sets of objects: 1) those that are discovered and created automatically by the various Integrations and 2) those that are created by the user. Users may only create the seven entity types shown below: Tier, Application, Host, HBA Card, Storage Array, Storage Controller, Storage I/O Module. VirtualWisdom ships with four pre-defined Tier definitions, Tier 0, Tier 1, Tier 2, and Tier 3, but these can be replaced by the end user.

IMPORTANT
Entity type names have both external (UI) and internal representations. Import files must use the internal entity type names. Please refer to the next section for information on finding the external to internal mapping of entity type names.

Entity Type	Internal Entity Type Name	Allowed Member Entity Types
Tier	**Tier**	Application
Application	**Application**	Host, HBA Card, ESX VM, Hyper-V VM, PowerVM Partition, PowerVM VIOS Partition, FC Conversation, NFS Conversation, SMB Conversation, iSCSI Conversation
Host	**Host**	HBA Card, HBA Port, Source IP Address, IP Address

Entity Type	Internal Entity Type Name	Allowed Member Entity Types
HBA Card	**HBA**	HBA Port
Storage Array	**StorageArray**	Storage Controller, Storage I/O Module, Storage Port, Destination Ethernet Port
Storage Controller	**StorageController**	Storage I/O Module, Storage Port, Destination Ethernet Port
Storage I/O Module	**IOModule**	Storage Port, Destination Ethernet Port

HBA Card, Storage I/O Module and Storage Controller entities are intermediary and, as such, could be considered optional entities. Meaning, Host entities can be created directly from HBA Port entities or Source IP Addresses and Storage Array entities can be created directly from Storage Port entities and Destination Ethernet Ports. However, as explained below, there are compelling reasons to employ them in customer environments.

Entity Type Names

External (UI) Entity Type Names vs. Internal Entity Type Names

CSV import requires VirtualWisdom internal entity type names, which are not generally visible in the VirtualWisdom UI. However, you can obtain these mappings using the VirtualWisdom public REST API. Please refer to API Token Management [212] for a discussion on how to generate a token for use with the following command, which will retrieve a set of entity schemas that contain, among other things, the internal and external name of each entity type.

```
curl -ks -H"authorization: bearer TOKEN" https://APPLIANCEIP/api/v1/types/schemas
```

Replace TOKEN with your API token and APPLIANCEIP with the IP address of your Appliance/Virtual Edition. The output generated by this command looks something like this:

```
{
  [
...
    {
      "id": "VirtualMachine",
      "name": "ESX VM"
    },
...
```

Above, you can see the mapping between an entities' external name (that which is shown in the VirtualWisdom UI), the "name" attribute, and its internal name, the "id" attribute.

Please note: case matters in CSV import files, so use the same case as it appears in the "`id`" attributes.

Intermediary Entities

HBA Card, Storage I/O Module, and Storage Controller are *intermediary* entities, which means they can be a higher-order entity type or a member entity type.

For example, an HBA Card can be an entity with one or more HBA Port members, and the HBA Card can be a member of the Host entity type. There are advantages to employing intermediary entities in your environments.

In addition to the fact that the intermediary entities can be used to model more complex storage environments, using the full hierarchy of storage-related entities allows you to perform actions such as the following examples:

- Create a report, Top N IOPS by Storage Controllers, filtered to Storage Array, that shows the distribution of a workload across Storage I/O Modules
- Create a report, Top N IOPS by Storage Ports, filtered by Storage I/O Module, that answers the question: Are you multi-pathing your traffic over the available ports correctly?
- Compare the workload and response characteristics of two controllers.

For some storage environments, such as those with active/non-active storage arrays in which the distribution of traffic between Storage Processor/Controller A and B has to be carefully managed, it would be helpful to map the Storage Ports into Storage Controllers (A or B) and then put the Storage Controllers into a Storage Array (skipping the use of Storage I/O Module).

- Modeling port groups.

For some storage environments, modeling the port groups or front-end directors (FEDs) as Storage Controllers can be useful. For VSP, it could be the port group (1a,2a,1e,2e).

The key to using intermediary entities is to view the entity hierarchy as logical units of organization, rather than strictly by their literal interpretation. Starting with a problem statement (i.e., what do you need to see?), model the environment to provide the most efficient solution to the problem.

Make sure that each entity only gets introduced once into the hierarchy. Each foundational entity (HBA Port, Storage Port, Source IP Address, etc.) should only be included in a higher-order entity once. For example, do not add a Storage Port to both a Storage I/O Module and a Storage Controller, and then add those entities to a Storage Array.

Methods of Creating Entities

The VirtualWisdom UI supports three methods to create entities:

- Via the Inventory Tab, wherein a user can create individual entities, one at a time,
- Via **Settings > Entity Matching**, and
- Via **Settings > Entity Import**.

Inventory Tab

Importing from the Inventory Tab is best for occasionally creating an ad hoc entity. It is not efficient for creating extensive hierarchies from discovered entities, or for adding or modifying a lot of alias mappings or new entities. Refer to the Entity Management topic in the User Guide for more information.

Entity Matching

Entity Matching creates Host and Storage Array entities from corresponding HBA Port and Storage Port discovered entities. It cannot be used to create any other entity type.

See Entity Matching [161] for more information.

Entity Import

Importing entity definitions is used when individual entity creation or entity matching are not sufficient for the entity creation or modification that you need to do. The two principal use cases are:

- Importing device aliases (either adding them or modifying them) for HBA Port and/or Storage Port entities
- Constructing entity hierarchies for complex environments

The process of importing entities is usually an iterative process with two main work streams:

1. Importing device aliases to either add them if they do not exist or to modify them if they do exist.
2. Creating entity hierarchies from discovered entities.

Getting all HBA Port and Storage Port entity names set correctly is important when modeling and viewing your environment. If you are working with a large number of entities, this process is likely be iterative in nature. You might encounter circumstances such as trying to create aliases for WWNs that were not discovered, or that were initially discovered but stopped displaying. It could, therefore, take several passes to get to a known good state.

After you complete the alias mappings, you can create entity hierarchies.

JSON Entity Import File Format

A JSON entity import file is a plain text file that must be named with a "`.json`" file name extension, such as "`entities.json`". Each import file must contain a single JSON object with the following attributes (name/value pairs):

JSON Attributes	Required?	Comments
common_attributes	no	An array of other objects
entities	yes	An array of other objects
version	yes	A number representing the JSON file format version used. At the time this document was written, version must be set to 2.

TIP

The order of the objects in the JSON file is irrelevant. Parent and child entities can be created in any order. VirtualWisdom runs through the entire file before creating entities.

WARNING

You cannot use any of the following characters for name and tags fields:

, ; * ? < > | + % ~ & = [ ]

Following is an example of a basic import file.

```
{
  "common_attributes": [...],
  "entities": [...],
  "version": 2
}
```

The common_attributes Element

These are shortcuts used to provide common descriptions, tags, and custom properties for entities contained in an input file. They are a container for objects consisting of the following attributes:

- `description` (optional) - the value is a string.
- `entity_types` (optional) - the value is an array of entity types taken from the following list. Import is now case-sensitive.
  - Application
  - fcport (used to provide aliases for either HBA Port or Storage Port entities)
  - HBA
  - Host
  - IOModule
  - StorageArray
  - StorageController
  - If the value is not null, then the attributes apply to all entities of the listed types contained in the file.
  - If the value is null, then the attributes apply to *all* entities contained in the file.
  - For custom properties, `entity_types` cannot be used, so you need to be careful how you apply custom properties to entities.

  If the value is not null, then the attributes apply to all entities of the listed types contained in the file.
  If the value is null, then the attributes apply to *all entities* contained in the file.
  For custom properties, `entity_types` cannot be used, so you need to be careful how you apply custom properties to entities.
- `tags` (optional) - the value is an array of strings.
- `addProperties` (optional) - the value is an object containing custom property attributes.

In the following `common_attributes` example, two sets of tags are defined: one for `fcport` entities and another for `host` and `hba` entities. Also, there is a custom property called `property1` that will be added to all entities in the file. ustom properties can only be included in the `common_attributes` section.

NOTE
Custom properties can only be included in the **common_attributes** section.

```
{
  "common_attributes": [
```

```
    {
      "entity_types": [
        "fcport"
      ],
      "tags": [
        "Device Aliases", // Example tag
        "JSONIMPORTED"    // Example tag
      ]
    },
    {
      "entity_types": [
        "Host",
        "HBA"
      ],
      "tags": [
        "Initiators",  // Example tag
        "JSONIMPORTED" // Example tag
      ]
    },
    {
      "addProperties": {
        "property1": "value1" // Example custom property
      }
    }
  ],
  "entities": [...],
  "version": 2
}
```

Typically, JSON files are constructed using tools that automate the process (e.g., converting a CSV to JSON), so `tags` and `description` are specified in-line rather than abstracted out. As a result, the remaining examples do not use `common_attributes`, to reflect that more common scenario.

The entities Element

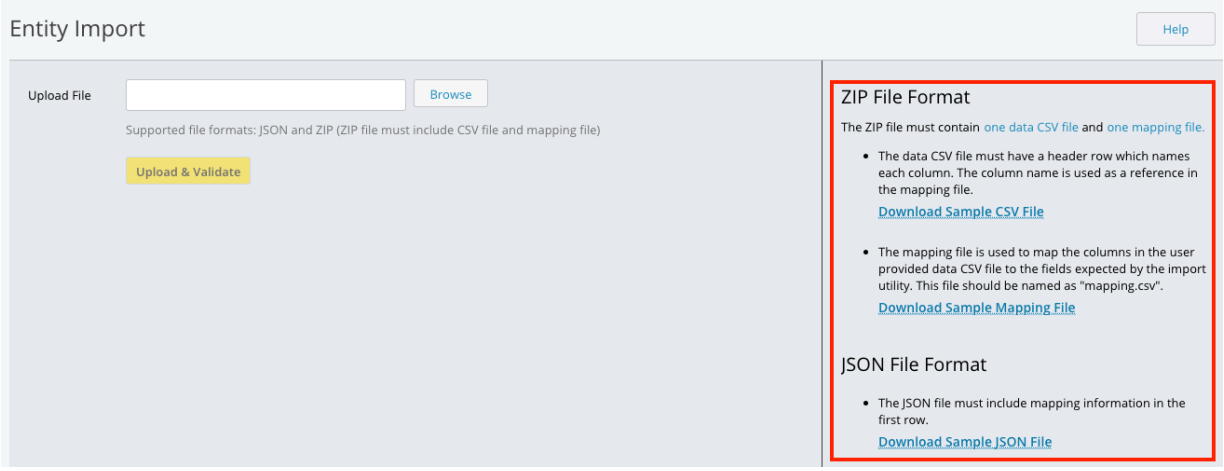
The `entities` attribute is an array of objects consisting of the following possible member pairs:

- `name` (required) - the value is a unique string that identifies the entity. It must be present for all types except `fcport`.
- `description` (optional) - the value is a string.
- `tags` (optional) - the value is an array of strings.
- `child_entities`
  - The value is an array of entity names or, as appropriate, port WWNs (e.g., HBA Port or Storage Port entities).

  - They can be existing user-created or discovered entities, or entities being imported in the same import file.
  - Specify child entity identifiers by WWN if child entities are port-level entities.
  - Specify by name of entity for user-created child entities.
- `devices`
  - The same as `child_entities`, but only used with `application` entities.
- `itl_patterns` - the value is an array of initiator, target, and LUN (ITL) specifications for `application` entities only.
- `type` - one of application, tier, host, hba, storagearray, storagecontroller, iomodule, or fcport.
- `wwn` - the value is a string representation of a WWN; only used with `fcport` type entities.
- `edit_type` - a string defined as either "`add`" or "`modify`"; the default is "`modify`".

Sample JSON File

A sample JSON file can be downloaded from VirtualWisdom. Go to Settings > Entity Import and then click on the appropriate link in the pane on the right side of the UI.



Importing Device Aliases

If you do not use aliases (nicknames for port WWNs), or if you do not use them in a consistent and coherent manner, then you might want to create them or to modify them, and then import them into VirtualWisdom. Without aliases, you only see FCIDs in the VirtualWisdom UI. Useful alias names are recommended to getting the most benefit out of using the Entity Creation Utility.

Alias import is done using the `fcport` type in a JSON import file. You can only perform alias mapping on the port level entities HBA Port and Storage Port. You cannot map aliases to switch ports.

Tip: The examples that follow use a singleton array with JSONIMPORTED as the only entry. This is simply a best practice. Tags can be any valid string.

The port WWN displays with the assigned entity name rather than the WWN in all parts of the user interface.

Structure of an alias import file:

```
{
  "entities": [
    {
      "description": "description",
      "edit_type": "add",
      "name": "entity name", // Real entity name goes here
      "tags": ["JSONIMPORTED"], // Example tag
      "type": "fcport",
      "wwn": "WWN" // Real WWN goes here
    }
  ],
  "version": 2
}
```

The `fcport` type is only used for mapping aliases to existing port-level entities (HBA Port and Storage Port).

Note that `description` and `tags` are optional elements, and `edit_type` defaults to `add`, so they are not explicitly required.

Example

```
{
  "entities": [
    {
      "description": "248d00059b2b78c0,fooserver_hba1 from customer.csv",
      "name": "fooserver_hba1",
      "tags": [
        "JSONIMPORTED"
      ],
      "type": "fcport",
      "wwn": "248d00059b2b78c0"
    },
    {
      "description": "5001438002b0dbb4,barserver_hba1 from customer.csv",
```

```
      "name": "barserver_hba1",
      "tags": [
        "JSONIMPORTED"
      ],
      "type": "fcport",
      "wwn": "5001438002b0dbb4"
    }
  ],
  "version": 2
}
```

When importing aliases, consider the following:

- You can only import aliases for the discovered, port-level entities HBA Port and Storage Port. Switch port aliases are not supported.
- You can override discovered aliases by providing an alternative name for a port WWN in an import file.
- You can revert to a discovered name using an import where the name strings for a port WWN is the empty string, "".

HBA Card and Host Entities

The JSON file required for importing Host or HBA Card entities is similar to the device aliases (nicknames) import file, but there are some differences:

- The `type` attribute is different. For HBA Card entities, the `HBA` type is used. For Host entities, the `Host` type is used.
- A `child_entities` attribute is used with an `add` verb to specify child entities. The `add` verb overrides the `edit_type` attribute, so it doesn't need to be used.

Example

This example will create three entities: two HBA Port entities and one Host entity. Note the order in which entity specifications appear: the Host entity appears first in the file. But the Host entity depends on the two HBA Port entities. That is okay. VirtualWisdom will read and parse the entire file before figuring out which entities need to be created in what order.

```
{
  "entities": [
    {
      "child_entities": {
        "add": [
          "server1_hba0",
          "server1_hba1"
        ]
```

```
      },
      "description": "description text",
      "name": "server1",
      "tags": ["JSONIMPORTED"],
      "type": "Host"
    },
    {
      "child_entities":
        "add": [
          "10000000c1234560",
          "10000000c1234561"
        ]
      },
      "description": "description text",
      "edit_type": "add",
      "name": "server1_hba0",
      "tags": ["JSONIMPORTED"],
      "type": "HBA"
    },
    {
      "child_entities": {
        "add": [
          "server1_hbaport2",
          "server1_hbaport3"
        ]
      },
      "description": "description text",
      "name": "server1_hba1",
      "tags": ["JSONIMPORTED"],
      "type": "HBA"
    }
  ],
  "version": 2
}
```

Storage I/O Module, Storage Controller, and Storage Array Entities

The process for creating Storage I/O Module, Storage Controller, and Storage Array entities is identical to creating HBA Card and Host entities, differing only by `type`. The types are `IOModule`, `StorageController`, and `StorageArray` respectively.

Example

```
{
  "entities": [
    {
      "child_entities": {
```

```
        "add": [
          ...
        ]
      },
      "description": "description text",
      "name": "name text",
      "tags": ["JSONIMPORTED"],
      "type": "IOModule" or "StorageController" or "StorageArray" // Pick one
    },
    {
      ...
    }
  ],
  "version": 2
}
```

Application Entities

The structure and content of an Application entities import file are very similar to the other hierarchical entities' import files. But instead of having a `child_entities` object, they have either an `itl_patterns` array or a `devices` object or both.

The `devices` object is identical in use to the `child_entities` object we've already seen.

The `itl_patterns` array contains objects consisting of the following elements:

- `edit_type` (required) - needs to be set to `add`.
- `initiator` (required) - set to the name of an HBA Port entity.
- `target` (required) - set to the name of a Storage Port entity.
- `LUN` (optional) - set to a LUN number or exclude, which means all LUNs.

Example

```
{
  "entities": [
    {
      "description": "description text",
      "devices": {
        "add": [
          "device1",
          "10.0.0.1:10.2.0.1:0",
          "10.0.0.3"
        ]
      },
      "itl_patterns": [
        {
```

```
          "edit_type": "add",
          "initiator": "somehbaport",
          "lun": 0,
          "target": "somestorageport"
        },
        {
          "edit_type": "add",
          "initiator": "somehbaport",
          "target": "somestorageport" // No LUN here means ALL LUNs
        }
      ],
      "name": "name text",
      "tags": ["JSONIMPORTED"],
      "type": "Application"
    }
  ],
  "version": 2
}
```

Adding Tier Entities

While you cannot add Tiers directly in Application entity JSON, you can add them separately.

Example

```
{
  "entities": [
    {
      "name" : "Tier Three",
      "type" : "Tier",
      "child_entities" : {
        "add" : [
          "app1",
          "app2",
          "app3"
        ]
      }
  ],
}
```

CSV Entity Import File Format

For existing customers currently using the Entity Import feature using JSON files, CSV import provides for only a subset of the features supported by JSON import. Please note the following differences.

- CSV import cannot be used to
  - Populate the entity description field
  - Create device aliases for HBA Port or Storage Port entities
  - Create Tier definitions for Application entities
  - Add ITLs to Application entities
- Use of WWNs in place of entity names for port-level devices is not supported.

A CSV entity import file is a ZIP file containing two CSV files. The first CSV file is a mapping file and must be named "`mapping.csv`". The second CSV file is the data file that contains descriptions of entities that will either be created or modified.

Mapping File (CSV)

The mapping file is one of the required files in a CSV import ZIP file. It is essentially a roadmap for how VirtualWisdom will identify content in the data CSV file. The mapping file consists of the following columns. The order in which columns appear in the mapping file is irrelevant.

Column Name	Required?	Description
`file_name`	yes	The name of the data file with no path information. The data file must reside in the same directory as the mapping file in the ZIP file.
`skip_rows`	no	Skip the specified number of rows from the data file after the header row. If the value is either empty or not present in the mapping file, the default is 0.
`entity_lookup_id`	no	How an existing entity will be identified. There are two possible values: • `name` This is the default if the value is either empty or not present in the mapping file. • `ip` If this value is specified for an entity type that does not support IP address lookup, an error will be reported. Please note: the supported entity types that can be searched by IP address are: Host, VirtualMachine (ESX VM), Partition (PowerVM Partition), HyperVVM (Hyper-V VM), and other entities of type host and virtual host with assigned IP address (e.g., KVMCapiHost/KVMCapiVirtualHost (KVM Host/KVM Virtual Host)).
`entity_lookup_col`	yes	The name of the entity lookup column in the data file.

Column Name	Required?	Description
`entity_type`	no	The entity type name as defined internally by Virtana. The following entity types are supported for entity creation and for device modification: Application, Host, HBA (HBA Card), IOModule (Storage I/O Module), StorageController, and StorageArray. If the field is either empty or not present in the mapping file, the import utility attempts to detect the type for an existing entity. If a new entity is being created, the default value `Application` is used. This field is associated with the `entity_lookup_col`. If the `entity_lookup_id` column is set to `ip`, this column must be set.
`device_lookup_id`	no	**NOTE** The fields starting with `device_` are used when adding or modifying child entities to container entities, such as Applications. How an existing device entity will be identified; same options as `entity_lookup_id`.
`device_lookup_col`	maybe	The name of device lookup column in the data file. This is required if the device should be associated with an entity.
`device_type`	no	The entity type name as defined internally by Virtana. The same entities that can be added to user-created entities in VirtualWisdom may be used here. If the field is either empty or not present in the mapping file, the import utility attempts to detect the type for an existing entity. This field is associated with the `device_lookup_col` column. If `device_lookup_id` is set to `ip`, this column must be set.
`entity_tag`	no	Zero or more columns can be added with this column name, each column representing one tag. The value specifies the name of a tags column in the data file. If multiple columns are specified with this column name, multiple tags are assigned to the imported entity.
`entity_custom_prop`	no	Zero or more columns can be added with this column name, each column representing one custom property. The value is the name of column in the data file which represents a custom property. The column name in the data file is the key of the custom property.

Column Name	Required?	Description
`replace_properties`	no	If set to `true`, all the existing custom properties associated with the entity will be replaced. The default value is `true`.
`replace_devices`	no	If set to `true`, all the existing devices associated with the entity will be replaced. The default value is `true`.

Data File (CSV)

The data file contains information about each entity that will either be created or updated upon import. The file must have a header row which names each column. The column names are derived from the columns in the mapping file. If the field values in the file contain characters which are not allowed or readable by VW, those rows will be skipped from import. The order in which columns appear in the mapping file is irrelevant.

WARNING

You cannot use any of the following characters for tags or `custom property` columns:

, ; * ? < > | + % ~ & = [ ]

Sample Mapping File (mapping.csv)

file_name	skip_rows	entity_lookup_id	entity_lookup_col	entity_type	device_lookup_id	device_lookup_col	entity_tag	entity_tag	entity_custom_prop	entity_custom_prop	entity_tag
apps.csv	0	name	app	Application	name	server	function	environment	data center	location	import_tag

In this example, the mapping file defines settings for Application creation and/or modification. Each Application defined in the associated data file (see below) will have a number of child entities defined by their names and will have three tags and two custom properties each. Column explanations follow in the left-to-right they appear in the file.

- The associated data file name must be apps.csv
- Zero rows will be skipped. As this is the default, this column could be omitted.
- Entities will be searched by name.
- Entity names will be located in the "app" column in the data file.
- Only Application entities will be added or modified.
- Application devices (child entities) will be identified in VirtualWisdom by name.
- Device names will be located in the "server" column in the data file.

- Three tags will be added to each Application entity, identified by the "function", "environment", and "import_tab" columns in the data file.
- Two custom properties will be added to each Application, identified by the "data center" and "location" columns in the data file.

Sample Data File (apps.csv)

app	server	function	import_tag	data center	location	environment
email_prod	server_1	email	hg_import	central	Texas	prod
email_stage	server_2	email	hg_import	central	Texas	stage
devops	server_3	jenkins	hg_import	west1	San Jose	dev
devops	server_4	jenkins	hg_import	west1	San Jose	dev
devops	server_5	jenkins	hg_import	west1	San Jose	dev
nas_prod	server_6	nas	hg_import	central	Texas	prod
nas_prod	server_7	nas	hg_import	central	Texas	prod
nas_prod	server_8	nas	hg_import	west1	San Jose	prod
nas_stage	server_9	nas	hg_import	central	Texas	stage

In this example, five total Application entities will either be created, if they don't currently exist, or be modified. Two of the Applications will have more than one device (child entity): "devops" and "nas_prod".

Importing an Entity File

You must have created either a JSON file with a ".json" extension or a ZIP file containing two CSV files, `mapping.csv` and another file containing the entity information for the type of import you intend to perform.

1. From the Settings screen, click **Entity Import** under **Entity Creation Utilities**.
2. Click **Browse** and select the file that you want to import.
3. Click **Upload & Validate**. The file will be evaluated to ensure that it conforms to the required specifications.
   If errors are found while validating the contents of the file, a warning displays. Some errors still allow you to proceed with the import, but only validated entries are imported.
   If there are no errors in the file, a message displays stating that the file was validated and the number of valid entities will be displayed.
4. Click **Import**.
   The import process runs in the background. The amount of time that the import takes depends on the number of entities being imported. During this time, you can navigate to other parts of the interface or log out of the VirtualWisdom UI.

When import is complete, view the imported entities from the Inventory tab.

Import File Validation

Import files are validated before an attempt is made to import them.

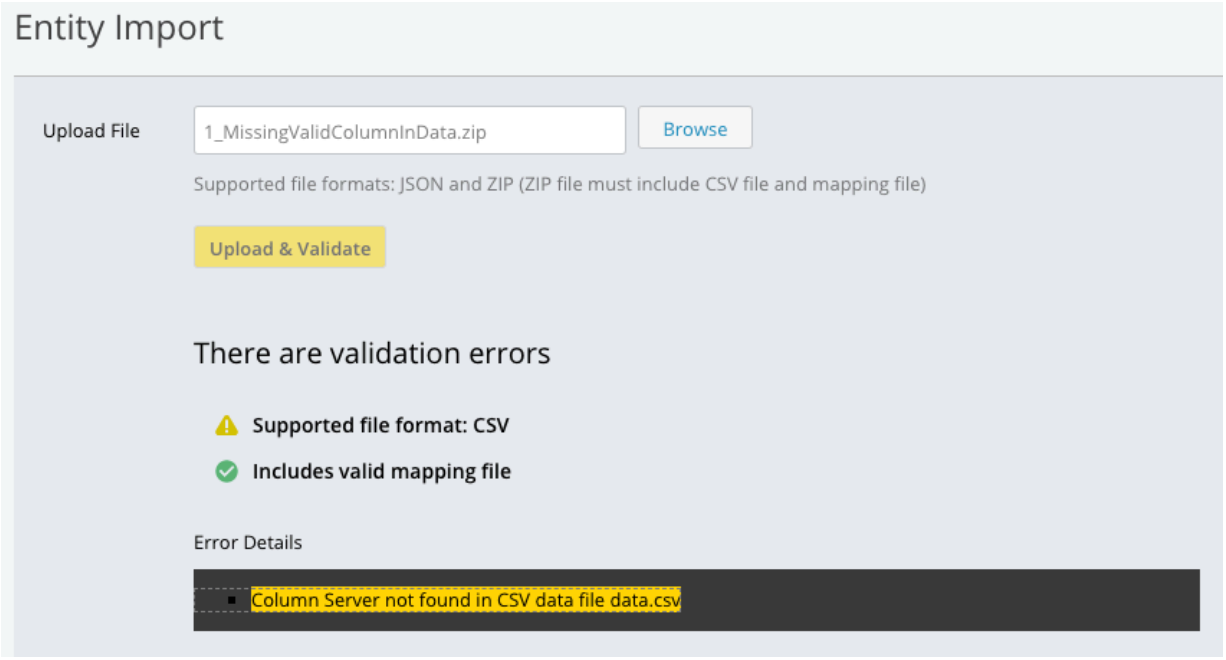
For JSON import, if an error is reported, VirtualWisdom will provide an error. The line number and character position represents the beginning of the entity object that is being imported.

For CSV import, if an error is reported, VirtualWisdom will provide an error, and, further, it will make annotations in your original CSV files and let you download them for correction.

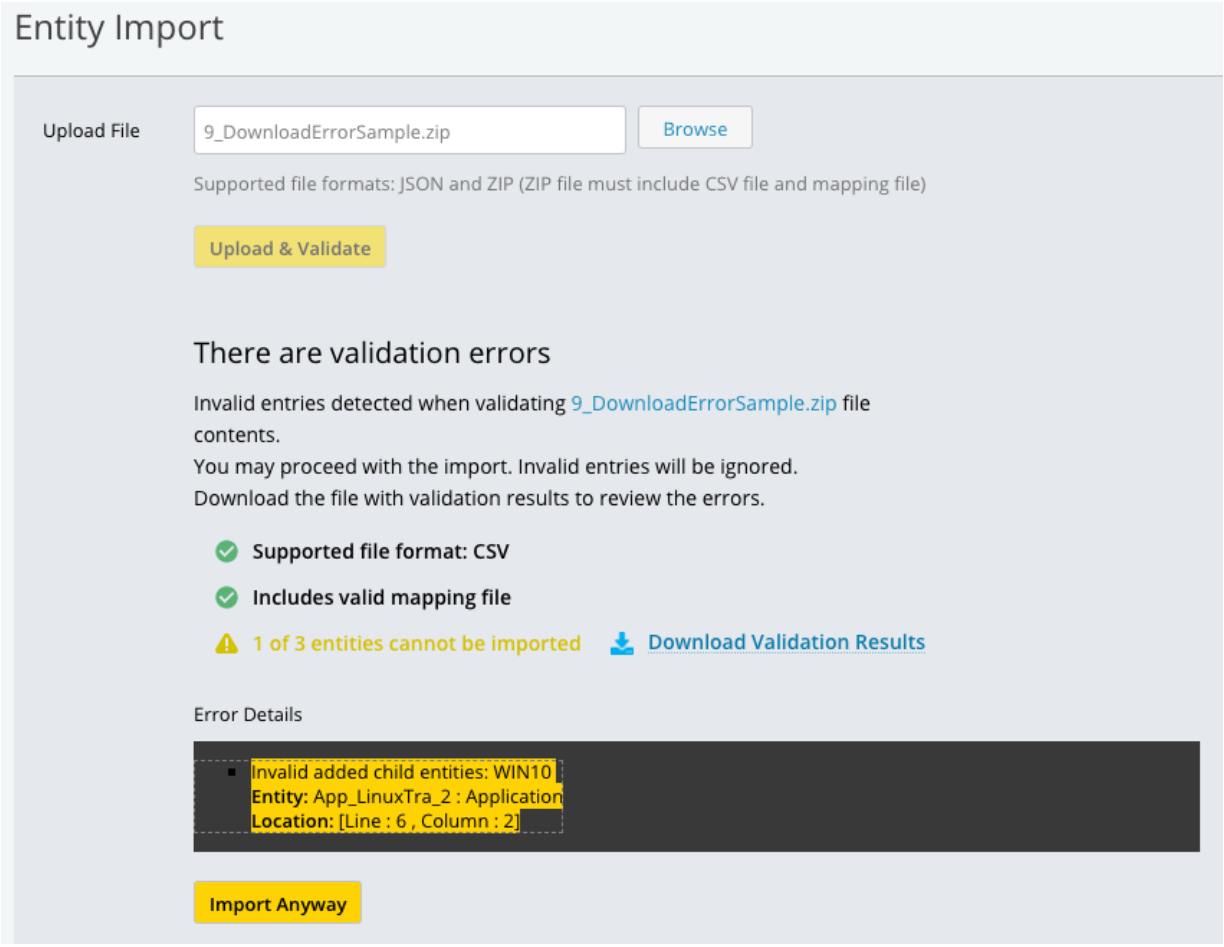
Sample Errors

CSV

In the following example, an error is reported, but no files are annotated because of the nature of the error.



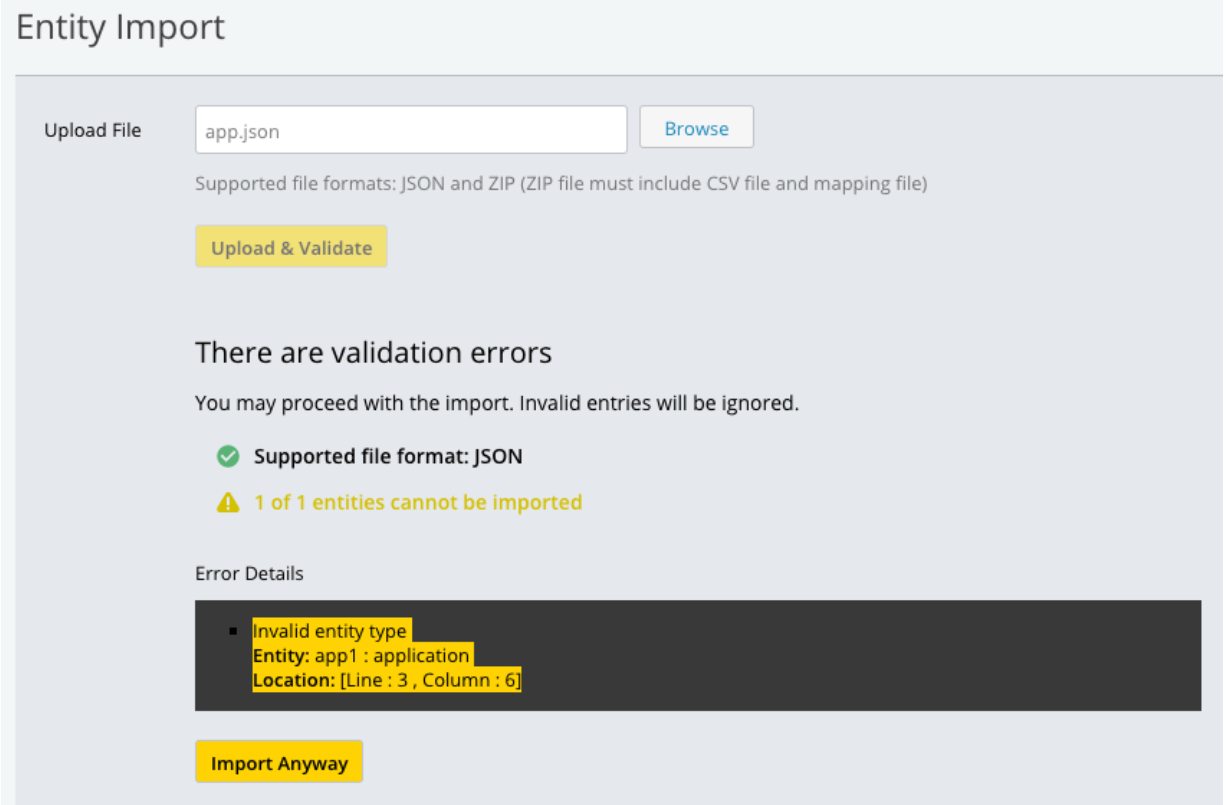
In the next example, an error is reported and one or more of the CSV files have been annotated and are available for download.



ID	ApplicationName	DeviceName	DeviceType	Function	CustomerProperty2	Microsoft	Tag	CustomerProperty1	ApplicationType	Validation error
1	App_LinuxTra_ESXVM	Docker1-master	VirtualMachine	LinuxTranslator	CP1_Low	OS1	Translator	App1	WebServer	
2	App_LinuxTra_ESXVM	Docker2-slave	VirtualMachine	LinuxTranslator	CP1_Med	OS2	Translator	App1	WebServer	
3	App_LinuxTra_ESXVM	Docker3-slave	VirtualMachine	ESXVM	CP1_High	OS3	Translator	App1	WebServer	
4	App_LinuxTra	Docker4-slave	VirtualMachine	LinuxTranslator	CP1_Med	OS4	Translator	App2	Database	
5	App_LinuxTra_2	WIN10	HyperVVM	HypervVM	CP1_High	OS5	hypervvm	App3	WebServer	column 2: Invalid added child entities: WIN10; column 3: Device entity WIN10 not found

JSON

In the following example, an error is reported.



Common CSV Import Errors

Error	Description
CSV Mapping file is missing	No mapping.csv file was found in the uploaded ZIP file.
Invalid mapping file	Mapping file has misspelled column names or is missing required columns.
Zip file is expected	Something other than a ZIP file was uploaded.
CSV data file X is missing	A data file with the expected name (the one listed under the file_name column of the mapping file) is missing from the ZIP file.

Common JSON Import Errors

Error	Description
Only HBA port or storage port can be identified by WWN	An entity other than HBA Port or Storage Port was used to map an alias.

Error	Description
Either entity name or WWN must be set	The entity name or WWN parameter for a child entity was omitted. Add the entity name or WWN.
ITL patterns can only be set with application type entities	An ITL pattern was added to the wrong entity type. Remove the ITL pattern and use valid children.
Invalid ITL Pattern. Allowed patterns are IT* and ITL	An invalid ITL combination was configured. Use either IT* or ITL. All other patterns are invalid.
Invalid initiator	Initiator WWN does not exist or has an invalid name.
Invalid target	Target WWN does not exist or has an invalid name.
Invalid added child entities	Entities either do not exist or entity type is not valid for child association (i.e., wrong hierarchy, such as adding a storage port into a host). Review the added children and remove the invalid children.
Invalid remove child entities	Listed entities cannot be removed or do not exist.
Invalid WWN	WWN is incorrect, does not exist, or has not been discovered yet.

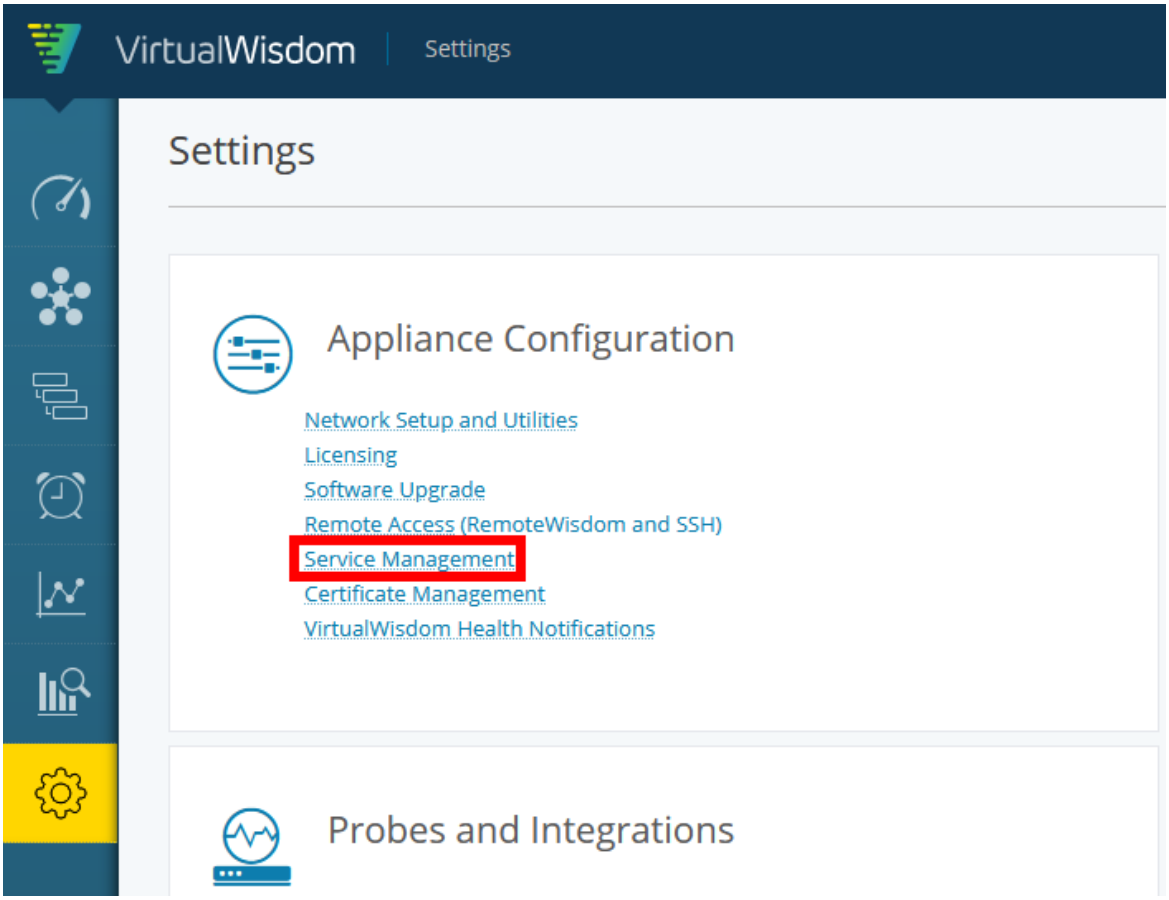
Chapter 5

Service Management

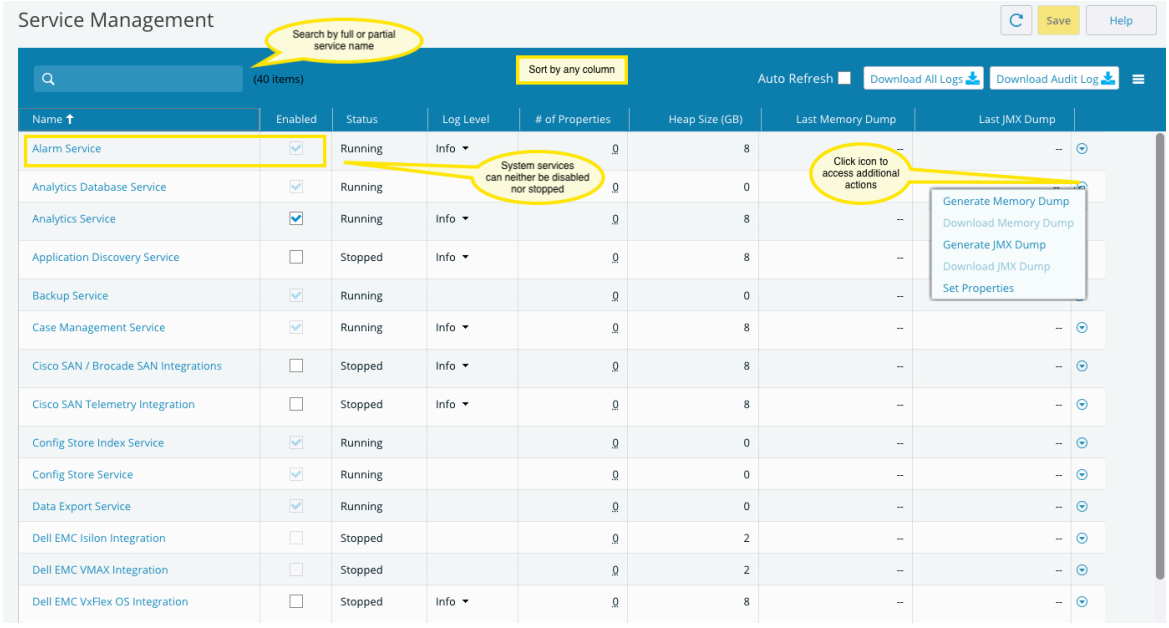
The Service Management function contains a table of specific information related to all VirtualWisdom services. You can also use this tab to download logs, generate JMX or memory dumps, and change log levels.

Follow these steps to access the **Service Management** page.

1. From the **Settings** screen, click **Service Management**.



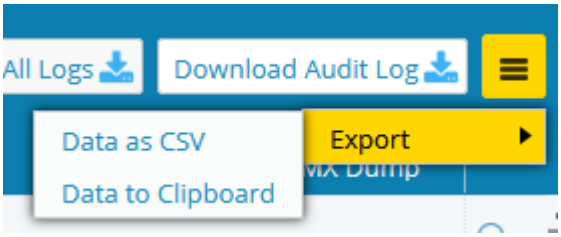
The **Service Management** page displays.



The Column Headings on this page are defined as follows:

Column Headings	Definition
Name	Name of the service.
Enabled	Enabled services have a checkmark in their boxes. Greyed out checkboxes indicate services that can neither be disabled nor have their statuses altered. Enable a service by clicking on its checkbox and then clicking on the **Save** button.
Status	Status of the service. Values are `Running`, `Inaccessible`, `Starting`, or `Stopped`. `Running` means that the service is running. `Inaccessible` means that the service is running, but not responding to requests. `Starting` means that the service is starting and not yet ready to accept requests. `Stopped` means that the service is stopped.
Log Level	Level of debug logging that the service is generating. Valid debug levels are: `Trace`, `Debug`, `Info`, `Warning`, and `Error`. If log levels for a service have been disabled by Virtana, nothing displays in the Log Level column.
# of Properties	Some services have properties that can be modified. This field contains the number of properties that have been modified for the service.
Heap Size (GB)	The current Heap Size setting. Only administrative users may alter heap sizes with a special property in consultation with Virtana Support. Heap size is read-only by default.
Last Memory Dump	Time stamp of the last user-generated Memory dump. If no memory dump has ever been generated, this field contains `-  -`.
Last JMX Dump	Time stamp of the last user-generated JMX dump. If no JMX dump has ever been generated, this field contains `-  -`.

2. You can export the Services list by clicking on the hamburger icon then selecting **Export**.

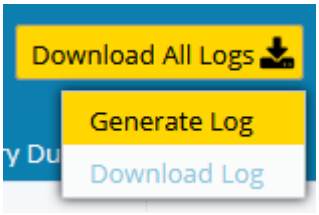


Download All Services Logs

You can download all logs associated with the VirtualWisdom services. These logs include data on crash and core dumps and are occasionally requested by Virtana Support for troubleshooting. These log files are encrypted during download.

1. Click the **Download All Logs** button to view a drop-down menu.

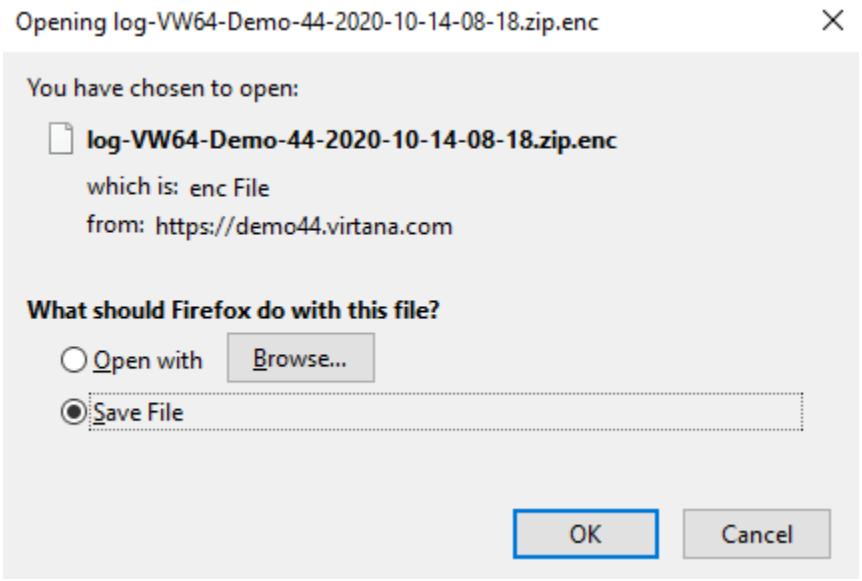
2. Select **Generate Log** to generate the log files.



A banner message is displayed indicating that log file generation is in process.

3. When the log file has been generated, the lettering on the **Download All Logs** button changes to the color blue. To download the generated log file, select **Download** from the **Download All Logs** drop-down menu and select the log file. The drop-down menu also includes the size of the log and the date and time that the log was generated.

The log file is downloaded as an encrypted zip file.

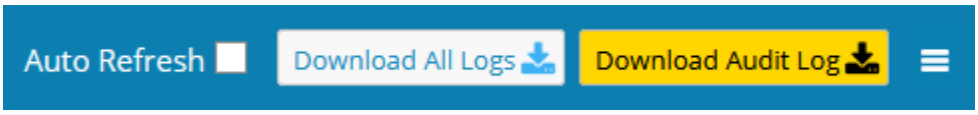


4. You can now send this file to Virtana Support for analysis.

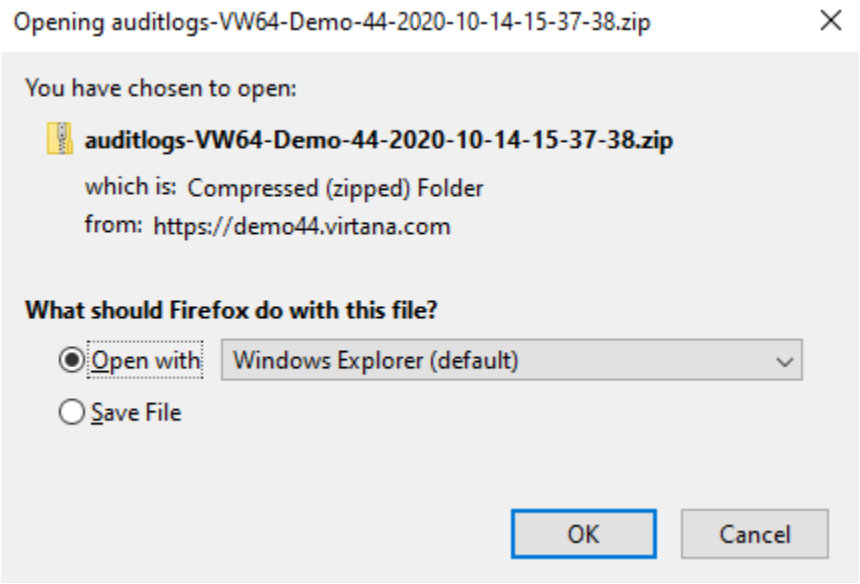
Download Services Audit Log Files

VirtualWisdom tracks user actions and saves these actions in audit logs. You can download these audit logs from the **Service Management** page.

1. Click the **Download Audit Log** button.



2. The log file is downloaded as a zip file.

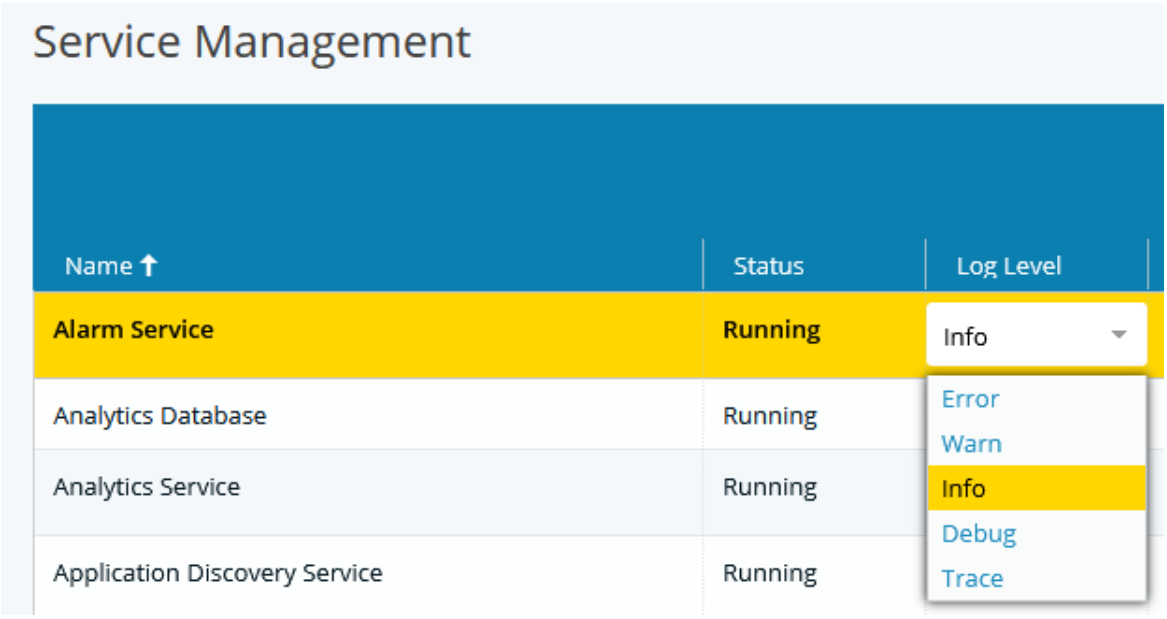


3. You can now send this file to Virtana Support for analysis or unpack and review it.

Change the Log Level on a Service

If log levels for a service have been enabled, you can change the log level for that service.

1. Click the down arrow in the **Log Level** field of the service to modify the level.



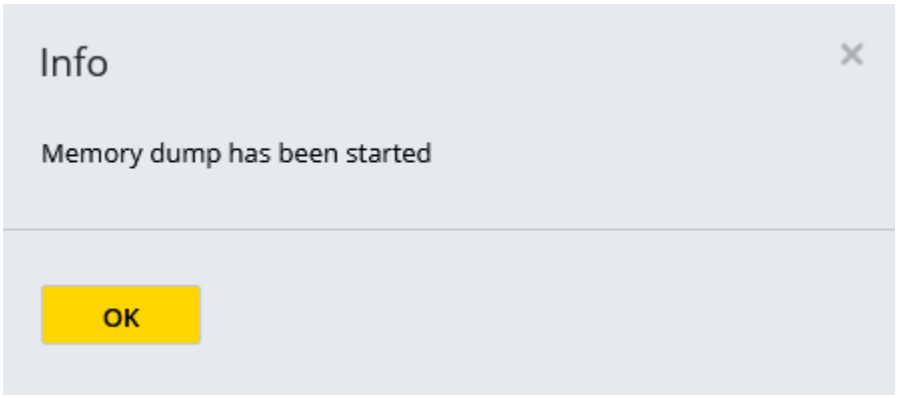
2. Choose the new log level for the service. Allow approximately thirty seconds for the Log Level to refresh.

Generate a Memory or JMX Dump

Virtana Support may request a memory or JMX dump for a service as part of a support ticket. You can use the **Services Management** page to generate and download the file.

1. Click the down arrow in the service's row and select **Generate Memory Dump** or **Generate JMX Dump**.

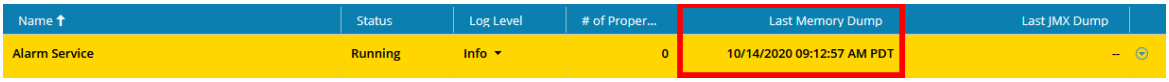
A dialog box confirms the dump has been started.



> **NOTE**
> Generating a memory dump could take some time. A spinner is displayed on the page while the dump is in process.

Check the **Auto Refresh** box to refresh the Services list every 30 seconds.

2. The **Last Memory Dump** or **Last JMX Dump** field is updated with the date and time of the dump.



3. Download the dump by selecting **Download Memory Dump** or **Download JMX Dump** using the drop-down menu for the row.

Set Service Properties

> **WARNING**
> Use the **Set Properties** option only in conjunction with Virtana Support. Do **not** use this button without their direction.

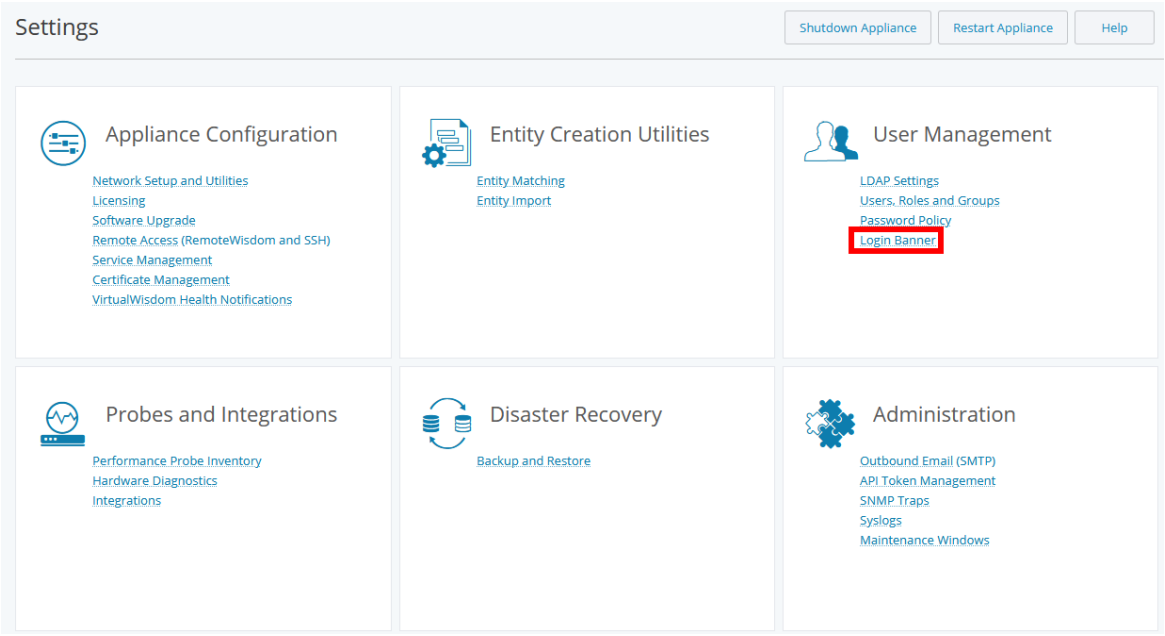
Chapter 6

Administering Your VirtualWisdom Portal

Login Banner

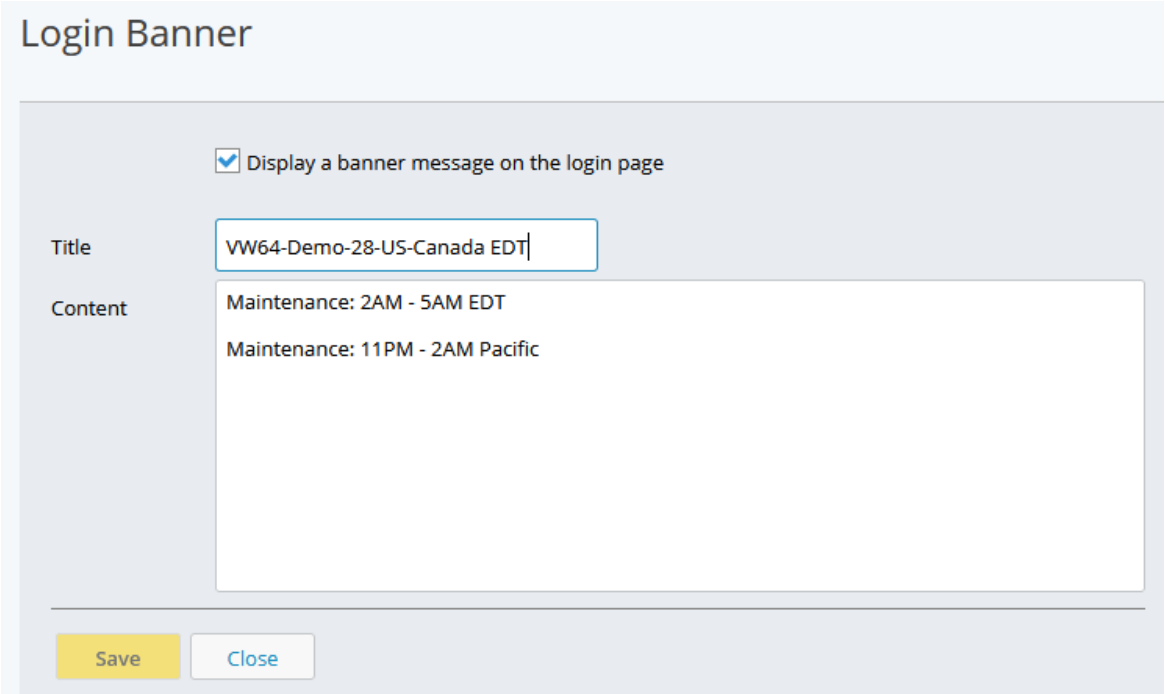
You can change the VirtualWisdom **Login Banner** to provide information, notifications, warnings, and so forth, at the time of login.

1. From the **User Management** section of the **Settings** screen, click **Login Banner**.



The Login Banner page is displayed.

2. Click the checkbox **Display a banner message on the login page**.

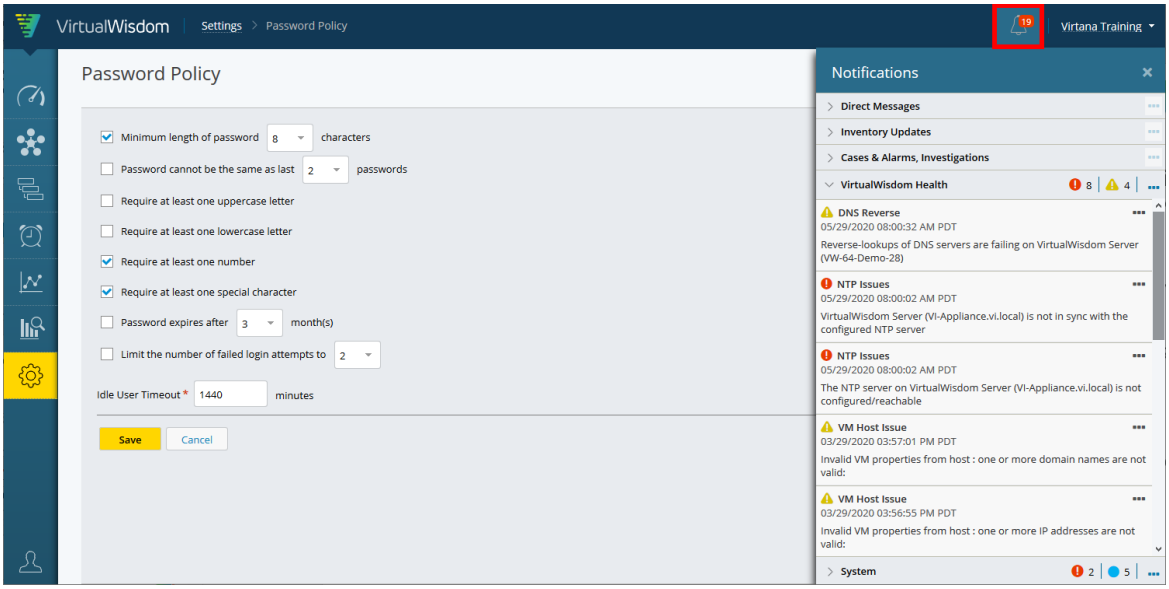


3. Enter a title and content for the banner.
4. Click the **Save** button.
5. To verify the banner displays correctly, log out of VirtualWisdom and view the log in page.

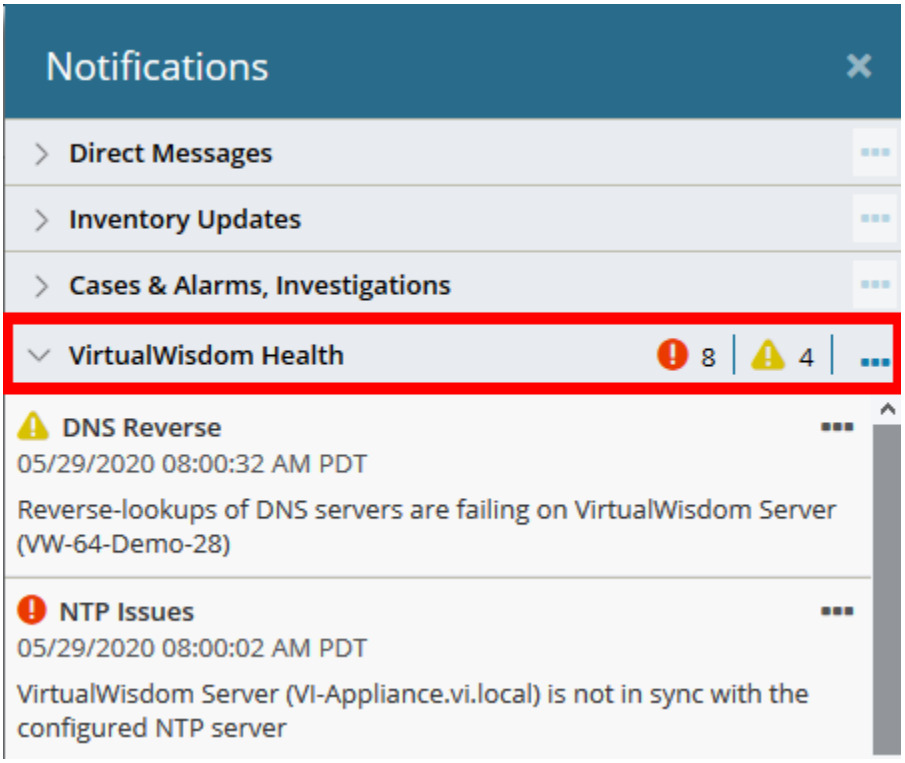
Integration Health Check

VirtualWisdom proactively monitors and alerts on any issues that occur with your integrations. Health issues are tracked using cases.

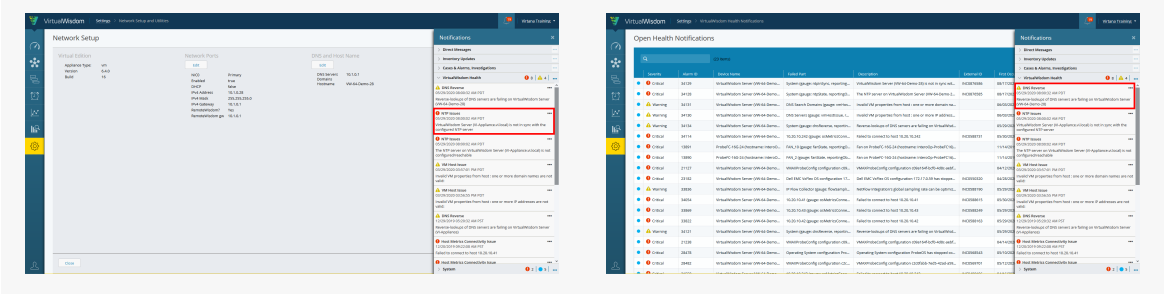
1. Click on the alarm bell at the top right corner of the VirtualWisdom user interface to view notifications on new cases.



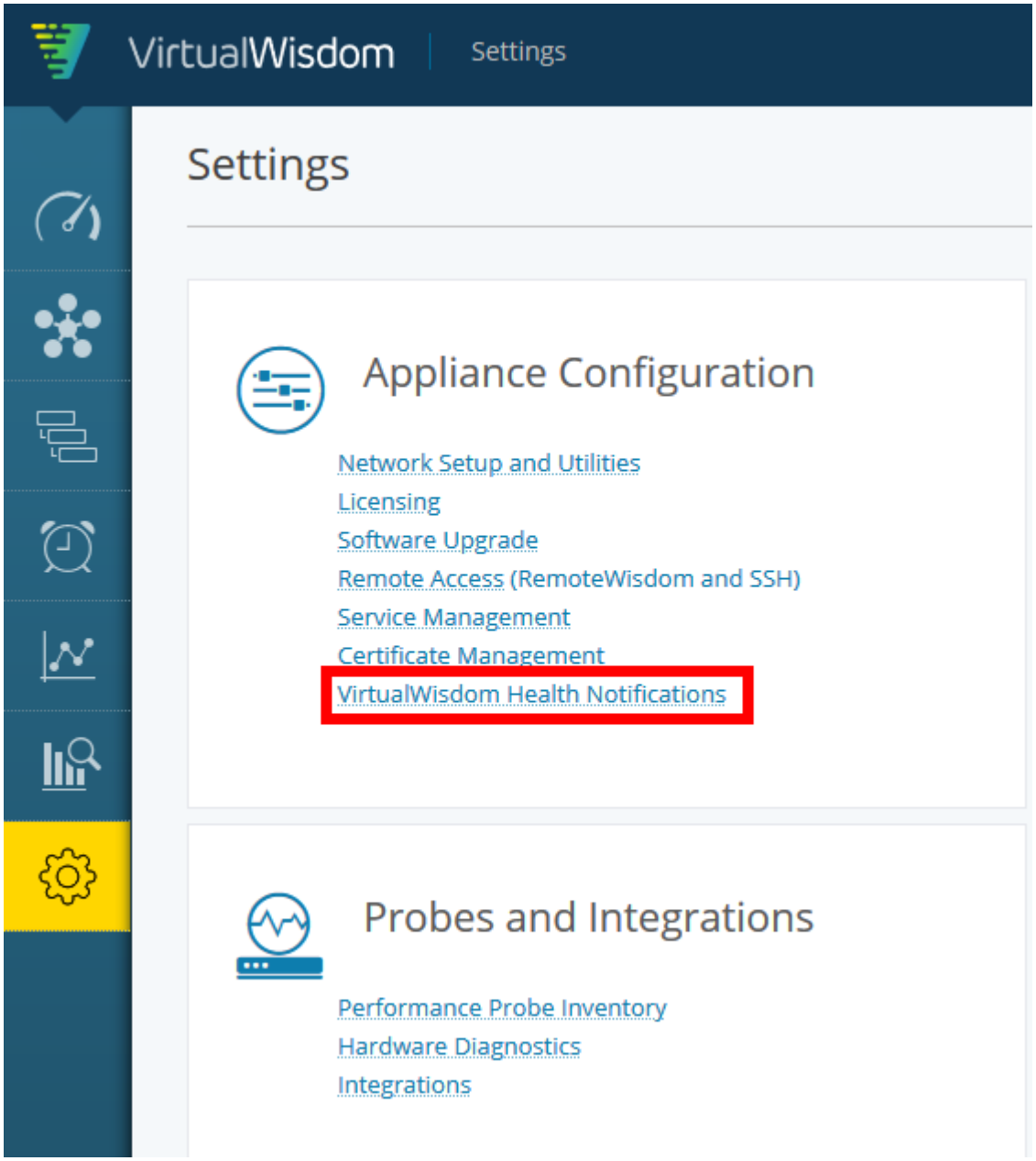
2. Expand the VirtualWisdom Health header to view issues with your integrations. Note that VirtualWisdom Health notifications are visible on to users holding the vw-admin (Administrator) role.



3. Drill down on the notification to view the open case(s). The notifications drawer remains open for reference.

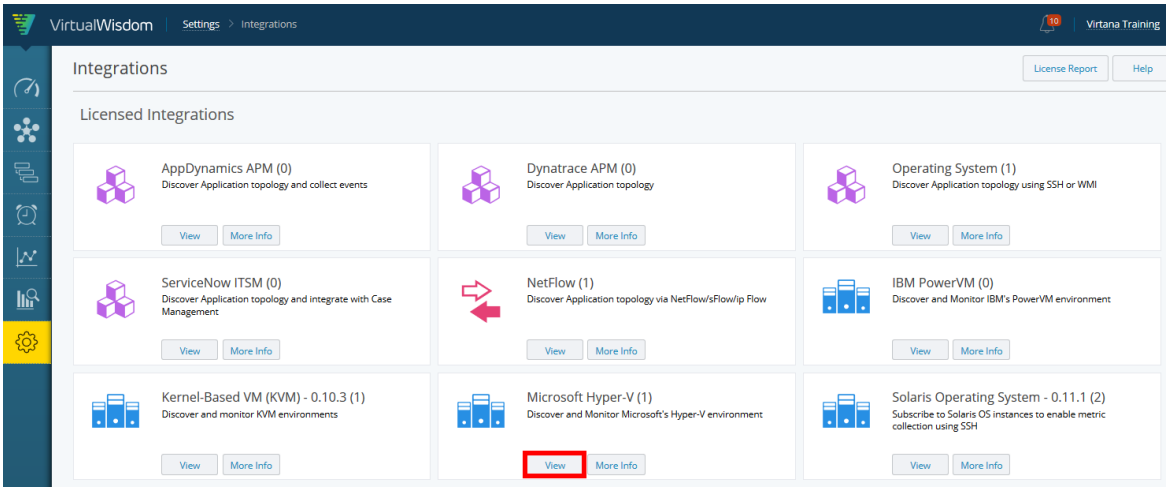


You can also view health notifications from the **Settings** page.

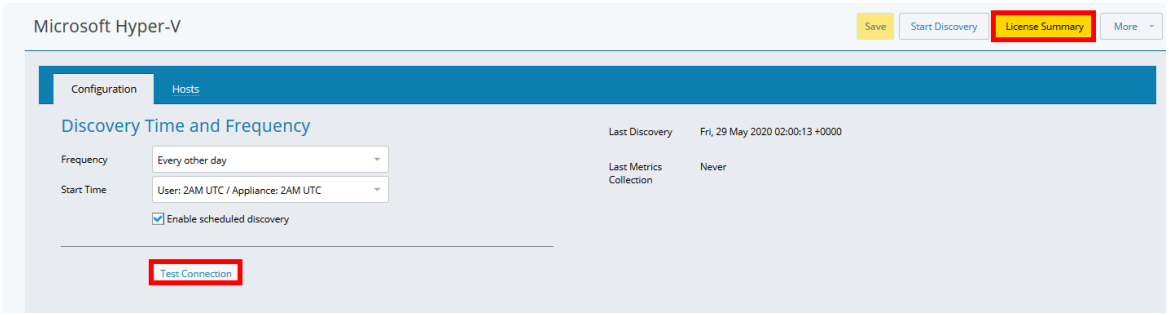


Investigating an Integration Health Issue

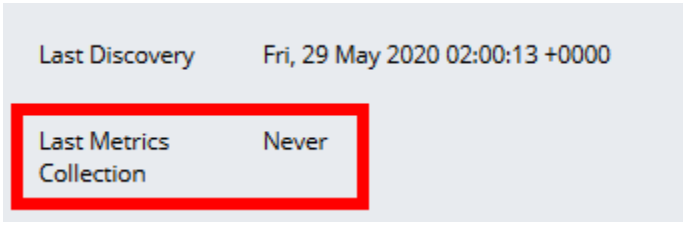
1. From the Integrations page under Settings, select View for the integration you wish to check.



2. Verify licensing by selecting License Summary. Use the Test Connection button to test the connection to the integration.



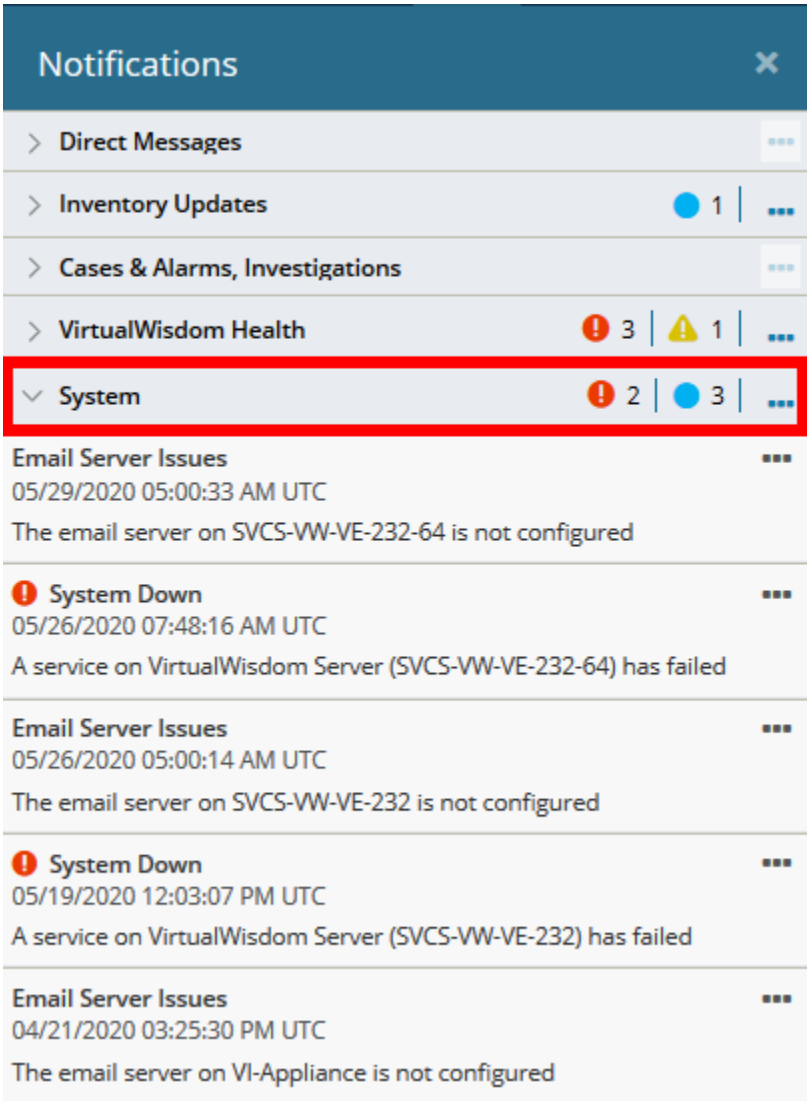
3. Check for successful discovery and metrics collection. Note that navigation for licensing and testing the connection may differ for different integrations, e.g., vSphere vs. Hyper-V.



System Health Notifications

System Health notifications apply to the VirtualWisdom system configuration (not the integrations), e.g., email failures.

1. Access System Health notifications via the notifications drawer. Click the header to expand the notifications.



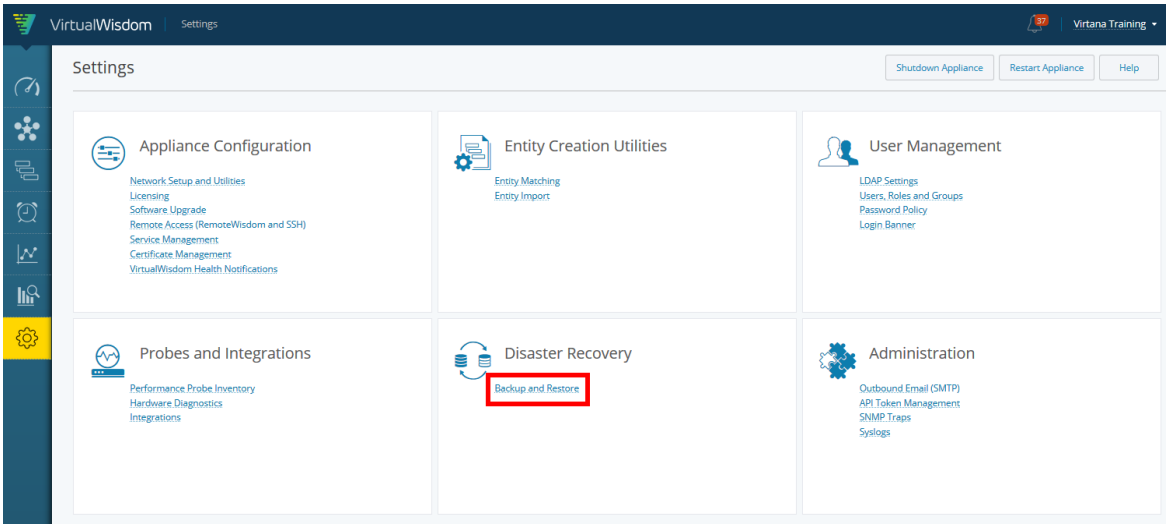
2. Drill down to view the System Health open case.

NOTE
Email server issues are informational only and are not associated with an open case. You cannot drill down on these notifications.

Performing Backups and Restores

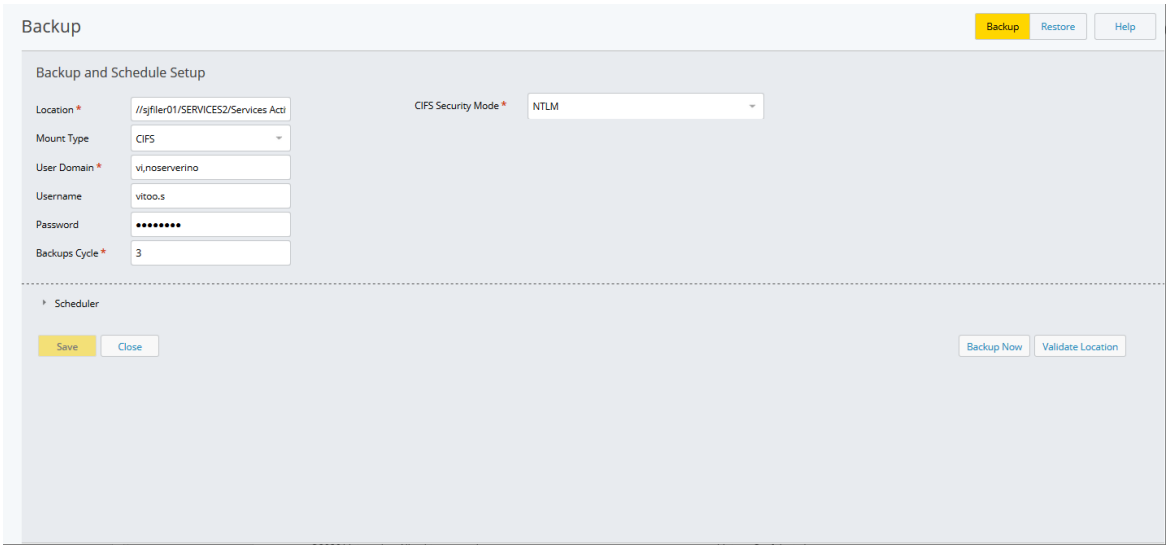
Use the Backup and Restore feature to back up your VirtualWisdom database. The back up feature saves settings, integration configurations, saved content, and configured users. You can set a backup schedule or perform an immediate backup.

1. Select Backup and Restore from the Settings page.



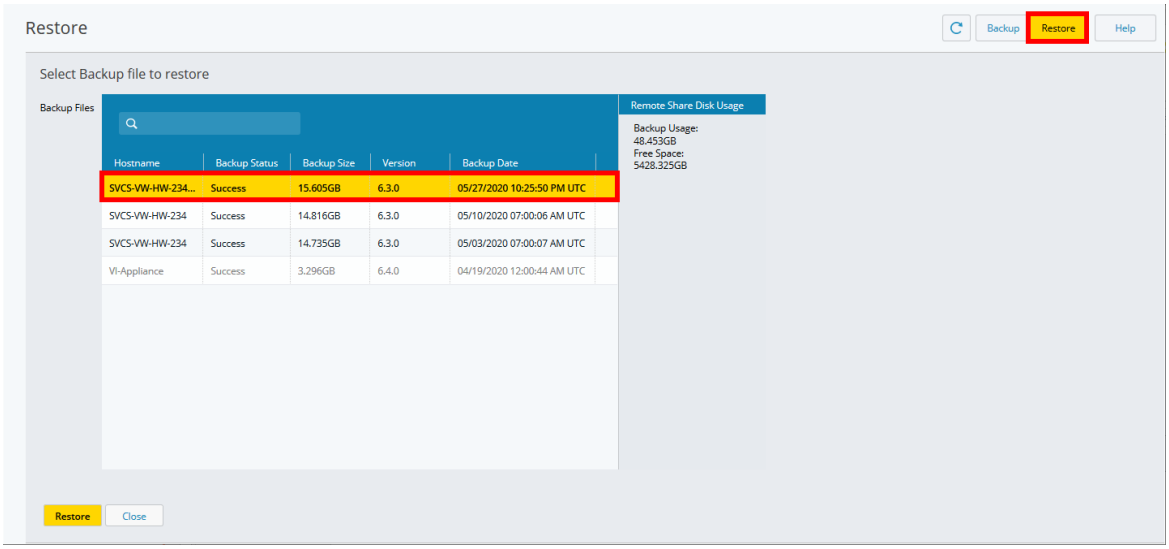
2. **Performing a backup**
   Use the Backup page to specify a location, mount type, user info, number of backups to maintain (Backups Cycle), advanced options based on the mount type, and schedule.

> **NOTE**
> For customers who have deployed more than one Appliance or Virtual Edition instance, it is recommended that separate share drives are used to back up each instance.



3. **Performing a restore**

   Select the Restore button to perform a restore of your VirtualWisdom database. You'll need to select a backup file to use in the restoration process.



Outbound Mail (SMTP)

The **Outbound Email (SMTP)** task on the *Settings* page enables you to configure settings for outbound emails. The outbound email server is used for SAN alarm notification. VirtualWisdom also uses it to notify users configured with the *admin* role of any VI infrastructure issues, such as a loss of communication to a Performance Probe.

Email notifications are not distributed to configured users until the user has logged into VirtualWisdom for the first time.

API Token Management

As an alternative to UI access, APIs provide stateless, token-based authentication access to some VirtualWisdom Appliance configuration functionality, including:

- Network, DNS, Host Name
- User Management (create, update delete)
- LDAP server configuration
- Email (SMTP server)
- Syslogs

The token is an auto-generated random alphanumeric identifier composed of user-visible and secret parts. The secret part is visible only during the generation process, when it can be copied to scripts that access the APIs.

Displaying Token Information

1. Click the **API Token Management** function on the *Settings* tab.
   The *API Token Management* page is displayed.
2. To display or edit information about an API token, click the row.
   The *Update API Token* screen is displayed. You can change the expiration date and/or description.

Field	Definition
API Key	User-visible key
Created By	User ID of creator
Created On	Token generation date (optional)
Expiration Date	Date expires
Description	Function of the token

3. If you make changes, click the **Save** button.
   To create a new token:
4. Click the **Create New Token** button.
   The *Create API Token* page is displayed.

Specify an expiration date (optional) and a description.

5. Click the **Save** button.
   The *API Secret and Key* page is displayed. The secret part of the key is highlighted so it can easily be copied.

> **NOTE**
> This is the only time in the process that the secret part of the key is displayed. If you forget the key, generate a new token.

6. Copy the highlighted **Secret** field.
7. Click **OK**.
   The *Create API Token* page is displayed. The token is added to the existing list, and public identifier is shown in the *API Key* field.
8. Paste the secret token into the script(s) to be submitted to the API.

SNMP Traps

VirtualWisdom offers Simple Network Management Protocol (SNMP) trap notifications, which are enabled per alarm rule. Notifications are sent out once per case, at the first occurrence of each case. VirtualWisdom supports SNMP Version 2 and Version 3 notifications.

The **SNMP Trap Settings** task on the *Settings* tab allows to specify the destination settings for SNMP trap notification as well as download SNMP MIB files.

Set SNMP Trap Settings

1. From the *Settings* tab, click **SNMP Traps** to access the *SNMP Trap Settings* page.
2. Enter the following information in the *SNMP Trap Settings* page:

Table 28. SNMP Settings for Version 2

Field	Definition
Destination Hostname	Hostname of the SNMP trap destination.
Port	Port used for SNMP trap communication.

Field	Definition
Community String	SNMP community string value (alphanumeric). This field is optional.
SNMP Version	SNMP version to be used is v2c.
Send Alarm Notifications to this SNMP Receiver	Check box on by default.
Send VirtualWisdom Health Notifications to this SNMP Receiver	Check box on by default.

Table 29. SNMP Settings for Version 3

Field	Definition
Destination Hostname	Hostname of the SNMP trap destination.
Port	Port used for SNMP trap communication.
SNMP Version	Available SNMPv3 versions are: - v3 No Auth No Privacy - v3 Auth No Privacy - v3 Auth Privacy
Username	A user id, such as community, which is required to be defined in SNMPv3.
SNMP Auth Password	Password administering the Authentication Protocol.
SNMP Auth Protocol	Protocol defined to ensure the identity of users. Supported protocols are: MD5 and SHA.
SNMP Privacy Password	Password administering the Privacy Protocol.
SNMP Privacy Protocol	Protocol defined to allow for encryption of SNMPv3 messages that ensure confidentiality of data. Supported protocols are: AES and DES.
Send Alarm Notifications to this SNMP Receiver	Check box on by default.
Send VirtualWisdom Health Notifications to this SNMP Receiver	Check box on by default.

3. Click **Save** to save the settings.
4. Click **Close** to return to the **Settings** page.

Download SNMP MIB Files

1. From the *Settings* tab, click **SNMP Traps** to access the *SNMP Trap Settings* page.
2. Click **Download SNMP MIB** to download the SNMP MIB files.
   This begins the SNMP MIB download process. You can view or upload the SNMP MIB files after they have been downloaded.
3. Click **Close** to return to the **Settings** page.

Syslogs

Syslog servers can be used redirect logging to an external server. Such logging can be related to system management, security, general informational, analysis, or debug.

Use the **Syslogs** task on the *Settings* tab to add, modify, or delete a syslog server. You can also send a test message to the syslog server to verify its configuration.

Proxy Servers

If your corporate security requirements include using proxies for internet access, you can add proxy servers to your integration configuration. You can use only one proxy server per integration type, but each proxy can be used with multiple integration types. Currently, ServiceNow is the only VirtualWisdom integration that supports proxy servers.

Maintenance Windows

Maintenance Windows in VirtualWisdom are used to suppress alarm notifications during specified time periods. Maintenance Windows are designed to reduce the number of false alarm notifications generated during known periods of abnormal activity. The intention of the Maintenance Windows feature is to increase the reliability of alarm notifications and drive up alarm notification usage.

Edit a Maintenance Window

1. From the *Administration* section of the *Settings* screen, click Maintenance Windows.
   The *Maintenance Windows* screen contains a grid that shows all of the currently configured maintenance windows.
2. Identify the maintenance window entry that you want to update and click on it.
   The *Edit Maintenance Window* screen displays.
3. Modify the fields that you need to update:

Field	Definition
Name	User-defined name for the maintenance window.
Date	Calendar date for the maintenance window. Also has option to select *Today*.
Time	Time of day for the maintenance window to begin, with options listed in 15 minute increments.
Duration	Time duration for the maintenance window.

- Scope
  Use the *Scope* settings to specify which entities to suppress during the maintenance window. The *All Entities* radio button is the default, and suppresses alarms on all entities during the maintenance window. Select the *Selected Entities* radio button to suppress alarms on specific entity types during the maintenance window.
- Recurring
  Use the *Recurring* checkbox to specify constraints for a monthly, weekly, daily, or hourly recurrence of the maintenance window.

4. Click **Save**.
5. Verify that the maintenance window is updated by verifying its entry on the *Settings> Maintenance Windows* page.

Delete a Maintenance Window

1. From the *Administration* section of the *Settings* screen, click **Maintenance Windows**.
   The *Maintenance Windows* screen contains a grid that shows all of the currently configured maintenance windows.
2. Identify the maintenance window entry that you want to delete.
3. Hover your cursor over the entry and click the **x** at the end of the row.
   A *Warning* dialog appears, asking you to confirm the deletion.
4. Click OK.
   The entry is deleted and no longer displays on the *Settings> Maintenance Windows* page.

Chapter 7

Contact Information

Sales Inquiries

To speak with a sales representative:

Complete the form at virtana.com/contact-us/.

Call us at +1-888-522-2557.

Support for VirtualWisdom Core and Integrations

VirtualWisdom support is available 24/7

Online Support

www.virtana.com/support

Technical Support

virtualwisdom.support@virtana.com

Weekend Severity 1 HOTLINE (For VirtualWisdom ONLY):

Toll Free: 1-888-988-9925

International: +1-408-579-4100

Feedback

We appreciate your input to help us improve the quality of our products and documentation. Send your suggestions, comments, and questions about Virtana products and documentation to:

Product Feedback

feedback@virtana.com

Documentation Feedback

techpubs@virtana.com

Chapter 8

Legal

Copyright

Virtual Instruments reserves the right to revise these specifications without notice or penalty.

Trademarks

Dell Technologies, Dell, EMC, Dell EMC, Isilon, Unisphere, VMAX, and other trademarks are trademarks of Dell Inc. or its subsidiaries.

IBM® and PowerVM® are registered trademarks of IBM Corporation in the United States, other countries, or both.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Windows Server®, and Hyper-V™ are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp®, OnCommand®, and ONTAP® are registered trademarks of NetApp, Inc., registered in the U.S. and/or other countries.

Oracle®, Java, and Solaris are registered trademarks or trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Pure Storage, the Pure Storage logo and the marks listed at http://www.purestorage.com/legal/productenduserinfo.html are trademarks or registered trademarks of Pure Storage, Inc. in the U.S. or other countries.

VMware®, vCenter®, and vSphere® are registered trademarks of VMware, Inc. in the United States and other jurisdictions.

VirtualWisdom is a registered trademark of Virtual Instruments Corporation (d/b/a Virtana).