



Virtual Traffic Manager Tenant Administration Guide

VTM Tenant Admin Guide

CONTENTS

1. About This Guide 3

2. Preface 4

3. END USER LICENSE AGREEMENT 6

4. What's New 7

5. Overview of Virtual Traffic Manager 8

6. Logging in as a Tenant Administrator 9

7. Registering Virtual Traffic Manager Gateway 14

8. Working with Gateways 16

9. Virtual Traffic Manager Analytics 19

10. Licensing/Subscription 26

1. About This Guide

The purpose of the document is to list the various aspects of the purchased bandwidth feature that will allow user to subscribe and allocate bandwidth to configured / registered Virtual Traffic Manager (vTM) gateways.

It covers the following subject areas:

- An overview of vTM and concepts. See [Overview of Virtual Traffic Manager](#)
- Logging into the Controller as a Tenant Admin. See [Logging in as a Tenant Administrator](#).
- Setting up one or more Gateways. See [Registering Virtual Traffic Manager Gateway](#) and [Working with Gateways](#).
- Using analytics to monitor your VTM platform and services. See [Virtual Traffic Manager Analytics](#).

2. Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in (Undefined variable: Custom.Company_Name) technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
<i>italic text</i>	Identifies emphasis
	Identifies variables
	Identifies document titles
<code>Courier Font</code>	Identifies command output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.
bold text	Identifies command names, keywords, and command options.

Code Block

Following is an example of Python based code block in the html documentation:

Bash

```
def some_function():
    interesting = False
    print 'This line is highlighted.'
    print 'This one is not...'
    print '...but this one is.'
```

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

3. END USER LICENSE AGREEMENT

The Ivanti product that is the subject of this technical documentation consists of (or is intended for use with) Ivanti software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://www.ivanti.com/company/legal/eula>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

4. What's New

The vTM Gateway versions listed below are the supported versions to use with nSA for respective releases:

- vTM 22.3R2

Version 22.7R1.2

✓ Virtual Traffic Manager Life Cycle Management

Ivanti Neurons for Virtual Traffic Manager (VTM) provides admin to:

- reboot gateway
- restart services

and to view progress of operation and status of the following operations:

- Downloading a software package for upgrade
- Upgrading the gateway's version
- Gateway certificate renewal
- Rebooting gateway
- Restarting gateway
- Rolling back gateway to previous version

For details, see [Viewing vTM Gateway Details](#) and [Monitoring vTM Gateway](#)

Version 22.6R1

✓ Virtual Traffic Manager Analytics

Ivanti Neurons for Virtual Traffic Manager (VTM) provides visibility of network activity and service usage across your enterprise through network activity analytics and performance graphs. For details, see [Virtual Traffic Manager Analytics](#).

Version 22.4R1

✓ Virtual Traffic Manager Gateway Registration

Virtual Traffic Manager (vTM) Gateway registered with Ivanti Neurons for Secure Access (nSA) allows the admin with the following capabilities:

- Provisioning feature packs to be used during the tenant creation.
- Option to select feature pack during tenant creation.
- Option for tenant to select feature pack and/or bandwidth for a gateway.

For details about registering a vTM, see [Registering Virtual Traffic Manager Gateway](#).

5. Overview of Virtual Traffic Manager

Neurons for Secure Access (nSA) is a SaaS-delivered, centralized management and reporting platform designed to work with Ivanti Connect Secure (ICS), Neurons for Zero Trust Access (nZTA) and Virtual Traffic Manager (vTM) Gateways.

Feature Pack is a set of features that are enabled along with a bandwidth. When feature pack is applied to one or more gateways, it in turn enables the features on the gateways. With respect to the bandwidth, user can assign an unallocated portion of the bandwidth in feature pack to the individual gateway.

For Example:

If a feature pack specifies a bandwidth of 1000 Mbps, the user is able to allocate this across multiple gateways considering how much is unallocated. The user is informed about the unallocated bandwidth available in the feature pack. When adding a gateway, user can select the feature pack and allocate a specific bandwidth to the gateway.

Admin can also modify the feature pack and / or allocate bandwidth for the gateway. If there is overallocation or under allocation of the bandwidth, the Admin will be notified.

vTM Gateway registered with nSA allows the admin with the following capabilities:

- Provisioning feature packs to be used during the tenant creation.
- Option to select feature pack during tenant creation.
- Option for tenant to select feature pack and/or bandwidth for a gateway.

For details about registering a vTM Gateway, see [Registering Virtual Traffic Manager Gateway](#)

Limitations and Assumptions

- Feature pack for the scope of this release is considered to be "Enterprise".
- Maximum bandwidth per tenant across feature packs is set to 80,00,000 Mbps. It means, if a tenant has two feature packs and bandwidth for one subscription is 10,00,000 Mbps, then for the other feature pack the maximum bandwidth allowed is 70,00,000 Mbps.
- Maximum bandwidth per vTM that can be set is 80,000 Mbps (80Gbps).
- Feature packs cannot be added / modified / deleted. Feature pack is set to a feature that contains a fixed set of features that cannot be modified.
- Cluster management of a vTM cluster is not supported. This means creating a vTM cluster is not possible from the nSA UI.
- Bandwidth usage analytics is not supported.

6. Logging in as a Tenant Administrator

- [Preparing to Login](#)
- [Logging into the Controller as a Tenant Admin](#)
- [Logging out of the Controller](#)

Preparing to Login

As a Tenant Admin, you can configure *Ivanti Virtual Traffic Manager (vTM)* to support the Gateways and resources that are required for your organization's *vTM* implementation.

To log into the *Controller*, you require a Tenant Admin login.

All Tenant Admin accounts are set up by the *Ivanti* DevOps team. Once your Tenant Admin account has been created, you will receive an email which describes how to log into the *Controller* as a Tenant Admin.

You can then proceed to login to the *Controller*, see [Logging into the Controller as a Tenant Admin](#).

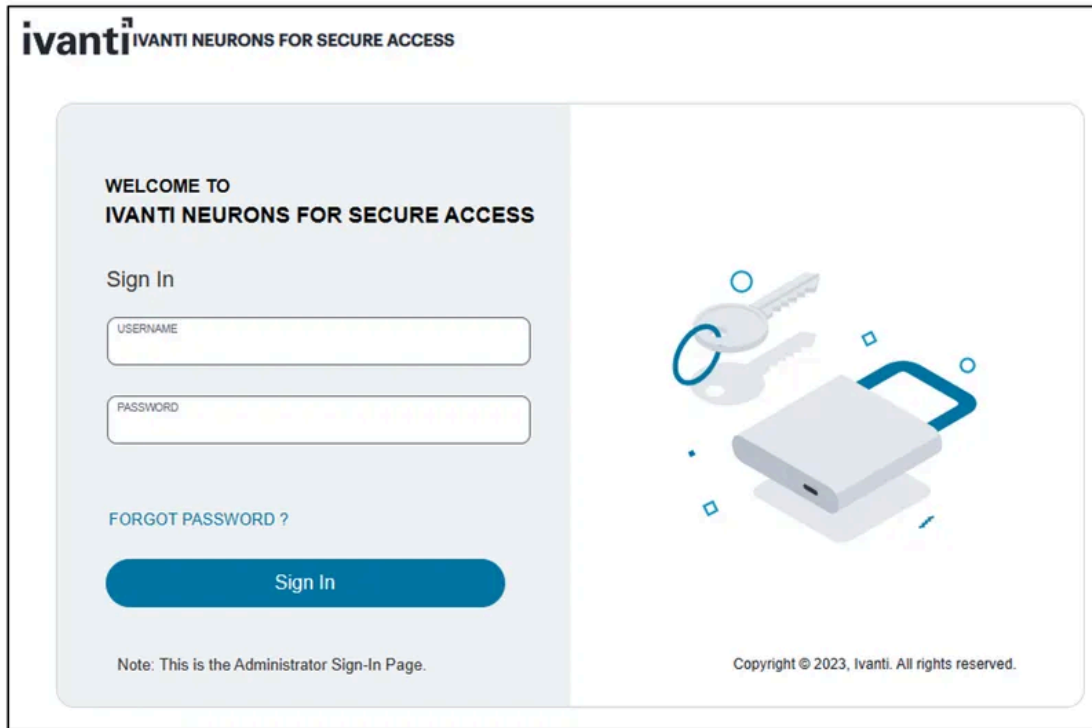
Logging into the *Controller* as a Tenant Admin

Before you can log in as a Tenant Admin, you will receive an email from the *Ivanti* DevOps team. This email contains:

- Your Tenant Admin user name.
- Your password.
- The *vTM* domain. That is, the FQDN of the *Controller*.
- A hyperlink to start the login process.

To log into your Tenant Admin account:

1. Click the hyperlink in your email.
The administrator login page appears.



Tenant Admin Login Page

Log in using your supplied Tenant Admin credentials.

3. If *vTM* requests it, specify a new password for your account.

Once this procedure is complete, you access the *vTM* graphical interface as an admin user. The graphical user elements that appear depend on your configured state.

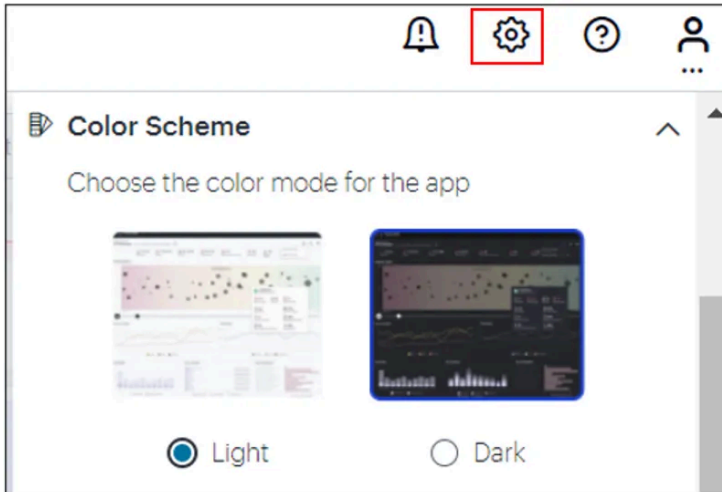
To reset a forgotten password, click **FORGOT PASSWORD**. This link presents a credentials form through which you enter a Username and Email address. If the entered credentials match a registered administrator account, *vTM* emails a password reset link to the entered address allowing the recipient to create a new password.

The Gateways page lists the *vTM* Gateways that are configured on nSA. For details about adding new gateways, see [Registering Virtual Traffic Manager Gateway](#).

Changing the UI Theme

nSA offers two themes for your UI display:

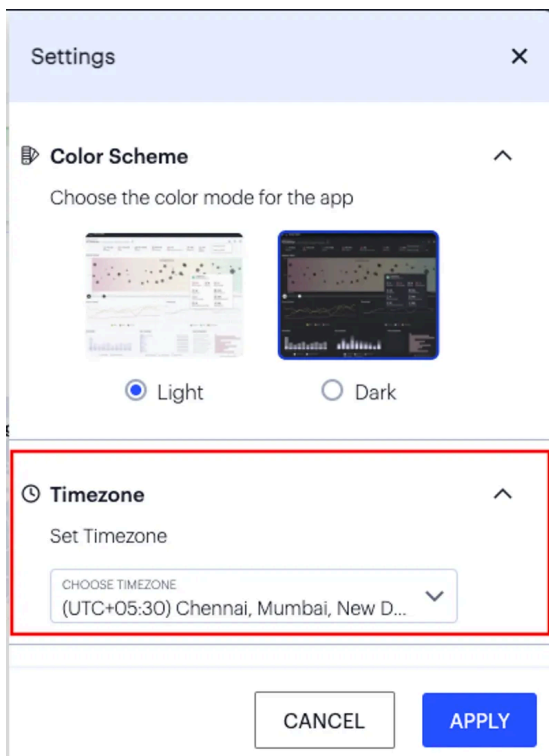
To change the current theme, which remains in place through subsequent logins, use the **Settings** menu located on the top-right-corner of the page:



Through the **Color Scheme** panel (indicated), click **Light** or **Dark** to switch between themes.

Setting the Timezone

To configure the default timezone for this admin login account, use the **Settings** menu located on the top-right-corner of the page:



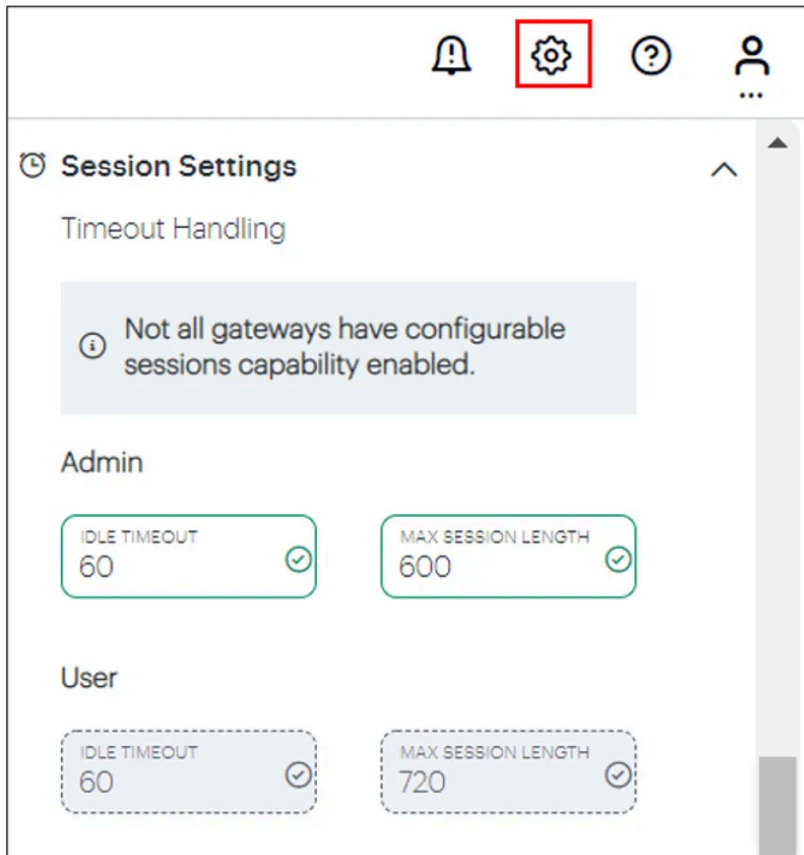
Choose a timezone in the provided drop-down selector, then click **Apply**.

The configured timezone affects the display of data on all **Insights** pages, and each admin login account within a tenant deployment has their own specific timezone configuration. Changes to the timezone persist across login sessions, and the default setting is *UTC (Coordinated Universal Time)*.

Changing the timezone can affect the data displayed in each chart or graph. For example, a recently-observed non-compliance event involving a client device in the GMT timezone that appears in the *Last Hour* view (when using GMT (UTC + 00:00) as your configured timezone) might then only appear in the *Last X Hours* view when you switch your timezone to IST (UTC+05:30).

Configuring Session Timeouts

To configure timeout values for admin and user sessions, use the **Settings** menu located on the top-right-corner of the page:



Through the **Session Settings** panel (indicated), you can set the following timeout values:

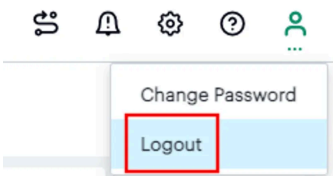
- **Admin Idle Timeout:** the time, in minutes, after which the admin login session to the Tenant Admin Portal times out due to inactivity. (default: 10)
- **Admin Max Session Length:** the time, in minutes, after which the admin login session to the Tenant Admin Portal ends and must be re-authenticated. (default: 60)
- **User Idle Timeout:** the time, in minutes, after which the user login session to nSA times out due to inactivity. (default: 60)
- **User Max Session Length:** the time, in minutes, after which the login session to nSA ends and must be re-authenticated. (default: 720)

To apply your changes, click **APPLY**.

To use these settings, your configured Gateways must all meet minimum version requirements for session control. nSA disables the panel and displays a warning message if this is not the case.

Logging out of the *Controller*

To log out of the *vTM* Tenant Admin Portal and end the current session, click the *Profile* icon and select **Logout**.



7. Registering Virtual Traffic Manager Gateway

Once you have logged into the Ivanti Neurons for Secure Access, you can register one or more vTM Gateways.

Before registering a vTM Gateway, ensure that the vTM GW is reachable and connection status is in "Connected" status.

To launch vTM Gateway UI:

1. In the Ivanti Neurons for Secure Access UI, select the Gateway Switcher icon located on the top left corner.



1. From the list, select **Ivanti Virtual Traffic Manager**.
The Virtual Traffic Manager UI page is displayed.

To register vTM Gateway:

1. From the Virtual Traffic Manager menu, click the **Gateways** icon, then select **Gateways > Gateways List**.
2. In the Gateways page that is displayed, click the **Create** drop-down list.



1. From the Gateway types list, select **vTM Gateway**.
The Register vTM Gateway page is displayed.

Register vTM Gateway

Gateway Details

To register a new gateway, enter the gateway name, location and feature pack along with bandwidth

NAME

Location

COUNTRY STATE/REGION CITY

Licensing

FEATURE PACK Bandwidth(Mbps)

Registration Summary

1. Enter a unique name for vTM gateway.

The name should be maximum 16 characters, only alphanumeric, underscores, and hyphens are allowed between characters, and **must start with a letter**.

1. Select your Location details such as Country, State / Region, and City.
2. Select your Licensing details such as Feature Pack and Bandwidth for the gateway.
If there is overallocation or under allocation of the bandwidth, the Admin will be notified.
3. Click **Register**.

The Registration Summary page contains the FQDN URL and Registration Key, which you need to enter in the vTM Gateway to complete the registration.

Pulse Secure Virtual Traffic Manager Community Edition Purchase license here: 22-6a1

Cluster: OK 0/0/0

Home Services Catalogs Diagnose Activity System Web Application Firewall Wizards Help

System Traffic Managers Fault Tolerance Web Application Firewall Networking Alerting SNMP Security Users Backups Licenses Analytics Export Global Settings Ingress Controller

License Keys Unfold All / Fold All

Your traffic managers need valid license keys to operate. License keys are restricted by IP address or MAC address, and may be limited to certain versions or dates. They may enable additional optional product features.

10.38.135.24
License Serial: Community_Edition

Installed License Keys

The following license keys are installed on your traffic manager:

License Serial	Details
Community_Edition	Used by traffic managers: 10.38.135.24

Install new License Key

Key file: No file chosen

Services Director Registration

Your traffic manager can register itself with a Services Director, for remote licensing purposes.

Ivanti Neurons for Secure Access Registration

Your traffic manager can register itself with Ivanti Neurons for Secure Access, for remote licensing purposes.

This should be the FQDN of your Ivanti Neurons for Secure Access controller
Registration FQDN:

This should be the registration key of your Ivanti Neurons for Secure Access controller
Registration Code:

1. Click **Close**.

The newly added vTM Gateway gets listed under vTM Gateways list. You can edit the Gateway configuration or delete the Gateway. For details, see [Working with Gateways](#).

8. Working with Gateways

- [Introduction](#)
- [Viewing vTM Gateway Details](#)

Introduction

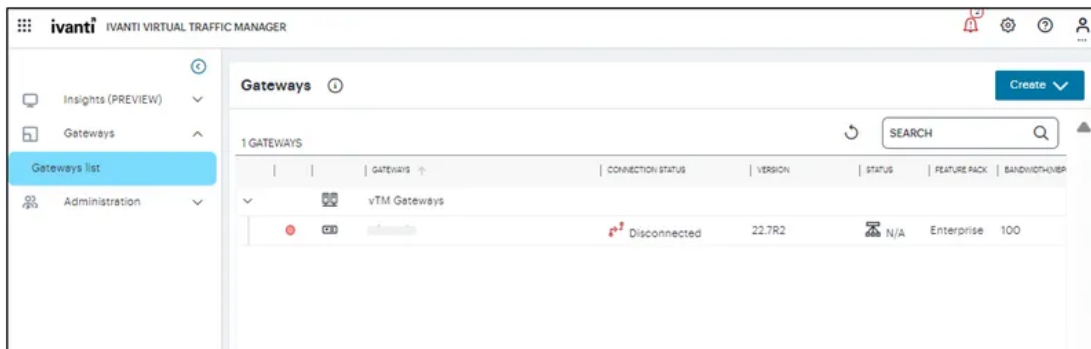
After you have successfully logged into the *Ivanti Neurons for Secure Access (nSA) Controller* as a Tenant Admin user (see [Logging in as a Tenant Administrator](#)), you can start the configuration of your vTM platform by adding Gateways.

nSA supports the following main Gateway types, depending on your subscription:

- nZTA Gateway
- *Ivanti Connect Secure (ICS)* Gateway
- Virtual Traffic Manager (vTM) Gateway

This chapter covers functionality relating to a vTM Gateway only. For details pertaining to nZTA and ICS Gateways, see the respective Tenant Admin Guide in the *Ivanti* documentation portal.

A Gateway controls access to the applications at the location to which it is deployed. This location could be a physical datacenter, a private or public cloud-based service, or some hybrid combination. Each Gateway communicates with the *Controller* to ensure that access requests are authenticated. A Gateway must be contactable by both the *Controller* and the applications that reside there.

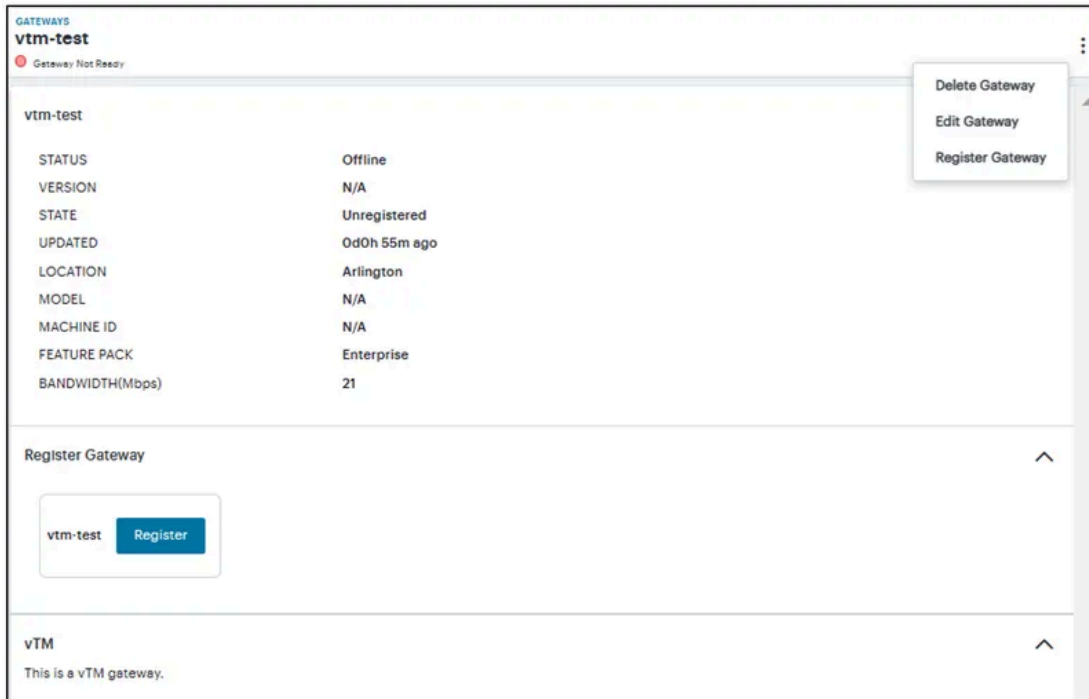


Viewing vTM Gateway Details

After you have registered your Gateways with the *Controller*, you can:

- View the list of Gateways
The gateway list page displays the additional columns to show the connection status, vTM version, feature pack used and the bandwidth allocated to the gateway.
- View the summary of the Gateway configuration
- Edit the Gateway configuration
- Delete a Gateway

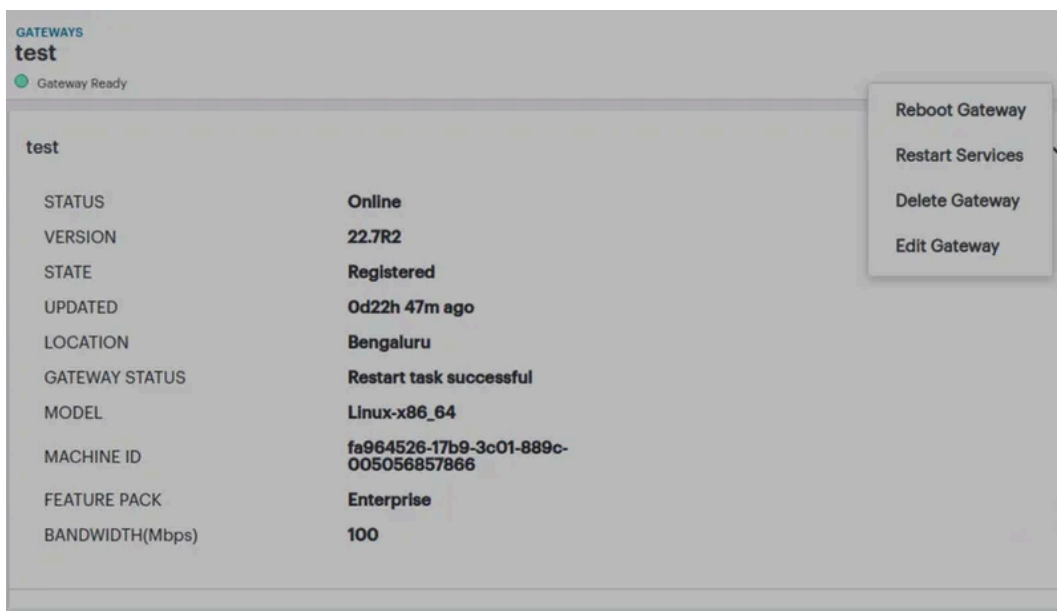
When you select a Gateway from the Gateways list, the Gateway details page displays the configuration information for the selected Gateway.



You can edit, delete, reboot or restart the Gateway from this page.

1. In the Gateways List page, click the Gateway name link.

The Gateway details page appears.



2. Click the three dots located on the top-right corner.

- To edit the Gateway, click **Edit Gateway** and in the screen that appears, select a different feature pack or allocate a different bandwidth, and then click **Save**.
- To delete the Gateway, click **Delete Gateway** and in the delete confirmation screen that appears, click **Confirm**.
- To reboot the Gateway, click **Reboot Gateway**. The Gateway is available again after a few minutes.

- To restart the services, click **Restart Services**. The Gateway is available again after a few minutes.

Monitoring vTM Gateway

An admin can view the progress of operation and status of the operation:

- Downloading a software package for upgrade
- Upgrading the gateway's version
- Gateway certificate renewal
- Rebooting gateway
- Restarting gateway
- Rolling back gateway to previous version

To open the gateway task page:

1. In the Gateways list page, click the Gateway name link.

The Gateway Details page appears.

2. In the left navigation, select **Gateway list > <Gateway name> > Tasks**.

The Tasks page displays the list of tasks.

3. In the Tasks page, choose the required task type from the drop-down list and period to view the details.

GATEWAYS

Gateway Not Ready

TASK TYPE

Choose your option

Choose your option

Downloading a software package for upgrade

Upgrading the gateway's version

Gateway certificate Renewal

Rebooting gateway

Restarting gateway

Rolling back gateway to previous version

STARTING FROM

05/17/2024

Clear

STATUS DESCRIPTION	CREATED DATE	CREATED TIME	COMPLETED DATE	COMPLETED TIME
--------------------	--------------	--------------	----------------	----------------

9. Virtual Traffic Manager Analytics

- [Introduction](#)
- [Reviewing Your Network Activity](#)
- [Exploring the Traffic Details](#)
- [Viewing Logs](#)

Introduction

Ivanti Neurons for Virtual Traffic Manager (vTM) provides visibility of network activity and service usage across your enterprise through network activity analytics and performance graphs.

After you log in to the Tenant Admin portal, *vTM* displays the Gateways Overview page. Through the *vTM* menu, use the Insights menu icon to monitor the vTM Gateways and Clusters, and analyze the gateways performance graphs.

Configuring Export Settings for Transaction Metadata Records

The Ivanti Virtual Traffic Manager maintains a series of long-lived TCP connections to the endpoint, with each connection managed by an internal data-plane process. The data-plane processes handle incoming transactions with the Traffic Manager and stream corresponding metadata records in JSON format, separated by newline characters, to the endpoint.

Use the Transaction Metadata settings at vTM gateway, to configure how the Traffic Manager exports transaction metadata records to the defined endpoint.

Transaction Metadata

These settings control how metadata about transactions processed by the traffic manager is exported.

[View JSON Schema for transaction metadata](#)

Export metadata about transactions processed by the traffic manager to an external location.

transaction_exporttenabled: ☒ Yes ☐ No Default: No

The endpoint to which transaction metadata should be exported. The endpoint is specified as a hostname or IP address with a port.

transaction_exportlendpoint:

Whether the connection to the specified endpoint should be encrypted.

transaction_exporttls: ☐ Yes ☒ No Default: Yes

Whether the server certificate presented by the endpoint should be verified, preventing a connection from being established if the certificate does not match the server name, is self-signed, is expired, is revoked, or has an unknown CA.

transaction_exporttls_verify: ☐ Yes ☒ No Default: Yes

As of now, TLS connections are not supported and all related config items should be mandatorily be set to 'No' .

Configuring Export Settings for Log Files

Use the Log Files section at vTM gateway, to configure how the Traffic Manager exports log data to the defined endpoint.

Log Files

These settings control which log files should be exported, and how entries from those log files should be exported.

Monitor log files and export entries to the configured endpoint.

log_exportenabled: ☒ Yes ☐ No Default: No

The URL to which log entries should be sent. Entries are sent using HTTP(S) POST requests.

log_exportendpoint:

Log file categories currently configured to be exported

Admin Server Access	☐
Application Firewall	☒
Audit Log	☒
Event Log	☒
Process Monitor	☐
Routing Software	☐
System - authentication log	☐
System - syslog	☐

Choose Log Files to export

The HTTP authentication method to use when exporting log entries.

☒ None

☐ Basic (Username and Password) ...

The username to use for HTTP basic authentication.

log_exportauthusername:

The password to use for HTTP basic authentication.

log_exportauthpassword:

☐ Splunk (HEC token) ...

The HTTP Event Collector token to use for HTTP authentication with a Splunk server.

log_exportauthhec_token:

Whether the server certificate should be verified when connecting to the endpoint. If enabled, server certificates that do not match the server name, are self-signed, have expired, have been revoked, or that are signed by an unknown CA will be rejected.

log_exporttls_verify: ☐ Yes ☒ No Default: Yes

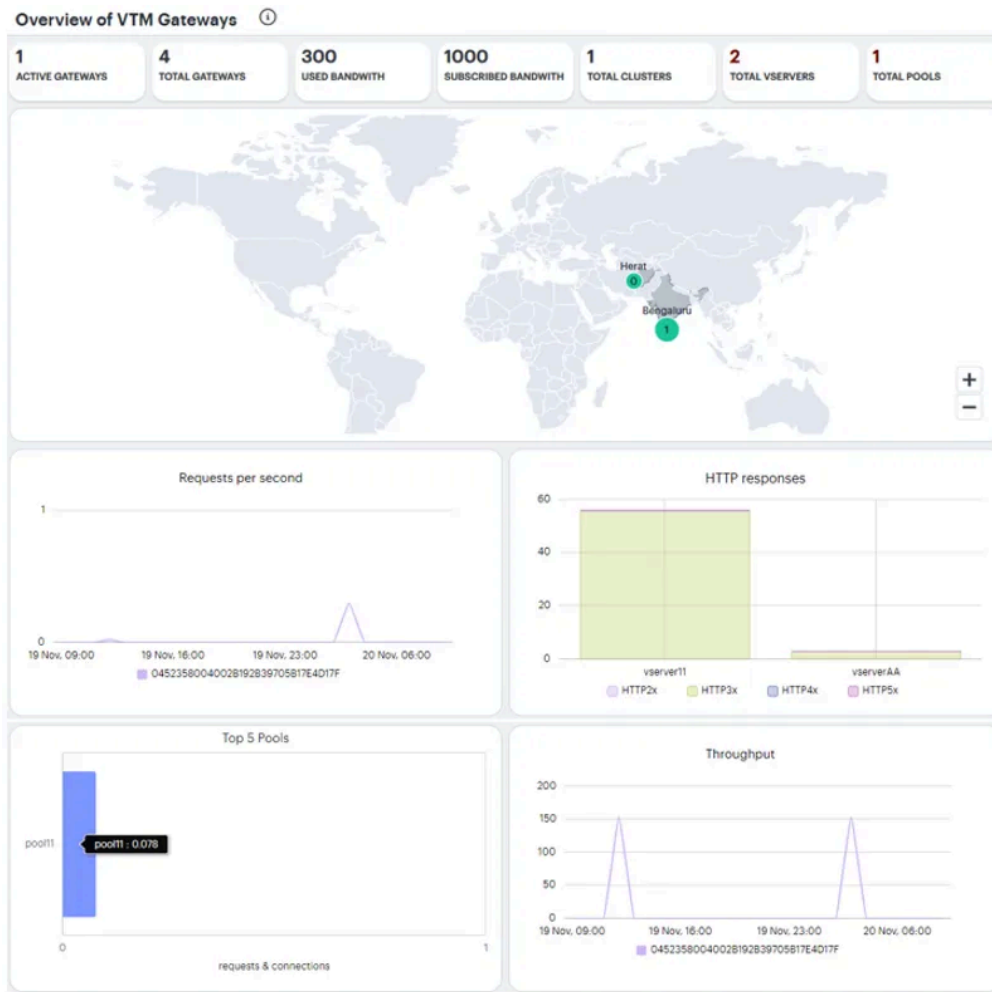
The number of seconds after which HTTP requests sent to the configured endpoint will be considered to have failed if no response is received. A value of 0 means that HTTP requests will not time out.

log_exportrequest_timeout: seconds Default: 30

As of now, TLS connections are not supported and all related config items should be mandatorily be set to 'No' .

Reviewing Your Network Activity

The *vTM Gateways* overview page shows real-time analytics data for your network infrastructure, providing a one-page dashboard of activity across your organization.



To access the Gateways Overview page:

1. Log into the *Controller* as a Tenant Admin, see [Logging in as a Tenant Administrator](#).
The Gateways Overview page appears by default.
2. To return to the Gateways Overview page at any time, select **Insights > Overview** from the left-hand menu. Alternatively, select the Ivanti banner at the top.

Understanding the Display

The primary components of the Gateways Overview page are the following:

- **Summary ribbon**, showing totals for Active Gateways, Total Gateways, Used Bandwidth, Subscribed Bandwidth, Total Virtual Servers, and Total Pools. For details, see [Using the Summary Ribbon](#).
- **World map**, showing the gateways locations, and each indicated location provides a summary of the activities observed there. Hover your pointer over a counter to view a visual representation of the number of gateways and the bandwidth usage at that location.
- **Charts**, showing the following data:
 - **Requests per second**: For each cluster, the number of requests per second in the last 24 hours.
 - **HTTP responses**: For each virtual server, the number of HTTP responses in the last 24 hours.
 - **Top 5 pools**: For the top 5 pools, the number of requests and connections in the last 24 hours.

- **Throughput:** For each cluster, the throughput (in mbps) in the last 24 hours.

For a detailed drill-down analysis of each of these primary charts and multiple secondary charts, with filters and time duration, see the section [Virtual Traffic Manager Analytics](#).

Using the Summary Ribbon

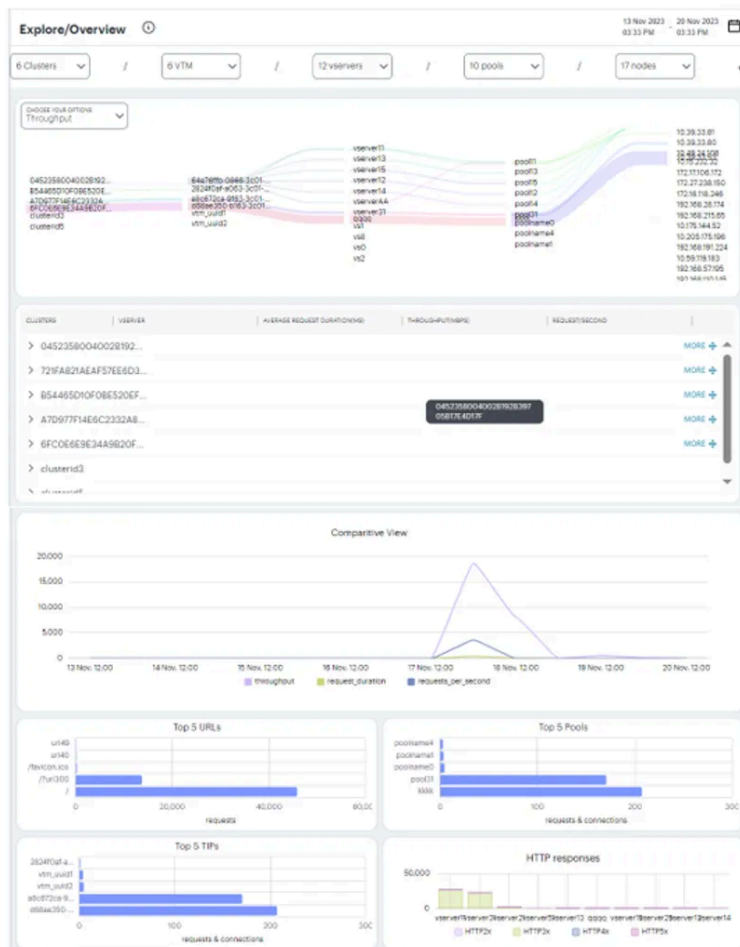
The Summary Ribbon at the top of the page shows data totals for each category:

- The number of Active Gateways
- The Total number of Gateways
- The total Used Bandwidth
- The total Subscribed Bandwidth
- The Total number of Clusters
- The Total number of Virtual Servers
- The Total number of Pools

Exploring the Traffic Details

The traffic details page shows charts of various aspects of the traffic. It allows the user to drill-down into the source of the issue.

To view the Traffic Details page, select **Insights > Explore**.



Using the Filter Bar

vTM uses the top part of the Explorer View page to show:

- current page title
- selected Time period and Timezone
- filters based on **Cluster**, **VTM**, **Virtual Server**, **Pool**, and **Node**

Set a specific *From* and *To* to denote the start and end of your date/time range.

The screenshot shows the vTM filter bar. At the top, there's a 'LOG TYPE' dropdown set to 'Event log'. To its right, the date range is '11 Nov 2023 - 18 Nov 2023' with a calendar icon. Below this, the 'From' and 'To' sections are visible. Each section has a calendar for the month of November 2023. In the 'From' calendar, the 11th is selected. In the 'To' calendar, the 18th is selected. Below the calendars, there are time selectors for 'HR' and 'MIN'. For 'From', the time is 22:03. For 'To', the time is 22:03. At the bottom of the filter bar, there are 'CANCEL' and 'APPLY' buttons.

Selecting a date and time range

To return to the current page without making any changes, select **Cancel**.

To apply your changes, select **Apply**. The selected time period is displayed in the filter bar and data across all **Insights** pages is updated accordingly.

Using the Sankey Chart View

The Sankey chart provides an alternate visualization of your services, showing directed flow between related objects based on the option you choose from the drop-down list - **Throughput**, **Requests per second**, and **Connections per second**. The width of each stream in the flow - **Cluster > VTM > Virtual Server > Pool > Node** - is proportional to the utilization of the object the flow passes through, allowing an administrator to view significant usage and relationships across your user base and infrastructure.

By hovering your pointer over a flow of interest, vTM displays a tooltip confirming the scale of the activity between the two objects connected by the flow.

Using the Clusters Tabular View

The Table view shows all the metrics in a table form. Grouped by cluster, the Table view shows all the three metrics - Average connection duration, Average request duration and Request per second, and Throughput - for each of the vTM instances.

Using the Comparative View

The Comparative View chart allows comparative analytics between two metrics. Multiple metrics can be displayed on this chart (that is, the user shall be able to select requests per second or throughput and plot them side by side).

Using the Charts

The Traffic Details page includes bar charts to provide a breakdown of **Top 5 URLs**, **Top 5 Pools**, **Top 5 Traffic IPs**, and **HTTP responses**.

Hover your pointer over a particular bar to view a tooltip showing the label and total.

Viewing Logs

The Logs page allows you to watch the Event, Authentication and System logs in real-time as records are appended to them. These events are reported to the Controller by your vTM Gateways.

To view the Logs page:

1. Log in to the Controller as a Tenant Admin, see [Logging into the Controller as a Tenant Admin](#).
2. From the vTM menu, click **Insights > Logs**.

The Logs page appears.

VTM Logs ⓘ

LOG TYPE
Event log

11 Nov 2023 09:32 PM - 18 Nov 2023 09:32 PM

📅

HOST	TIME	SEVERITY	MESSAGE	
10.39.33.88	18/Nov/2023:07:48:43 +0530	WARN	log_export/* exporterreaderror The ...	MORE +
10.39.33.88	18/Nov/2023:07:48:43 +0530	INFO	fluentbitstopping Fluentbit process ...	MORE +
10.39.33.88	18/Nov/2023:07:48:43 +0530	FATAL	zxtmswerror fatal Parent 399884 hit...	MORE +
10.39.33.88	18/Nov/2023:07:48:43 +0530	INFO	flippershutdown Flipper shutdown r...	MORE +
10.39.33.88	18/Nov/2023:07:48:43 +0530	INFO	Pulse Secure Virtual Traffic Manager...	MORE +
10.39.33.88	18/Nov/2023:07:48:43 +0530	INFO	Version 22.5b1INTERNAL USE ONLY, ...	MORE +
10.39.33.88	18/Nov/2023:07:48:43 +0530	INFO	eventdstart Eventd started, pid: 524...	MORE +
10.39.33.88	18/Nov/2023:07:48:43 +0530	INFO	linenakeve/automatically installed	MORE +

←

1

2

3

4

5

→

1. Click the **Log Type** drop-down and select Event Log or Other log.
2. Set a specific *From* and *To* to denote the start and end of your date/time range.

LOG TYPE
Event log

11 Nov 2023 10:03 PM - 18 Nov 2023 10:03 PM

From

To

MONTH
November

YEAR
2023

Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2

HR
22

MIN
3

MONTH
November

YEAR
2023

Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2

HR
22

MIN
3

CANCEL

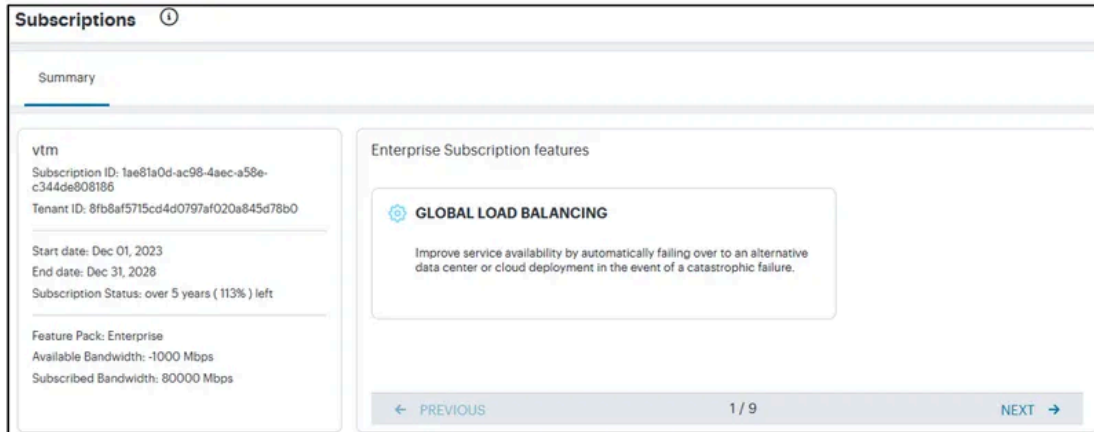
APPLY

To apply your changes, click **Apply**. The selected time period is displayed in the filter bar and data on the page updates accordingly. To return to the current page without making any changes, select **Cancel**.

10. Licensing/Subscription

Licenses/subscriptions are added to your nSA by Ivanti.

The **Subscriptions** page displays the licenses/subscriptions that are active on your nSA. To access this page, click **Administration > Subscriptions**.



The **Summary** tab displays for each subscription/license:

- vTM License/Subscription ID and Tenant ID.
- Subscription start and end dates, and subscription status.
- Feature pack and Subscribed bandwidth and available bandwidth details.

If a feature pack specifies a bandwidth of 1000 Mbps, the user is able to allocate this across multiple gateways considering how much is unallocated. The user is informed about the unallocated bandwidth available in the feature pack. When adding a gateway, user can select the feature pack and allocate a specific bandwidth to the gateway.

- One or more descriptions of the features in the license/subscription. Where there are multiple features, use **Previous** / **Next** to navigate.