Kaseya

Traverse (Cloud)

Quick Start Guide

Version R95

September 2, 2017

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Preface 1

Installation and Logon (Cloud) 3

Basic Configuration 13

Advanced Features 29

Preface

About this Traverse Quick Start Guide

This guide provides a quick installation guide and overview for the cloud (SaaS) version of **Traverse** monitoring software.

Audience

This guide is intended for **Traverse** cloud administrators.

About Traverse

Traverse is a breakthrough IT infrastructure monitoring and service management solution for mission-critical, distributed, and complex environments for enterprises and managed services providers (MSPs). **Traverse** delivers real-time, correlated, end-to-end, service-oriented views of the performance of the entire IT infrastructure - physical, virtual and cloud. **Traverse**'s massively-scalable, patented solution architecture supports tens of thousands of distributed end-points, and processes millions of metrics. The software's innovative service container technology supports creation of purpose-specific, logical management views of business services and the underlying cloud and IT infrastructure. **Traverse** is fully-aligned with ITIL and provides an open, extensible API and plug-in framework for integration with the enterprise ecosystem.

Contacting Kaseya

- Customer Support - You can contact Kaseya technical support online at:
  - **https://helpdesk.kaseya.com/home** *(https://helpdesk.kaseya.com)*
- Community Resources - You can also visit the following community resources for Kaseya **Traverse**:
  - Knowledge base at: **http://community.kaseya.com/kb/w/wiki/1206.kaseya-traverse.aspx** *(https://helpdesk.kaseya.com/forums/22931123)*
  - Forum at: **http://community.kaseya.com/xsp/f/340.aspx** *(http://community.kaseya.com/xsp/f/340.aspx)*

Chapter 1

Installation and Logon (Cloud)

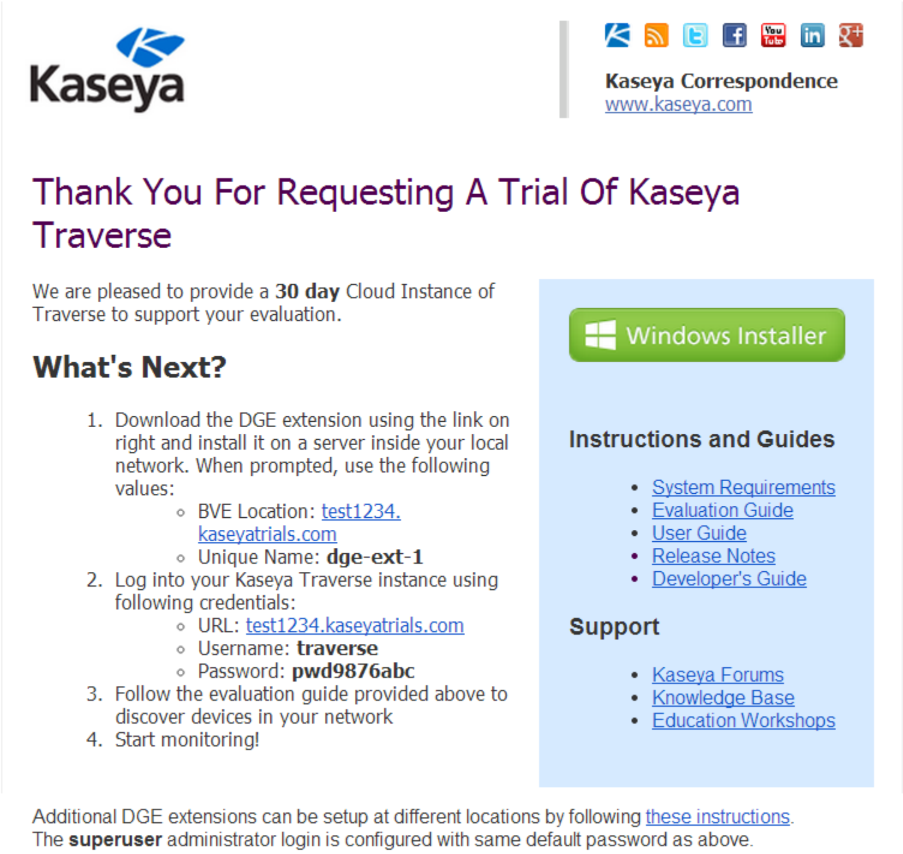
In This Chapter

Getting Started

You can **request either a production or trial subscription to the Kaseya Traverse cloud** *(http://www.kaseya.com/forms/free-trial?prodcode=travsaas)*.

The trial subscription might limit the number of devices that you are allowed to monitor (about 50 devices).

Once your **Traverse** Cloud instance has been created, you will receive a **Kaseya Traverse** production or trial email similar to the sample image below. The email summarizes 4 simple steps to start monitoring devices on a network.



Thank You For Requesting A Trial Of Kaseya Traverse

We are pleased to provide a **30 day** Cloud Instance of Traverse to support your evaluation.

What's Next?

1. Download the DGE extension using the link on right and install it on a server inside your local network. When prompted, use the following values:
   - BVE Location: test1234.kaseyatrials.com
   - Unique Name: **dge-ext-1**
2. Log into your Kaseya Traverse instance using following credentials:
   - URL: test1234.kaseyatrials.com
   - Username: **traverse**
   - Password: **pwd9876abc**
3. Follow the evaluation guide provided above to discover devices in your network
4. Start monitoring!

Instructions and Guides

- System Requirements
- Evaluation Guide
- User Guide
- Release Notes
- Developer's Guide

Support

- Kaseya Forums
- Knowledge Base
- Education Workshops

Additional DGE extensions can be setup at different locations by following these instructions.
The **superuser** administrator login is configured with same default password as above.

Traverse Minimum Requirements (Cloud)

Traverse R95 requires a DGE extension be installed on a network Windows machine, one for each network you intend to monitor. The DGE extension relays collected data to the Traverse cloud website.

Note: Using Netflow requires a larger platform than one without Netflow (Network Flow Analysis).

Known Issue: An issue with the installer on Windows 2012 R2 can be worked around easily by following **these instructions** *(https://helpdesk.kaseya.com/hc/en-gb/articles/229042328)*.

Without Netflow

- Windows 2003 (for DGEx only), 2008, 2008 R2, 7, 2012, 2012 R2
- 2 GB RAM
- 10 GB free disk space
- 1 CPU

With Netflow

- Windows 2003 (for DGEx only), 2008, 2008 R2, 7, 2012, 2012 R2
- 4 GB RAM
- 50 GB disk space
- 2 CPU

Supported Browsers

- Windows
  - Internet Explorer 10 and later
  - FireFox 25 and later
  - Chrome 30 and later
- Apple OS X
  - Safari 6 and later
  - FireFox 25 and later
  - Chrome 30 and later
- In addition, Traverse requires the Adobe Flash Player plugin be installed on your browser.

Disk Space Requirements

- 36 GB free space in a RAID 5 configuration is recommended.
- Additional free space for the `<TRAVERSE_HOME>\logs` directory. Plan for 5 GB of disk space for log files. The default `<TRAVERSE_HOME>` directory is `\Program Files (x86)\Traverse`.

> **Note:** *See* **Installation Prerequisites** *(http://help.kaseya.com/webhelp/EN/TV/9050000/index.asp#17290.htm).*

DGE Extension Installation Prerequisites

Prior to installing a DGE extension, review the following:

1. Ensure the Windows machine you will install the DGE extension on has access to the internet.
2. Ensure the time on the Windows machine is accurate. Windows includes Internet Time Synchronization software (under **Date & Time**, click the **Internet Time** tab and enable it with default settings). See a detailed explanation below.
3. Identify the administrator password for your Windows servers so that they can be queried using WMI.
4. Identify the username and password with SYSDBA level rights you will use to monitor Oracle databases.
5. Identify, and if necessary, enable the (read-only) SNMP community string (SNMP v1 or v2) or username, password and optionally encryption key (SNMP v3) used by SNMP-capable devices on your network.
6. Update firewall rules and/or access lists (ACL) on routers to allow SNMP queries from the DGEx to monitored devices. The default is UDP 161. Also, ensure the DGEx has TCP access to the Cloud using the ports listed in the table below.

Source Port	Destination Port	Direction	Description
(any)	7651	DGEx > Cloud	Provisioning Database
(any)	7652	DGEx > Cloud	Provisioning Database
(any)	7653	DGEx > Cloud	Internal Messaging Bus
(any)	9443	DGEx > Cloud	Upstream DGE

Setting the Time on a Non-Domain Server

Since **Traverse** is a distributed platform, it is important to make sure that the time on your DGE extension server is accurate. Windows has a built in time synchronization mechanism to set the time from an internet time server.

Note: For domain machines, time is synchronized from the domain controller.

To set the time on the server running the DGE extension:

- Open Date and Time by clicking the Start button, clicking Control Panel, clicking Clock, Language, and Region, and then clicking **Date and Time**.
- Click the **Internet Time** tab, and then click **Change** settings. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
- Click **Automatically synchronize with an Internet time server**, select a time server, and then click **OK**.

Install the DGE Extension

Identify Your BVE Location and Unique Name

This information is provided by Kaseya and included in **step 1** of the **Kaseya Traverse Evaluation** *(page 4)* email you received. For example:

- BVE Location: `your-unique-site-name.kaseyatrials.com`
- Unique Name: `your-unique-DGE-name`

Download the Installer

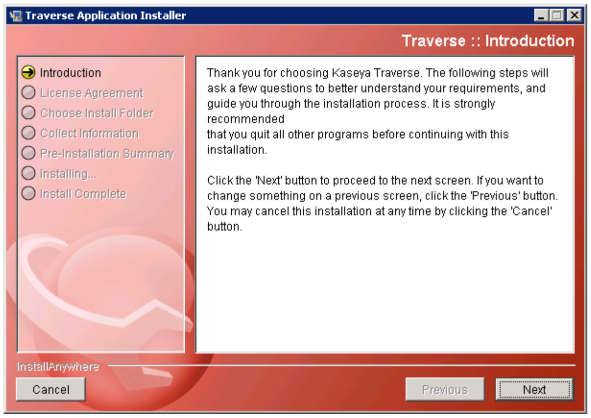
Download the Windows installer for the DGE extension by clicking the **Windows Install** button displayed on the **Kaseya Traverse Evaluation** email.

Run the Installer

Run the installer as a local or domain administrator, not a standard user.

Introduction

Click **Next**.



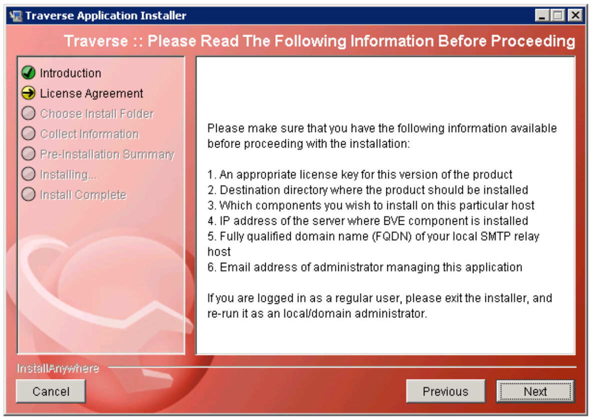
Thank you for choosing Kaseya Traverse. The following steps will ask a few questions to better understand your requirements, and guide you through the installation process. It is strongly recommended
that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button.

Checklist

Except for running the installer as a local or domain administrator, ignore the instructions on this page.

Click **Next**.



Please make sure that you have the following information available before proceeding with the installation:

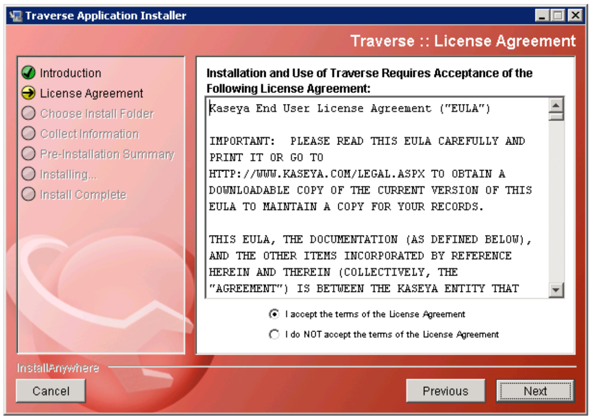
1. An appropriate license key for this version of the product
2. Destination directory where the product should be installed
3. Which components you wish to install on this particular host
4. IP address of the server where BVE component is installed
5. Fully qualified domain name (FQDN) of your local SMTP relay host
6. Email address of administrator managing this application

If you are logged in as a regular user, please exit the installer, and re-run it as an local/domain administrator.

License Agreement

Review the License Agreement, then click the **I accept the terms of the License Agreement** option.

Click **Next**.



Installation and Use of Traverse Requires Acceptance of the Following License Agreement:

```
Kaseya End User License Agreement ("EULA")

IMPORTANT:  PLEASE READ THIS EULA CAREFULLY AND
PRINT IT OR GO TO
HTTP://WWW.KASEYA.COM/LEGAL.ASPX TO OBTAIN A
DOWNLOADABLE COPY OF THE CURRENT VERSION OF THIS
EULA TO MAINTAIN A COPY FOR YOUR RECORDS.

THIS EULA, THE DOCUMENTATION (AS DEFINED BELOW),
AND THE OTHER ITEMS INCORPORATED BY REFERENCE
HEREIN AND THEREIN (COLLECTIVELY, THE
"AGREEMENT") IS BETWEEN THE KASEYA ENTITY THAT
```

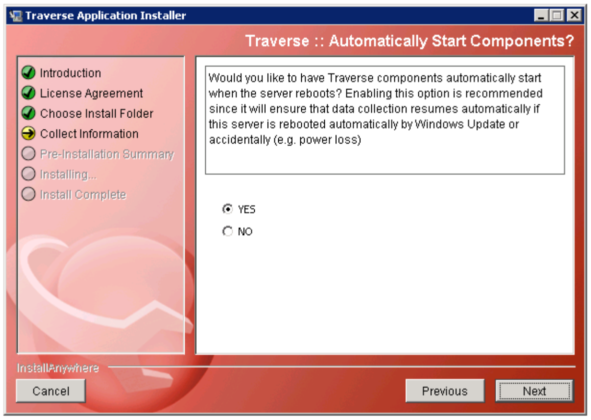
● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

Automatically Restart DGE Extension Services After a Reboot

Accepting the default **Yes** option to this prompt is strongly recommended. It ensures all DGE extension services will be restarted if the network Windows machine is rebooted.

Click **Next**.



Traverse :: Automatically Start Components?

Would you like to have Traverse components automatically start when the server reboots? Enabling this option is recommended since it will ensure that data collection resumes automatically if this server is rebooted automatically by Windows Update or accidentally (e.g. power loss)

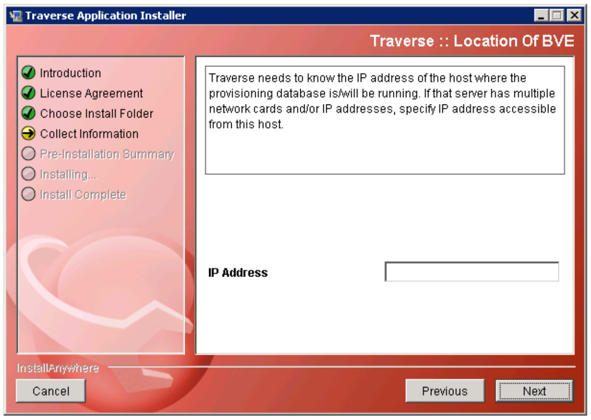
● YES
○ NO

Location BVE

Enter the value for the **BVE Location** you identified in **Install the DGE Extension** *(page 6)* in the **IP Address** field. It should be similar in format to **your-unique-site-name.kaseyatrials.com**.

> **Note:** Do not include an `http://` prefix when you enter this value.

Click **Next**.



Traverse :: Location Of BVE

Traverse needs to know the IP address of the host where the provisioning database is/will be running. If that server has multiple network cards and/or IP addresses, specify IP address accessible from this host.

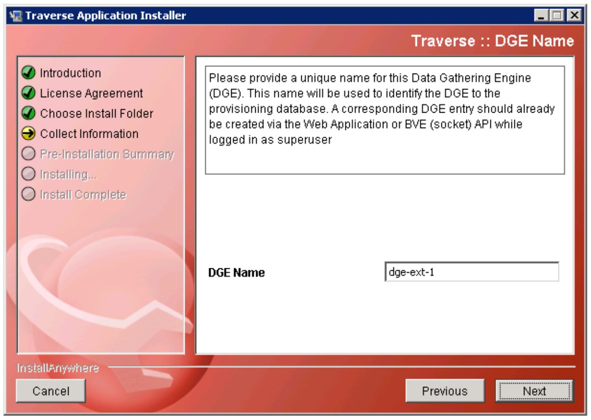
IP Address

DGE Name

Enter the value for the **Unique Name** you identified in **Install the DGE Extension** *(page 6)* above in the **DGE Name** field. It should be similar in format to `your-unique-DGE-name`.

> **Note:** Typically your first DGE extension is called `dge-ext-1`.

Click **Next**.



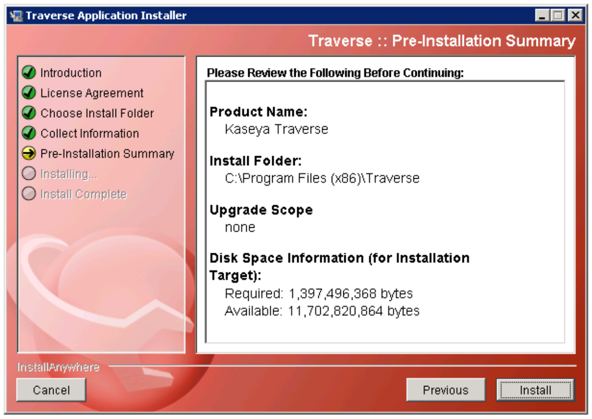
Please provide a unique name for this Data Gathering Engine (DGE). This name will be used to identify the DGE to the provisioning database. A corresponding DGE entry should already be created via the Web Application or BVE (socket) API while logged in as superuser

DGE Name: dge-ext-1

Pre-Installation Summary

Review the following information before beginning the installation.

Click **Install**. It may take a few minutes to complete the install.



Please Review the Following Before Continuing:

Product Name:
Kaseya Traverse

Install Folder:
C:\Program Files (x86)\Traverse

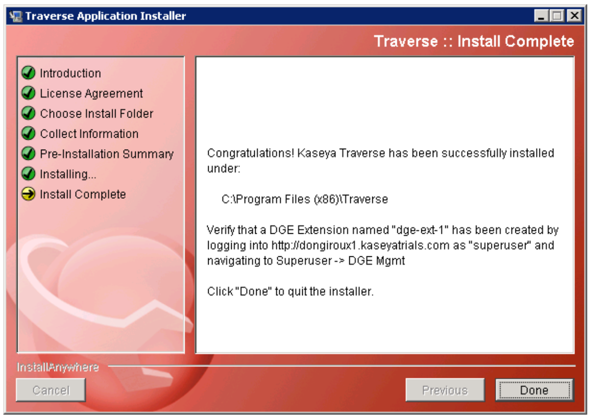
Upgrade Scope
none

Disk Space Information (for Installation Target):
Required: 1,397,496,368 bytes
Available: 11,702,820,864 bytes

Close the Installer

Ensure the text displayed in this box matches the values you were provided in **Install the DGE Extension** *(page 6)*.

> **Note:** The text prompts you to continue by logging on to your unique **Traverse** website, using the username `superuser` and the same assigned password you were provided in the **Kaseya Traverse Evaluation** *(page 4)* email.



Congratulations! Kaseya Traverse has been successfully installed under:

C:\Program Files (x86)\Traverse

Verify that a DGE Extension named "dge-ext-1" has been created by logging into http://dongiroux1.kaseyatrials.com as "superuser" and navigating to Superuser -> DGE Mgmt

Click "Done" to quit the installer.

Traverse Cloud Logon

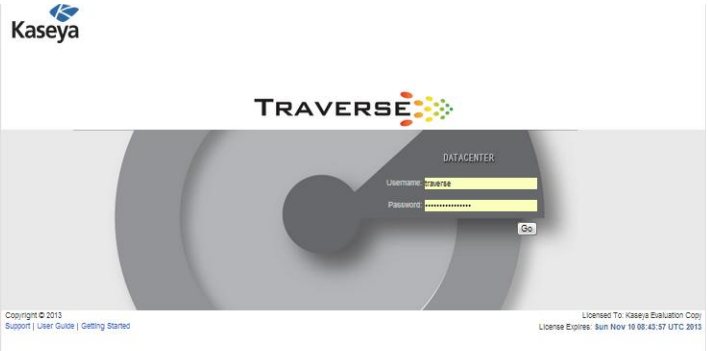
Logon as a Standard User

Identify your **Traverse** Cloud assigned URL, username and password.

This information was included in **step 1** of the **Kaseya Traverse Evaluation** *(page 4)* email you received. For example:

- URL: `your-unique-site-name.kaseyatrials.com`
- Username: `traverse`
- Password: `your-assigned-password`

Use these values to logon to your unique **Traverse** Cloud website as a standard user.



Username: traverse

Password: ••••••••••••••••

Copyright © 2013

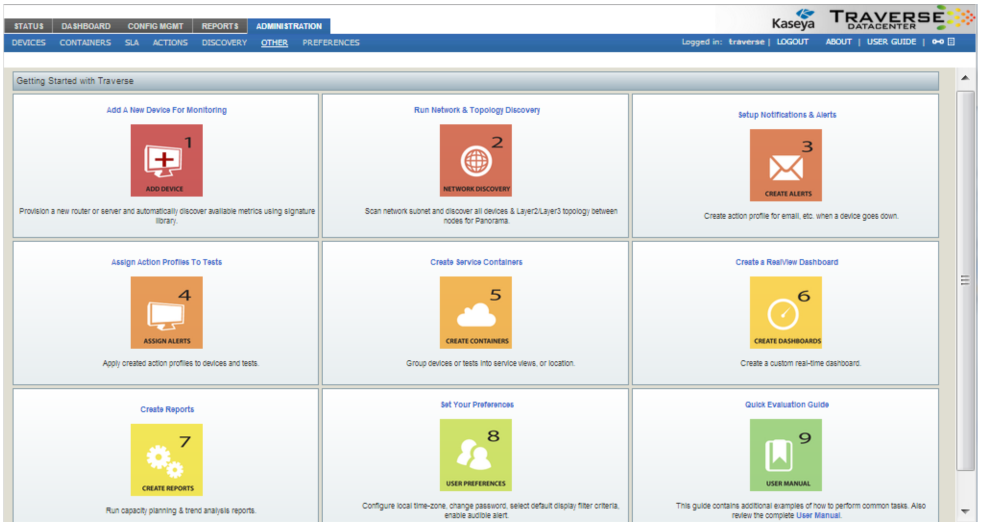
Licensed To: Kaseya Evaluation Copy

License Expires: Sun Nov 10 08:43:57 UTC 2013

Initial Page after Standard User Logon

By default, the first page a standard user sees after logon is the **Getting Started with Traverse** page. You can click any tile to jump immediately to one of these frequently used pages.

You can also navigate to other pages using the menu bar at the top.



Provision a new router or server and automatically discover available metrics using signature library.

Scan network subnet and discover all devices & Layer2/Layer3 topology between nodes for Panorama.

Create action profile for email, etc. when a device goes down.

Apply created action profiles to devices and tests.

Group devices or tests into service views, or location.

Create a custom real-time dashboard.

Run capacity planning & trend analysis reports.

Configure local time-zone, change password, select default display filter criteria, enable audible alert.

This guide contains additional examples of how to perform common tasks. Also review the complete User Manual.

Logon as a Superuser

You can also logon using the administrator-level username `superuser` **and the same assigned password you were provided in the Kaseya Traverse Evaluation** *(page 4)* **email**.

Navigate your browser to the URL you were provided, similar in format to `your-unique-site-name.kaseyatrials.com`

- Username: `superuser`
- Password: `your-assigned-password`

> **Note:** You should only logon as a `superuser` when you need to perform an administrative-level task. Otherwise, logon as a standard user.

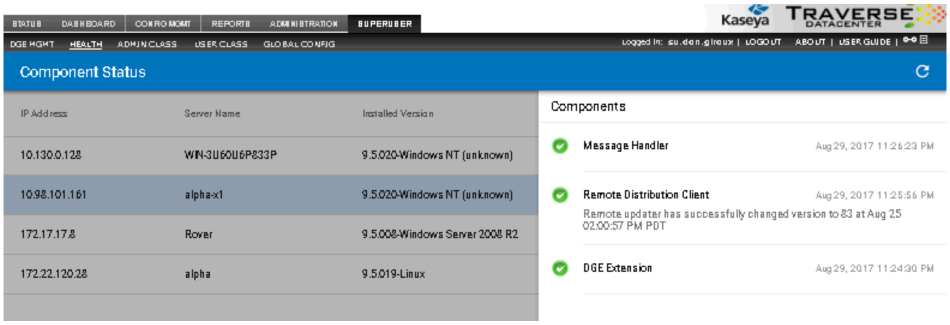
Initial Page after Administrator Logon

> By default, the first page a `superuser` or other administrator sees after logon is the Status > **Departments** page.

Check the Health Status of the DGE Extension

> **Note:** Whenever you install a new DGE extension, you should logon as the `superuser` to verify the connection.

Logon as `superuser`. Navigate to the Superuser > **Health** page. Verify the `IP address` and `Server Name` of the DGE extension you installed. The "heartbeats" for all the components of your DGE extension should display a green OK icon. Logoff when you're done. Re-logon as a standard user to resume normal operations.



Component Status

IP Address	Server Name	Installed Version
10.130.0.128	WIN-3U60U6P833P	9.5.020-Windows NT (unknown)
10.98.101.161	alpha-x1	9.5.020-Windows NT (unknown)
172.17.17.8	Rover	9.5.008-Windows Server 2008 R2
172.22.120.28	alpha	9.5.019-Linux

Components

- ✓ Message Handler — Aug 29, 2017 11:26:23 PM
- ✓ Remote Distribution Client — Aug 29, 2017 11:25:56 PM
  Remote updater has successfully changed version to 83 at Aug 25 02:00:57 PM PDT
- ✓ DGE Extension — Aug 29, 2017 11:24:30 PM

A component displays in the status list when the component begins operating. The **Component Status** page includes information about the following:

- IP address of the component
- component name
- the last status update received by the BVE
- the version of the component
- the last action performed on the component

By default, **Traverse** components are configured to send status updates every two minutes. The status changes to a state of "warning" if **Traverse** does not receive an update after more than five minutes. The status changes to "critical" after 10 minutes elapse without **Traverse** receiving an update.

Refresh the **Component Status** page to view the latest **Traverse** component information.

If components are in a "warning" or "critical" state, see **Troubleshooting Traverse** *(http://help.kaseya.com/webhelp/EN/TV/9050000/index.asp#16912.htm)*.

Change Your Passwords

> **Note:** Kaseya strongly urges you to change the passwords you were assigned when your **Traverse** website was created.

1. Navigate to the Administration > **Preferences** page.
2. Change the password for the admin called `superuser`.
3. Change the password for the user called `traverse`.

> **Note:** Unless a feature specifically requires `superuser` access, you should logon as the `traverse` user.

Chapter 2

Basic Configuration

In This Chapter

Shared Credentials/Configurations

Administration > Other > Shared Credentials/Configuration

Before running **Network Discovery** *(page 15)* or creating tests manually, you should register shared credentials required to *provision* tests on discovered devices. Each shared credential you create:

- Authenticates running multiple tests on multiple devices.
- Is specific to a department.
- Has additional options, based on its *monitor type.* For example:
  - SNMP credentials
  - Windows Management Instrumentation (WMI)
  - Amazon Web Services
- Are validated against the appropriate tests automatically. The mapping is remembered from that point forward.

Adding a Shared Credential

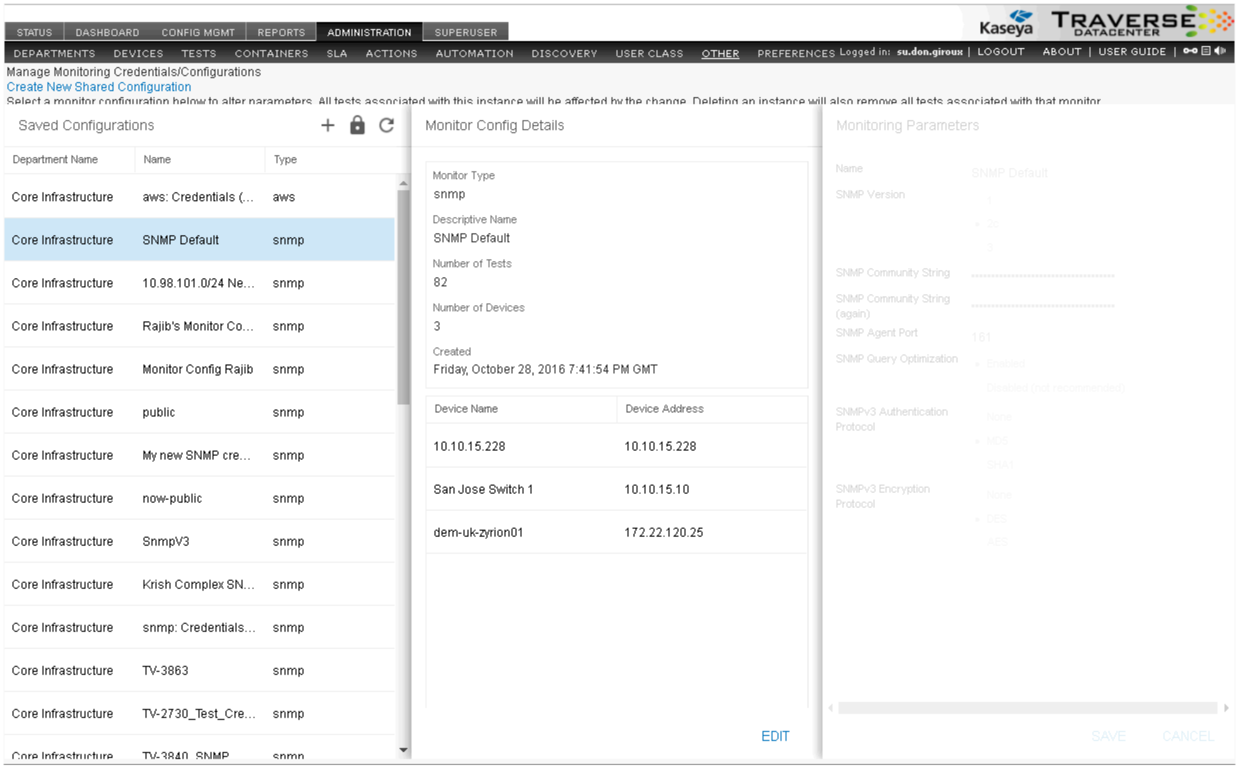
1. Navigate to Administration > Other > **Shared Credentials/Configuration**.
2. Click the plus ⊞ icon in the title bar of the **Saved Configuration** panel.
3. Enter the following:
   - Department - Select a department
   - Monitor Type - Select a monitor type.
   - Additional properties as required for the monitor type.

Editing a Shared Credential

1. Click a row in the **Saved Configuration** panel.
2. Click **Edit** in the middle panel.
   - The middle panel also lists the devices that use this credential.

Deleting a Shared Credential

Deleting a shared credential/configuration removes it from all the tests that use it. You'll have to apply a new shared credential/configuration of the same monitor type to enable those tests to return data.



Manage Monitoring Credentials/Configurations

Create New Shared Configuration

Select a monitor configuration below to alter parameters. All tests associated with this instance will be affected by the change. Deleting an instance will also remove all tests associated with that monitor

Department Name	Name	Type
Core Infrastructure	aws: Credentials (...	aws
Core Infrastructure	SNMP Default	snmp
Core Infrastructure	10.98.101.0/24 Ne...	snmp
Core Infrastructure	Rajib's Monitor Co...	snmp
Core Infrastructure	Monitor Config Rajib	snmp
Core Infrastructure	public	snmp
Core Infrastructure	My new SNMP cre...	snmp
Core Infrastructure	now-public	snmp
Core Infrastructure	SnmpV3	snmp
Core Infrastructure	Krish Complex SN...	snmp
Core Infrastructure	snmp: Credentials...	snmp
Core Infrastructure	TV-3863	snmp
Core Infrastructure	TV-2730_Test_Cre...	snmp
Core Infrastructure	TV-3840_SNMP	snmp

Monitor Type
snmp

Descriptive Name
SNMP Default

Number of Tests
82

Number of Devices
3

Created
Friday, October 28, 2016 7:41:54 PM GMT

Device Name	Device Address
10.10.15.228	10.10.15.228
San Jose Switch 1	10.10.15.10
dem-uk-zyrion01	172.22.120.25

Name: SNMP Default

SNMP Version: ○ 1 ● 2c ○ 3

SNMP Community String: ••••••••••••••••••••••••••••••••••••

SNMP Community String (again): ••••••••••••••••••••••••••••••••••••

SNMP Agent Port: 161

SNMP Query Optimization: ● Enabled ○ Disabled (not recommended)

SNMPv3 Authentication Protocol: ○ None ● MD5 ○ SHA1

SNMPv3 Encryption Protocol: ○ None ● DES ○ AES

Run Network Discovery

Device Discovery and Test Discovery

The **Discovery Sessions** page searches a network and discovers devices and tests.

For four monitor types—ping, snmp, wmi, port—discovery includes the concept of *test discovery.* Test discovery scans a device to identify what metrics are supported on that specific device. For example, scanning a router using SNMP returns tests related to interfaces, system resources, etc. In contrast, a linked device template or static device template only creates the tests you specify. No actual scan against the device is performed.

> **Note:** You can perform test discovery for additional monitor types using the **Perform auto-discovery of supported (*) test types** option on the Add Standard Tests page.

Discovery sessions:

- Can automatically provision discovered devices with tests and start monitoring them immediately.
- Can be scheduled on a recurring basis.
- Should be limited to class-C networks instead of class-B or larger.

Automation Profiles

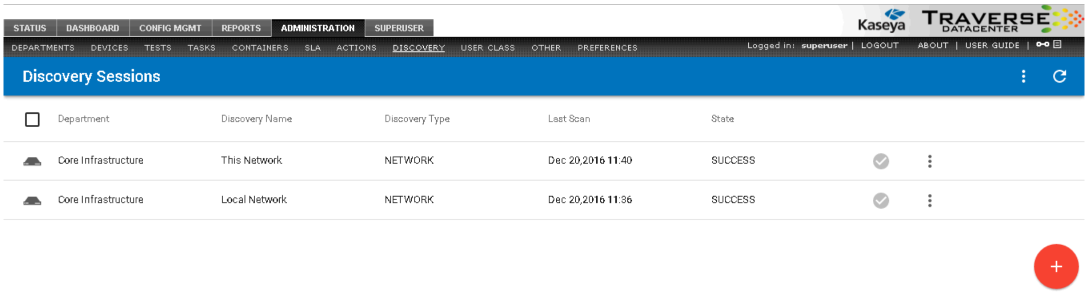
Automation profiles are new functionality that enable you to customize tests automatically during discovery and rediscovery. The default settings assigned to tests are overridden, based on the criteria you provide in automation profiles. For more information see Automation.

Prerequisites

Discovery requires the appropriate **shared credentials** *(page 14)* be defined for the networks you want to scan.

Procedure

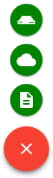
1. Navigate to the Administration > **Discovery** page.
   - A list of existing Discovery sessions displays.



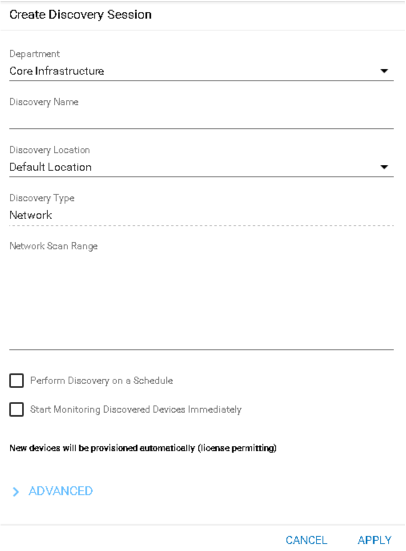
Discovery Sessions

□	Department	Discovery Name	Discovery Type	Last Scan	State		
	Core Infrastructure	This Network	NETWORK	Dec 20,2016 11:40	SUCCESS	✓	⋮
	Core Infrastructure	Local Network	NETWORK	Dec 20,2016 11:36	SUCCESS	✓	⋮

2. Click the add + icon, then click the **Network Discovery** icon.



The **Create Discovery Session** dialog displays.



Create Discovery Session

Department
Core Infrastructure

Discovery Name

Discovery Location
Default Location

Discovery Type
Network

Network Scan Range

□ Perform Discovery on a Schedule

□ Start Monitoring Discovered Devices Immediately

New devices will be provisioned automatically (license permitting)

3. Enter the following values:
   - **Department**
   - **Discovery Name** - Enter a name.
   - **Discovery Location** - Your DGE extension was assigned a unique location when it was installed. Select it from the drop-down list. Most private networks use the same range of IP addresses. This is how **Traverse** identifies which network you want to run Network Discovery on.
   - **Discovery Type** - `Network`

- **Network Scan Range** - Enter a network subnet starting value followed by the network mask. Example: `192.168.1.0/255.255.255.0`. The DGE extension you installed must have network access to the range of IP addresses you specify.
- **Perform Discovery on a Schedule** - If checked, enter the number of intervals to wait between recurring discovery session runs.
- **Start Monitoring Discovery Immediately** - If checked, newly discovered devices are provisioned with tests, becoming managed assets, and begin being monitored immediately. If unchecked, devices are discovered but not yet provisioned.

4. You can now click **Apply** or...
5. Click **Advanced** to enter values in these optional fields.

> **Note:** Ignore these advanced features for your first run of network discovery.

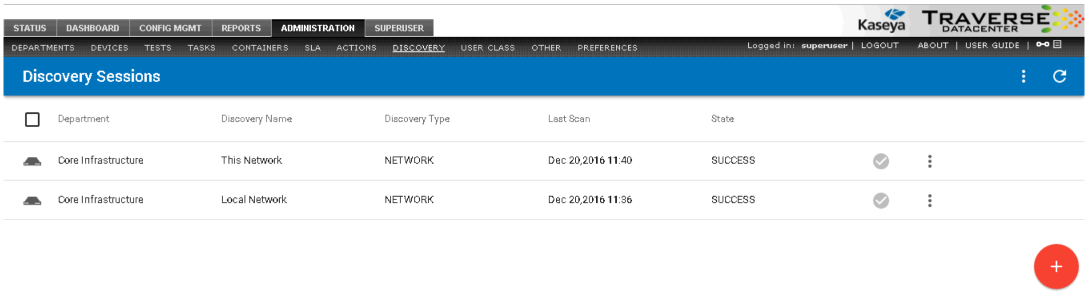
- **SNMP Community Strings/Credentials** - Optionally toggle each SNMP credential to include or exclude it from the discovery session.
  - ✓ Bolded text means the credential is included.
  - ✓ Unbolded text means the credential is excluded.
- **VMware Hypervisor Credentials** - Optionally enter a VMware credential to discover additional information about VMware hypervisors.
- **Filter by Device Type**
- **Physical Connectivity - Topology**
  - ✓ **Discover new devices and new/updated topology**
  - ✓ **Update topolog information for provisioned devices only**
- **Seed Router** - Discover connected devices from following 'seed' router (must be SNMP enabled)
  - ✓ **IP address of seed router**
  - ✓ **Limit search within number of hops**

6. Click **Apply**.

Review Network Discovery Results

To review the results of a Discovery session:

1. Click a row.

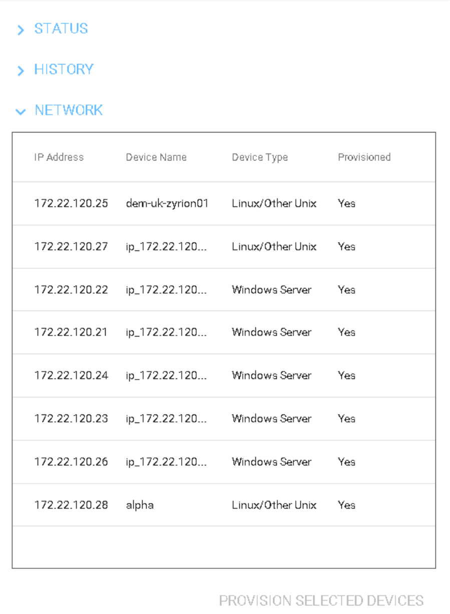


Discovery Sessions

□	Department	Discovery Name	Discovery Type	Last Scan	State
	Core Infrastructure	This Network	NETWORK	Dec 20,2016 11:40	SUCCESS
	Core Infrastructure	Local Network	NETWORK	Dec 20,2016 11:36	SUCCESS

2. A dialog displays in three sections:
   - **Status**
   - **History**
   - **Network**

3. Click the **Network** section to display the list of items discovered.



IP Address	Device Name	Device Type	Provisioned
172.22.120.25	dem-uk-zyrion01	Linux/Other Unix	Yes
172.22.120.27	ip_172.22.120...	Linux/Other Unix	Yes
172.22.120.22	ip_172.22.120...	Windows Server	Yes
172.22.120.21	ip_172.22.120...	Windows Server	Yes
172.22.120.24	ip_172.22.120...	Windows Server	Yes
172.22.120.23	ip_172.22.120...	Windows Server	Yes
172.22.120.26	ip_172.22.120...	Windows Server	Yes
172.22.120.28	alpha	Linux/Other Unix	Yes

4. If you chose not to provision newly discovered devices immediately, you can optionally click the rows you now want to provision, then click the **Provision Selected Devices** link..
5. Click the options ⋮ icon on an existing discovery row to **Run Now**, **Update Discovery**, or **Delete Discovery**.

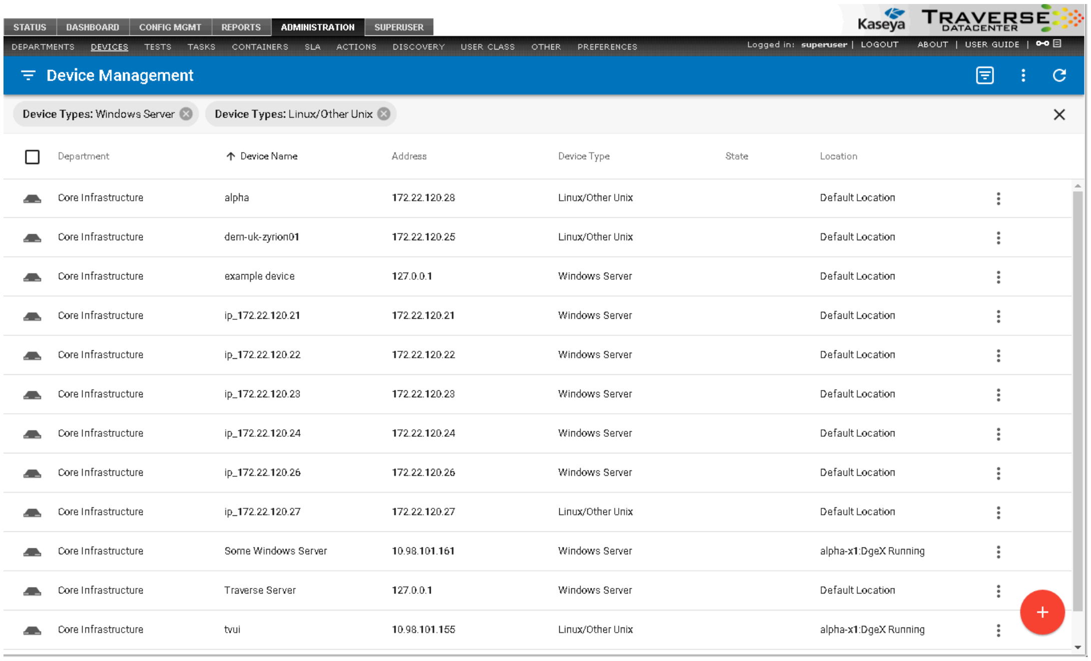
Device Management

Administration > Devices

The **Device Management** menu configures all devices managed by Traverse. The initial page lists all the devices the user is authorized to see. Each row contains the Department, Device Name, Address, Device type, State (Active or Suspended) and Location.

- Users can search, filter, add and edit multiple devices within their own department.
- Administrators can search, filter, add and edit devices *across multiple departments.*

- Devices are typically added using **Discovery** *(page 15)*. They can also be imported or added manually.



Device Management

Device Types: Windows Server ⊗ Device Types: Linux/Other Unix ⊗ ✕

□	Department	↑ Device Name	Address	Device Type	State	Location	
	Core Infrastructure	alpha	172.22.120.28	Linux/Other Unix		Default Location	⋮
	Core Infrastructure	dem-uk-zyrion01	172.22.120.25	Linux/Other Unix		Default Location	⋮
	Core Infrastructure	example device	127.0.0.1	Windows Server		Default Location	⋮
	Core Infrastructure	ip_172.22.120.21	172.22.120.21	Windows Server		Default Location	⋮
	Core Infrastructure	ip_172.22.120.22	172.22.120.22	Windows Server		Default Location	⋮
	Core Infrastructure	ip_172.22.120.23	172.22.120.23	Windows Server		Default Location	⋮
	Core Infrastructure	ip_172.22.120.24	172.22.120.24	Windows Server		Default Location	⋮
	Core Infrastructure	ip_172.22.120.26	172.22.120.26	Windows Server		Default Location	⋮
	Core Infrastructure	ip_172.22.120.27	172.22.120.27	Linux/Other Unix		Default Location	⋮
	Core Infrastructure	Some Windows Server	10.98.101.161	Windows Server		alpha-x1:DgeX Running	⋮
	Core Infrastructure	Traverse Server	127.0.0.1	Windows Server		Default Location	⋮
	Core Infrastructure	tvui	10.98.101.155	Linux/Other Unix		alpha-x1:DgeX Running	⋮

Search and Filter Options

Use the filter icon in the far left of the titlebar to display filter options.

- Enter a free-form **Search** string to filter by Device Name or Address.
- Select values by filter *facet*. For example, by Device Type.
- Your selected filter criteria displays just below the title bar.
- Filter settings are remembered when you leave this page and return to it.

Manage Perspectives

Use the perspective icon to select or save a filter by name.

- Click the **Create New Perspective...** to save the currently selected filter criteria to a new name.
- Click the filter icon to modify the perspective, then click the **Save** icon to resave the perspective.
- Use a selected perspective's options ⋮ icon to **Clone** or **Delete** the perspective.
- Perspectives cannot be shared between users.

Add or Edit a Single Device

- Click the **Create New Device** *(page 20)* + icon to create a new device manually.
- Click any single row to display the **Device Details** dialog for an existing single device. These are the same properties as **Create New Device** except for the **Suspended** checkbox.

Edit Multiple Devices

1. Check multiple rows.
2. Click the edit icon in the page title bar.
3. Check each property you want update and enter a value.
   - ➢ These are the same properties as **Create New Device** except for the **Suspend/Resume** checkbox.
4. Click **Apply**.

Delete Devices

> **Warning:** Deleting a device will remove all information about that device from the database, including all historical records. Deletions are not reversible. Suspending a device may be preferable because there is no loss of data.

1. Check multiple rows.
2. Click the delete 🗑 icon.
3. Click **Delete**.

Suspending a Device

- Edit one or more device rows, then click the **Suspended** checkbox.
- When a device is suspended, polling and data collection for all tests on the device are suspended. All actions and notifications associated with the tests are not generated.
- Time is not included in total downtime reports since it is considered a planned outage.
- A 'polling disabled' icon ⊗ displays in the **Status** column of the **Manage Device** page when a device is suspended.
- Tests can also be suspended.

Row Options

Click a device row's options ⋮ icon to select:

- **Update Existing Tests** - Displays the Test Management page, filtered by the selected device.
- Create New Standard Tests
- Create New Advanced Tests
- Move Device
- Export Device
- Update Device Dependency.
- Test Baseline Management
- Create Device Template
- **Delete Device** - Deletes the existing device.

Header Options

Click the ⋮ icon in the header to select:

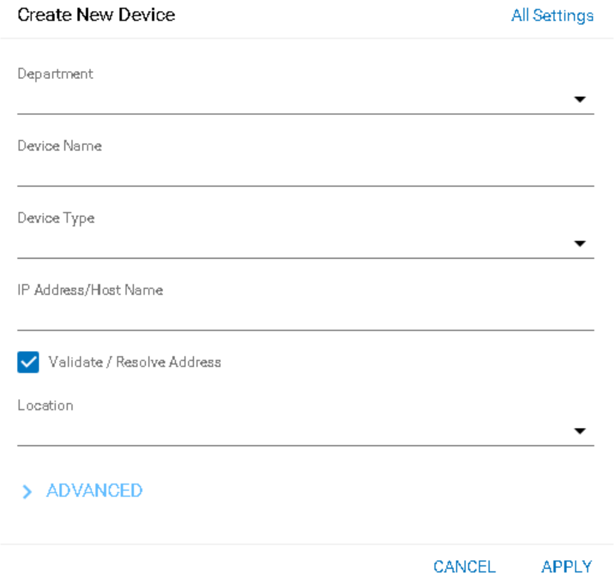
- Device Dependency - Sets a dependency for all devices shown by the current filter.
- Test Baseline Management - Sets baseline test thresholds all devices shown by the current filter.

Create New Device

You can create a new device manually. See **Network Discovery** *(page 15)* to create devices automatically.

1. Navigate to Administration > **Devices**.
   - ➢ Click the **Create New Device** *(page 20)* ⊕ icon to create a new device manually.

- Click any single row to display the **Device Details** dialog for an existing single device. These are the same properties as adding a new device.



Create New Device All Settings

Department

Device Name

Device Type

IP Address/Host Name

☑ Validate / Resolve Address

Location

> ADVANCED

CANCEL APPLY

2. Enter values in these required fields:
   - **Department** - Only displays when logged in as an administrator.
   - **Device Name** - Enter a name for the device.
   - **Device Type** - Select the type of device you are configuring from the drop down list (for example Linux or any other UNIX server, Windows server, managed switch/hub, IP router, firewall appliance, load balancer, proxy server, VPN concentrator, wireless access point or any other).
   - **IP Address/Host Name** - Type in the fully qualified host name or IP address of the device.
   - **Validate / Resolve Address** - If checked, validates the address immediately when you click **Apply**.
   - **Location** - Select a location. Locations are created by a superuser using the Superuser > DGE Mgmt page. (Each DGE Location is a collection of DGEs, not necessarily in the same physical location, that are grouped for load-balancing purposes.) If this device will be monitored via WMI, select a DGE Location that contains WMI-enabled DGEs.
3. You can now click **Apply** or...
4. Click **Advanced** to enter values in these optional fields.
   - **Device/OS Vendor**
   - **Device/OS Model/Version**
   - **Tag 1** through **Tag 5** - Specify custom attributes. You can use these attributes to create rules for populating device containers. For example, if can use **Tag 1** to store values for the `City` the device is located in, **Tag 2** to store the value of the `State`. Once users have entered city and state information for each device, you can create a device container that automatically includes all devices where `City` equals `San Jose` and `State` equals `CA`.
   - **Comment** - Add a comment as necessary.
   - **Display Comment in Summary** - If checked, displays the comment on the Status > Devices > Device Summary page..
   - **Automatically Clear Comment When In OK State** - If checked, clears comments from device information when a device is "OK". This option is useful during maintenance periods. If you are disabling a device maintenance, you can insert a text message (such as `down for maintenance`) in the comment field and click on the **Display** comment on the **Summary Screen**

to display the message. If you select the **Automatically Clear Comment When...** option, this text message is automatically cleared when the device is enabled and has 0% packet loss. This prevents situations where a device fails after maintenance, but (because of the maintenance message) the administrator sees the device as down due to maintenance.

- **Flap Prevention Wait Cycles** - Select the number of cycles to show a state of TRANSIENT when a devices has switched to a new state. For example, assume the flap-prevention cycle is configured to be 2, and a ping test is configured for a 3 minute interval. When the ping test switches from a state of OK to a state of WARNING, the **Traverse** user interface will display the ping test in a TRANSIENT state for 2 additional cycles (2 times 3 min = 6 min) before displaying the ping test in a WARNING state.
- **Enable Smart Notification** - Leave selected to prevent getting alarms on tests when the device is unreachable. See Smart Notifications for more information.
- **Enable Test Parameter Rediscovery** - If checked, several other options display on this page. **Traverse** uses these options to periodically rediscover SNMP and WMI tests. See Test Parameter Rediscovery for more information.

5. Click **Apply**..

All Settings

Click the **All Settings** link to create a device manually using the legacy **Create Device** page. The **Create Device** page has these additional properties.

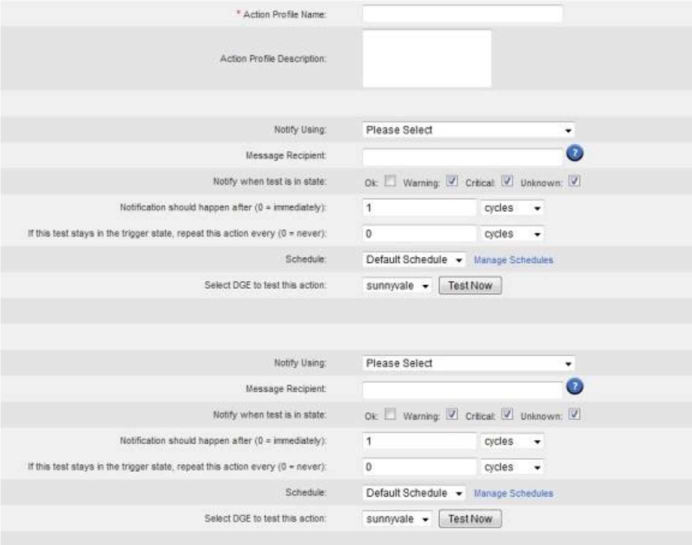
- Click **All Settings** create a device using the legacy **Create Device** page. This page includes
- **Create New Tests After Creating This Device** - If checked, when you save this page, an additional **Add Standard Tests** page displays enabling you to create tests for this device.
- **Create Device Dependency After Creating This Device** - If checked, when you save this page, an additional window displays enabling you to assign the device a parent device. See Device Dependency.
- **Enable Network Configuration Management** - If checked, **Traverse** backs up configurations for a network device. See Network Configuration Manager for more information. If this option is selected, an additional **Schedule Configuration Backup Frequency** option displays. Enter a frequency and choose Hour(s) or Day(s) from the drop-down menu to enable automated backups.
- **Enable Process Collection** - If checked, you can use the process monitor to return metrics for device processes. Requires the device be either WMI or SNMP enabled.**Read Only** - Displays only for admin group users. Enables an administrator to create a read-only device in a department.

Creating Actions and Schedules

When a test result crosses a threshold, **Traverse** takes action based on rules defined in action profiles. Some possible actions include sending email, sending SNMP traps, opening trouble tickets, or running an external script.

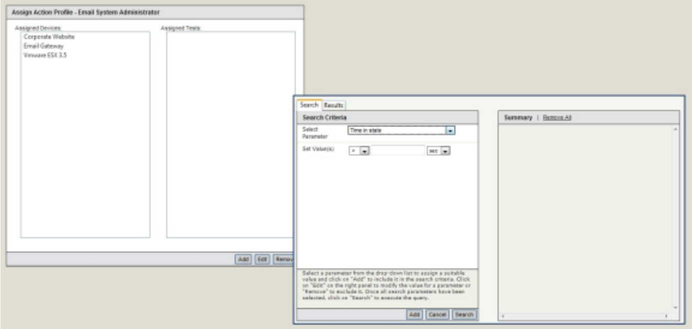
1. Navigate to Administration > Actions > **Create an Action Profile**.

2. Create an action profile with two levels of escalation. In this example, email is sent immediately to the admin when a test goes into warning, critical, or unknown state, and to the manager after a test is critical for 15 minutes during peak hours.



* Action Profile Name:	
Action Profile Description:	
Notify Using:	Please Select
Message Recipient:	
Notify when test is in state:	Ok: ☐ Warning: ☑ Critical: ☑ Unknown: ☑
Notification should happen after (0 = immediately):	1 cycles
If this test stays in the trigger state, repeat this action every (0 = never):	0 cycles
Schedule:	Default Schedule Manage Schedules
Select DGE to test this action:	sunnyvale Test Now
Notify Using:	Please Select
Message Recipient:	
Notify when test is in state:	Ok: ☐ Warning: ☑ Critical: ☑ Unknown: ☑
Notification should happen after (0 = immediately):	1 cycles
If this test stays in the trigger state, repeat this action every (0 = never):	0 cycles
Schedule:	Default Schedule Manage Schedules
Select DGE to test this action:	sunnyvale Test Now

3. Click **Create Action Profile** to create the profile.
4. To assign this profile to tests, click **Assign to Tests** in the row where the new action profile now appears on the **Manage Action Profiles** page, and then click **Add**.
5. Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**.



Assign Action Profile - Email System Administrator

Assigned Devices:
Corporate Website
Email Gateway
Vmware ESX 3.5

Assigned Tests:

Search Criteria

Select Parameter: Time in state

Set Value(s): > sec

Select a parameter from the drop-down list to assign a suitable value and click on "Add" to include it in the search criteria. Click on "Edit" on the right panel to modify the value for a parameter or "Remove" to exclude it. Once all search parameters have been selected, click on "Search" to execute the query.

6. In the **Results** pane, select the devices whose tests you want to use the action profile, and then click **Assign Action Profile**.
7. The **Assign Action Profile** page now lists all of the devices with tests to which this action profile is assigned, and if you click on a device, you can see the specific tests on that device that are using the profile.

By default, tests and actions run all the time, but you can control when they run by creating and assigning schedules to them. For instance, you might want some tests and actions to run only during business hours.

1. Navigate to Administration > Other > Custom Schedules > **Create a Schedule**.
2. Enter "business hours" in the **Schedule Name** field, uncheck all the boxes for days and times that fall outside of business hours, and then click **Create Schedule**.
3. To assign this schedule to a device, click **Select Devices For Schedule** in the row where the new schedule appears, and then click **Add**.
4. Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**.

5. In the **Results** pane, select the device you want to add, and then click **Assign Schedule**. The new schedule is assigned to all tests for that device.

You can also assign a schedule to specific tests through device administration.

1. Navigate to Administration > **Devices** and click **Tests** in the row for the device whose tests you want to schedule.
2. Click the **Modify** icon in the row for the test you want to schedule, and then use the drop-down Schedule menu to assign a schedule.

You can assign the new business hours schedule to the actions in your action profiles as well.

1. Navigate to Administration > **Actions** and click **Update** in the row for the action profile you created.
2. For each action, use the drop-down **Schedule** menu to assign a schedule.

Adjusting Thresholds & Baselining

Traverse comes with pre-defined thresholds for most metrics, but these warning & critical thresholds might be too low for your environment and require adjustments. If you have a small number of devices, and if you are seeing some devices in warning or critical state for long periods of time, you should click on the devices and increase the thresholds as needed.

1. Click on Status > **Tests** from the main menu
2. Click once on the test name which is in red or yellow state to select that row. Note the current result, and then click on the **edit** icon on the top right menu.
3. On the **Update Test** page, change the warning threshold to be a little higher than the current value for the test that you noted earlier and a matching critical threshold (slightly higher than warning).
4. Click on the **Submit** button.
5. Repeat these steps for the remaining tests which are in warning or critical state.

If you have a large number of devices, you can use the "baselining" feature in **Traverse** to automatically adjust the thresholds based on the historical data collected. This option is under Administration > Devices > **Test Baseline Management**.

Adaptive Thresholds

Traverse also supports dynamic, **Adaptive Thresholds**. This feature allows setting alarm thresholds that match varying patterns of use or load in the IT infrastructure. For example, if nightly back-up jobs increase the utilization levels of a server during the evening hours, then you can set higher threshold levels for this time period so that unnecessary alarms are not generated. Currently you have to enable this on a per test basis. To access this feature for a test:

1. Select a device and display its tests by going to Administration > Devices > **Tests**
2. Then click on the **Modify** button for a test, and select the **Time Based Threshold** checkbox.
3. You can either click on the **Configure** link if you want to set the thresholds manually, or else you can configure the thresholds automatically using the baselining feature by going to Administration > Devices > **Test Baseline Management**.
4. Click on the **Submit** button.

Generating Reports

Traverse has extensive and flexible reporting generated in real time from data collected by your DGE extensions and relayed to your **Traverse** instance in the cloud. Navigate to **Reports** to access the different report capabilities. **Traverse** reports are organized and accessible in four areas, each one serving a specific purpose.

Advanced

These are a set of pre-defined reports that allows users to view and analyze different "types" of performance data for a user-specified set of devices or containers (and some additional context depending on the report itself). These reports are designed to allow users to quickly perform specific types of operational analysis of the IT infrastructure, and answer some commonly asked questions for specific tests, devices and containers.

Custom

There reports allow users to conduct system-wide or broader analysis of events, thresholds, capacity, future-trending and availability. Users have greater flexibility in selecting the report parameters, and can choose to run more granular reports for specific test, devices and containers if desired.

SLA

These reports are designed for the purpose of historical and deeper analysis of the SLA metrics and measurements configured and monitored in **Traverse**.

Ad Hoc Reports (My Reports)

Users can create ad hoc report queries for the first three types of reports, and retrieve and run these in the future. **Traverse** allows adding individual components from the various pre-defined reports into the same composite, user-specific report. The reporting framework is very flexible and allows completely arbitrary user-defined statistics generated on an as needed basis.

1. Run a report, and then click on the icon next to a component title to bring up the **Add To My Reports** dialog.
2. Name your ad hoc report in the **Create A New Report** field, and then click **Submit**.
3. Your saved report now shows up when you navigate to Reports > **My Reports**, where you can click the name of the report to run it.

Scheduling Automatic Reports

You can also schedule any saved report (saved query parameters or ad hoc reports) to execute automatically and email the results to a list of recipients.

1. Navigate to Reports > Emailed > **Create A Scheduled Report**.
2. Name your scheduled report in the **Scheduled Report Name** field, use the drop-down **Generate Using Saved Query** menu to select a saved report, and then enter the recipient(s) and define the schedule.

Security Model

The **Traverse** security model controls user access to the data generated by customer networks and to **Traverse** user functions that act on that data.

> **Note:** A full description of the security model is described in **Users and Departments** *(http://help.kaseya.com/webhelp/EN/TV/9050000/index.asp#17371.htm)* in the *Traverse User Guide*.

To help quickstart your deployment of **Traverse**, the most common security scenario for MSPs is described below. This configuration will ensure that *all* your MSPs have access *across all* departments. Keep in mind the following guidelines:

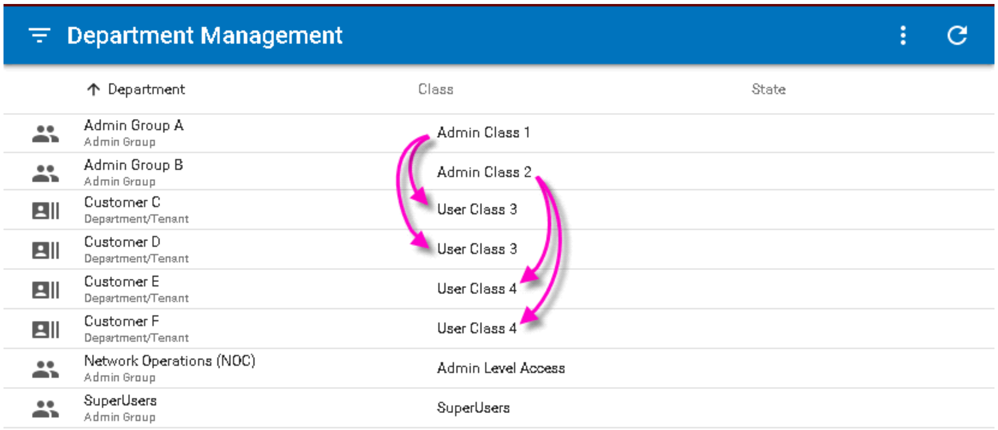
- Create a unique **department** for each customer organization. You may need to create more than one department for larger organizations.
- Ensure all the departments you create use the same, single **user class**.

- Define the customers of MSPs as **users** of a selected department. Users of departments only have access to the data in their own department. A department user with the same name as the department is created automatically for you, each time you create a department.
- Define all MSPs as users of the same, single **admin group**. Each admin group can only be assigned to one **admin class**. *Ensure the admin class you select is mapped to the single user class you are using for all your departments.*

Some of the steps below require `superuser` access. Your configuration steps make use of the following pages, in case you have to return to them.

- Superuser > **User Class**
- Superuser > **Admin Class**
- Administration > **Departments**

When you're done, review the Administration > **Departments** page. It's a good way to summarize your security configuration, as shown in the example below:



Department Management

Department	Class	State
Admin Group A Admin Group	Admin Class 1	
Admin Group B Admin Group	Admin Class 2	
Customer C Department/Tenant	User Class 3	
Customer D Department/Tenant	User Class 3	
Customer E Department/Tenant	User Class 4	
Customer F Department/Tenant	User Class 4	
Network Operations (NOC) Admin Group	Admin Level Access	
SuperUsers Admin Group	SuperUsers	

Configure an Admin Group and Admins

1. Log in to your **Traverse** website as `superuser`.
2. Navigate to Superuser > **User Class** and click on **Update** for the `Default User Class`.
3. Change the name to be `Default Customer Class` and click **Update User Class**. Alternatively, you can create a new user class instead of renaming the existing one.
4. Navigate to Superuser > **Admin Class** and create a new admin class called `MSP Class`.
5. Now click **User Class Mappings** and then **Assign User Class to Admin Class**. Select the default grid that is presented and click the **Update Privileges** button.
6. Navigate to Administration > **Departments** and click **Create new Admin Group**. Create a new admin group called `MSP Group` belonging to the `MSP Class`.
7. Create new users in the `MSP Group` for each of your staff by going to Administration > **Departments** and clicking on **Create User**.
8. At this point, you have the basic security model setup with all your staff belonging to `MSP Group`.

Configure a Department and User

1. Log into your **Traverse** website as `superuser`.
2. Navigate to Administration > **Departments** and then click **Create New Department**.
3. Give a meaningful name to the department. *A default user will be automatically be created with the same name as the Department name.* You can provide this user logon to the MSP's customer if the customer requests access.
4. Ensure the new department uses the `Default Customer Class` described in step 2 of the previous procedure.

5. You can optionally create a **Read Only** user for this same department. Click **Create User** and add a new user. Using the user's email address as the login is recommended. Make sure you set the user's role to **Read Only** when you do.

> **Creating URL with auto-login:** You can create a URL with an encrypted username and password to do autologin for a single **Traverse** page by using the Auto-Login URL generator at **www.zyrion.com/support/tools/urlgen/** *(http://www.zyrion.com/support/tools/urlgen/)*

Adding Additional DGE Extensions

Installing a DGE extension is required to relay monitoring data from a local network to your **Traverse** website. Use the following procedure for creating *additional* DGE extensions.

> **Note:** Adding **additional** DGE extensions to your **Traverse** Cloud instance requires a different procedure than the one used to install your first DGE extension.

1. Navigate to Superuser > **DGE Mgmt**.
2. Click **Create New DGE Extension**.
3. Provide a unique name like `dgex-customerA`.
4. Give a suitable **Description** to identify the customer.
5. Select the upstream DGE name from the drop down list. This is the **Upstream DGE Name** *(page 4)* you were originally assigned when your **Traverse** website was created. Unless support has created additional upstream DGEs for you, there should only be one upstream DGE you can select.
6. Select the **Upstream DGE Fully Qualified Host Name/IP Address**. This is `your-unique-site-name.kaseyatrials.com` without the `http://` prefix.
7. Click on **Create DGE Extension**.
8. Run the DGE extension installer.
9. Installations steps are **described in detail here** *(page 7)*.
10. When the installer prompts you to enter a **DGE Name**, ensure it matches the **Unique Name** you just specified above for the new DGE extension you are creating.
11. Finish up by confirming the "health" of the new DGE extension, **as described in the installation procedure** *(page 11)*.
12. You are now ready to provision the monitoring of devices for this new network by running Network Discovery or by adding devices and tests manually.

Branding (Logos)

If the provided **Traverse** license permits you to change the logo, you can set the logo and theme and custom URL for each of the customers (and intermediate MSPs) by logging in as `superuser` and going to Administration > **Departments** and selecting **Themes** from the **Modify** column.

Chapter 3

Advanced Features

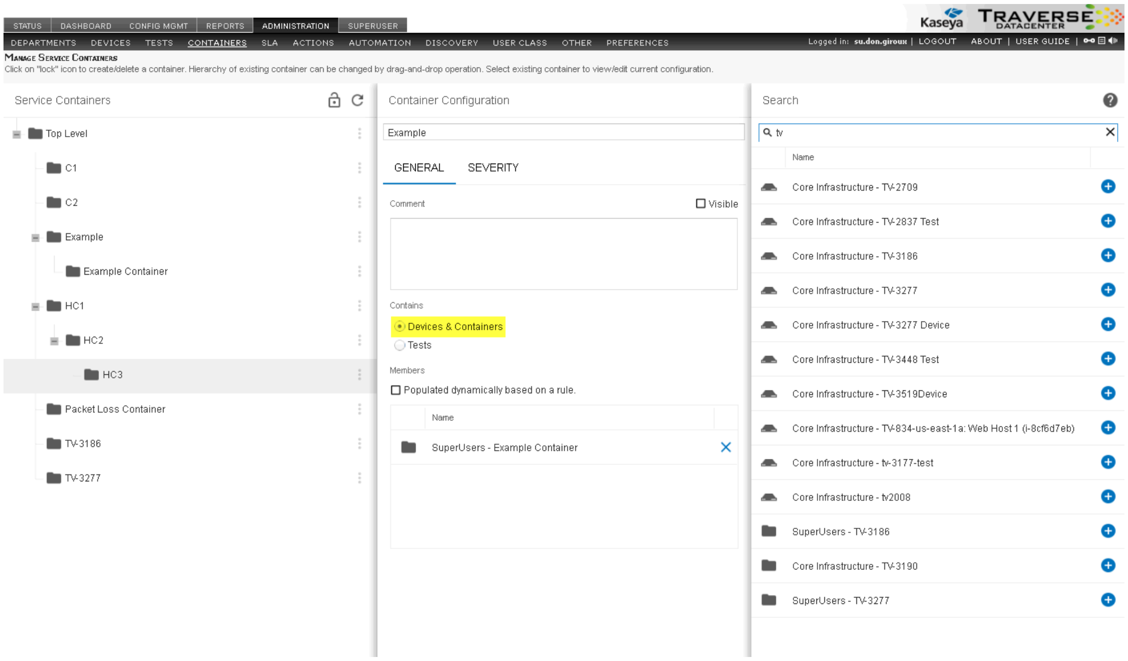
In This Chapter

Service Monitoring & Containers

Service containers allow you to group tests and devices to create logical, business-oriented views of your network in addition to your hardware-oriented views. A service container can hold virtual devices (special types of containers that hold only tests), real devices, or other service containers.

Creating a Service Container for Devices

1. Navigate to Administration > Containers > **Create a Service Container**. A middle **Container Configuration** panel displays.
2. Enter `Servers` in the field at the top of the **Container Configuration** panel.
3. Select the **Contains: Devices & Containers** option.
4. You can assign devices to a container either by performing a search in the right hand panel and manually selecting the devices to include, or by specifying rules and having the results automatically assigned to the container.
5. For this example, check the **Populated dynamically based on a rule** checkbox. A **Define Rule** panel slides in from the right side of the page. Enter `server` in the **Device Type** field. Click **Apply** to see which devices match this rule. You can add additional rules, such as entering `*win*` in the **Device Name** field to filter the list of devices found even further.
6. Click the **Severity** tab in the middle panel when you are done.



MANAGE SERVICE CONTAINERS

Click on "lock" icon to create/delete a container. Hierarchy of existing container can be changed by drag-and-drop operation. Select existing container to view/edit current configuration.

Service Containers:

- Top Level
  - C1
  - C2
  - Example
    - Example Container
  - HC1
    - HC2
      - HC3
  - Packet Loss Container
  - TV-3186
  - TV-3277

Container Configuration: Example

Comment □ Visible

Contains

● Devices & Containers

○ Tests

Members

□ Populated dynamically based on a rule.

Name: SuperUsers - Example Container

Search: tv

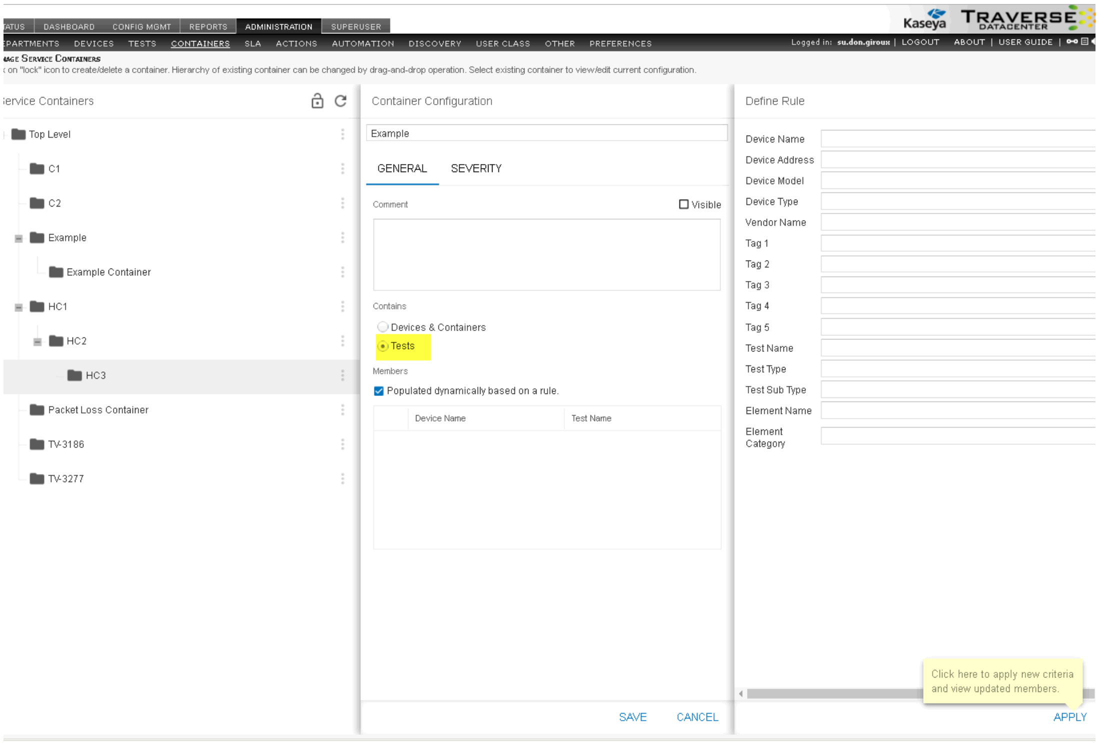
- Core Infrastructure - TV-2709
- Core Infrastructure - TV-2837 Test
- Core Infrastructure - TV-3186
- Core Infrastructure - TV-3277
- Core Infrastructure - TV-3277 Device
- Core Infrastructure - TV-3448 Test
- Core Infrastructure - TV-3519Device
- Core Infrastructure - TV-834-us-east-1a: Web Host 1 (i-8cf6d7eb)
- Core Infrastructure - tv-3177-test
- Core Infrastructure - tv2008
- SuperUsers - TV-3186
- Core Infrastructure - TV-3190
- SuperUsers - TV-3277

7. Assign an action profile if desired, decide the criteria for determining the severity status of the container, and then click **Save**.

Creating a Service Container for Tests

1. Navigate to Administration > Containers > **Create a Service Container**.
2. Enter `Test Type Container` in the field at the top of the **Container Configuration** panel.
3. Select the **Contains: Tests** option.

4. You can assign monitoring tests to a container either by performing a search in the right hand panel and manually selecting the test to include, or by specifying rules and having the results automatically assigned to the container.
5. For this example, check the **Populated dynamically based on a rule** checkbox. A **Define Rule** panel slides in from the right side of the page. Enter `Ping` in the **Test Type** field. Click **Apply** to see which devices have tests that match this rule.
6. Click the **Severity** tab in the middle panel.
7. Assign an action profile if desired, decide the criteria for determining the severity status of the container, and then click **Save**.



ᴀɢᴇ Sᴇʀᴠɪᴄᴇ Cᴏɴᴛᴀɪɴᴇʀѕ
: on "lock" icon to create/delete a container. Hierarchy of existing container can be changed by drag-and-drop operation. Select existing container to view/edit current configuration.

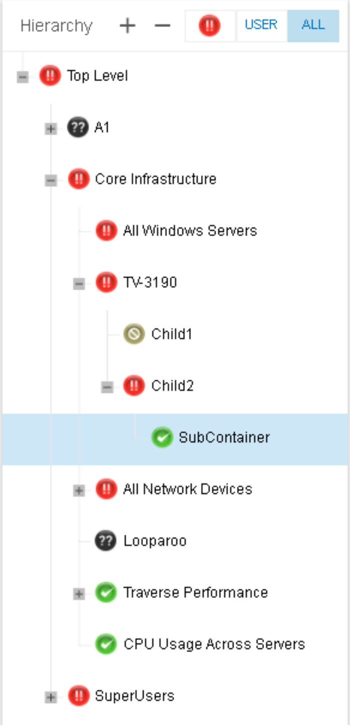
Container Configuration: Example

Contains: ○ Devices & Containers ● Tests

Members: ☑ Populated dynamically based on a rule.

Nesting Service Containers

You can nest service containers to build a logical hierarchy of your environment. For example, you might have critical services for different departments within an organization, all contained within a `Critical Services` container.

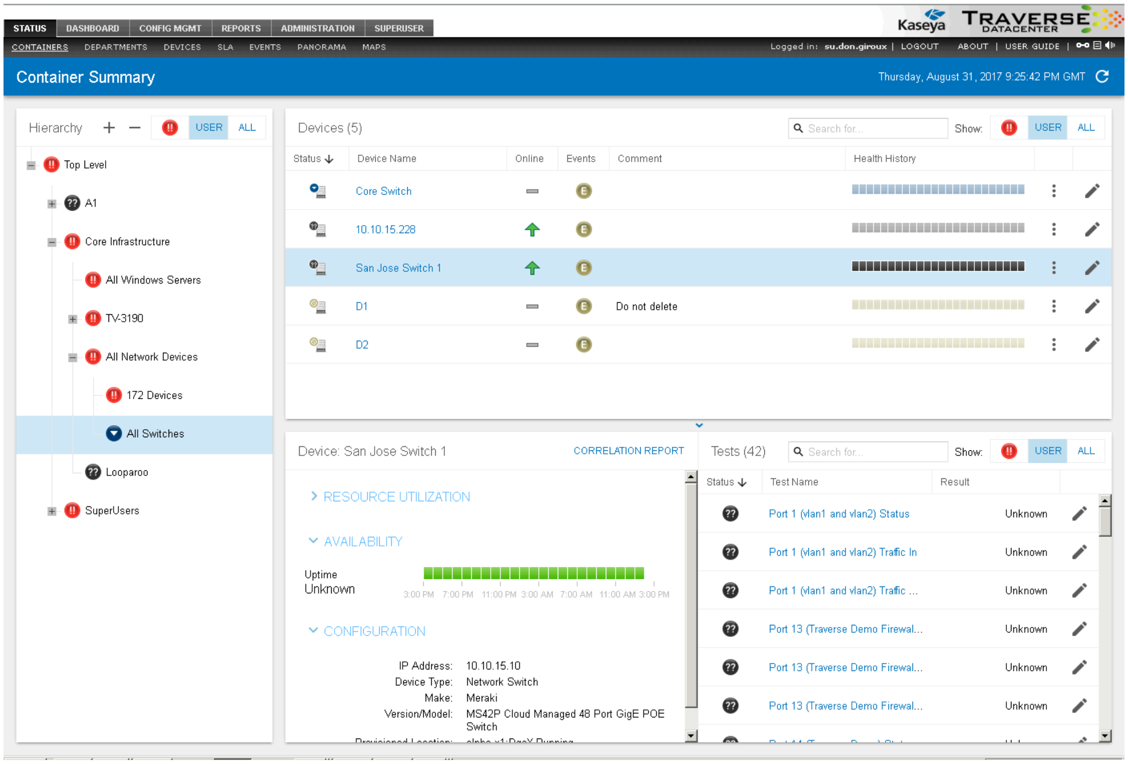


- Top Level
  - A1
  - Core Infrastructure
    - All Windows Servers
    - TV-3190
      - Child1
      - Child2
        - SubContainer
    - All Network Devices
    - Looparoo
    - Traverse Performance
    - CPU Usage Across Servers
  - SuperUsers

Examining Service Container Status

1. Navigate to Status > **Containers** to view a status summary for all containers. **Traverse** provides a number of built-in containers ready to use.
2. Click on a container name to list its contents.
3. Drill down into the container hierarchy to reach a test container. Then click the **Correlation Report** button at the top of the page to generate reports of **Recent Events** and **Correlation**.
4. Click on a test name to see its status page and access **Long-Term History**, **Trend Analysis**, and **Raw Data** reports.

Note: The ‼ USER ALL options filters the hierarchy of containers in the left hand panel, and items displayed in the right hand panel, *by their state*. Set state filter preferences for the **User** option using the Administration > Preferences > **Only Show Devices In Following State(s) When Filter Is On** settings.



Status	Device Name	Online	Events	Comment	Health History
	Core Switch	—	E		
	10.10.15.228	↑	E		
	San Jose Switch 1	↑	E		
	D1	—	E	Do not delete	
	D2	—	E		

IP Address: 10.10.15.10
Device Type: Network Switch
Make: Meraki
Version/Model: MS42P Cloud Managed 48 Port GigE POE Switch

Status	Test Name	Result
??	Port 1 (vlan1 and vlan2) Status	Unknown
??	Port 1 (vlan1 and vlan2) Traffic In	Unknown
??	Port 1 (vlan1 and vlan2) Traffic ...	Unknown
??	Port 13 (Traverse Demo Firewal...	Unknown
??	Port 13 (Traverse Demo Firewal...	Unknown
??	Port 13 (Traverse Demo Firewal...	Unknown

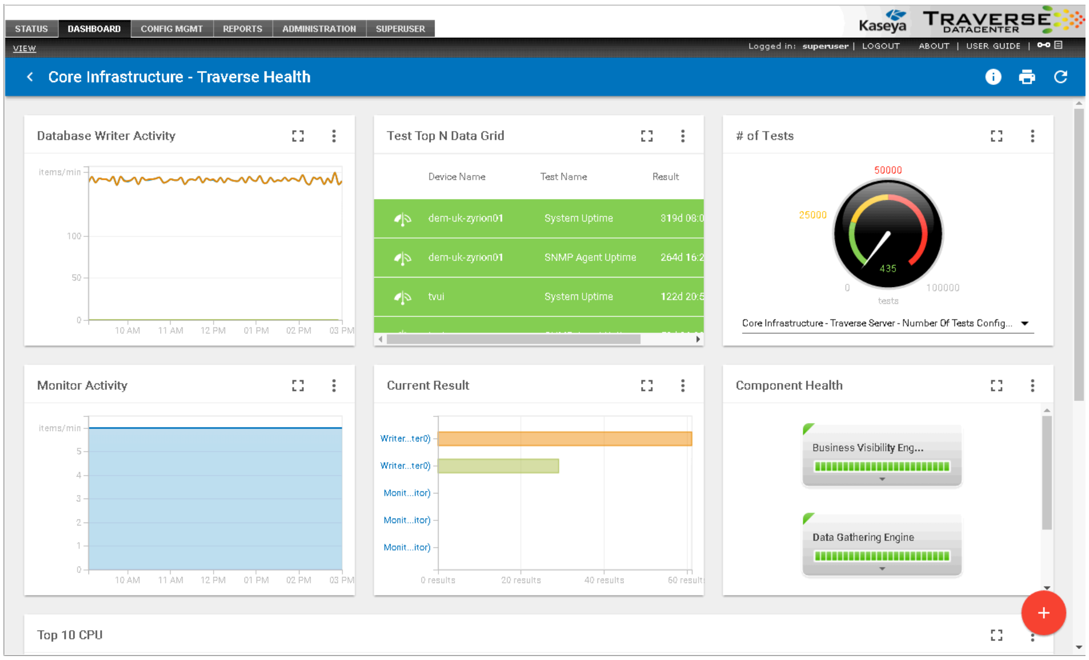
Dashboards Overview

Click the **Dashboard** menu to display the default dashboard.

Dashboards provide real-time, top-level views of all critical issues, services and infrastructure. Whereas service containers let you group tests and devices according to business-oriented views, the dashboards provide a more abstract way to organize information. For example, you might create a dashboard to monitor bandwidth across your entire network, or a dashboard that reports which devices are the top resource hogs.

- You can create multiple dashboards, each containing up to twenty components that can display and chart any metrics selected, and update in real time.
- In some types of components, you can click through to view the test details for reported tests or test summary for devices.
- By default, a dashboard is visible only to the user who created it, but you can mark a dashboard as "Public" to give other users in the department a read-only view of it.

- You can drag and drop your dashboard components to arrange them in the dashboard.



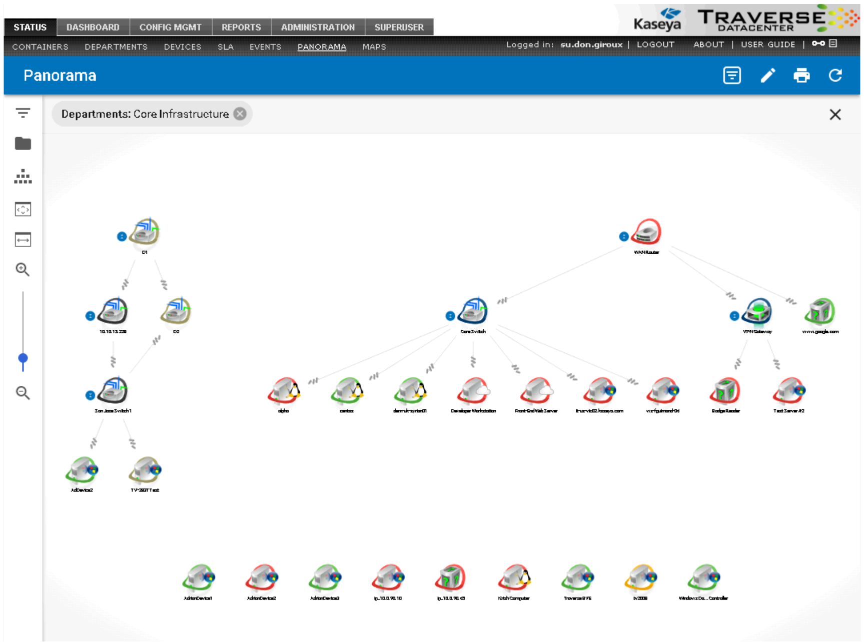
Device Name	Test Name	Result
dem-uk-zyrion01	System Uptime	319d 08:0
dem-uk-zyrion01	SNMP Agent Uptime	264d 16:2
tvui	System Uptime	122d 20:5

Panorama Topology & Maps Display

The **Panorama** feature offers an interactive graphical representation of the devices in your network that are being monitored, including the status of the devices and the dependency relationships between them. **Panorama** offers three different topology layouts, flexible display filters, pan and zoom functionality, the ability to configure and save custom views, and the ability to add or remove device dependencies.

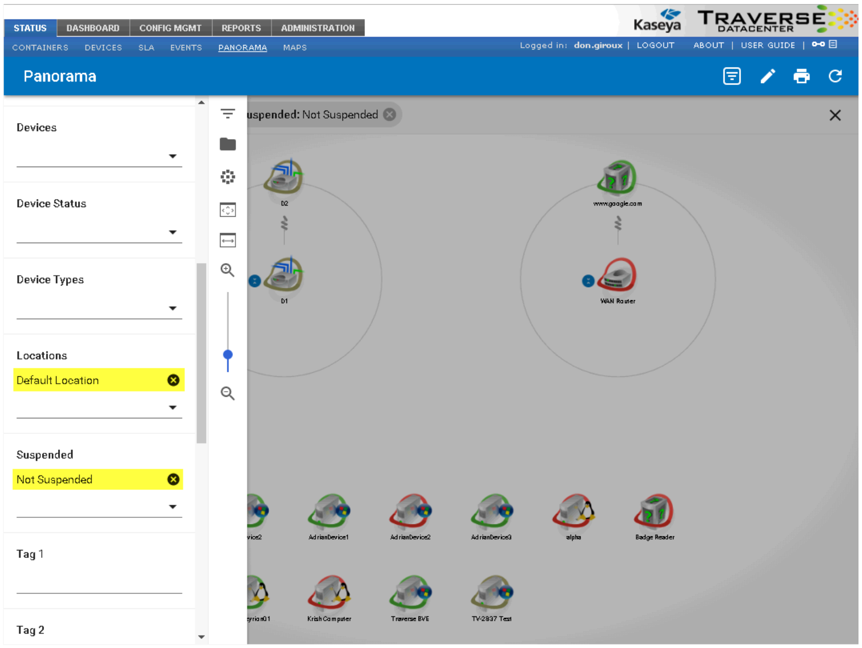
1. Navigate to Status > **Panorama**.

2. Click on the **Display Filter** icon on the top left hand corner to view various filtering and layout options.



Departments: Core Infrastructure

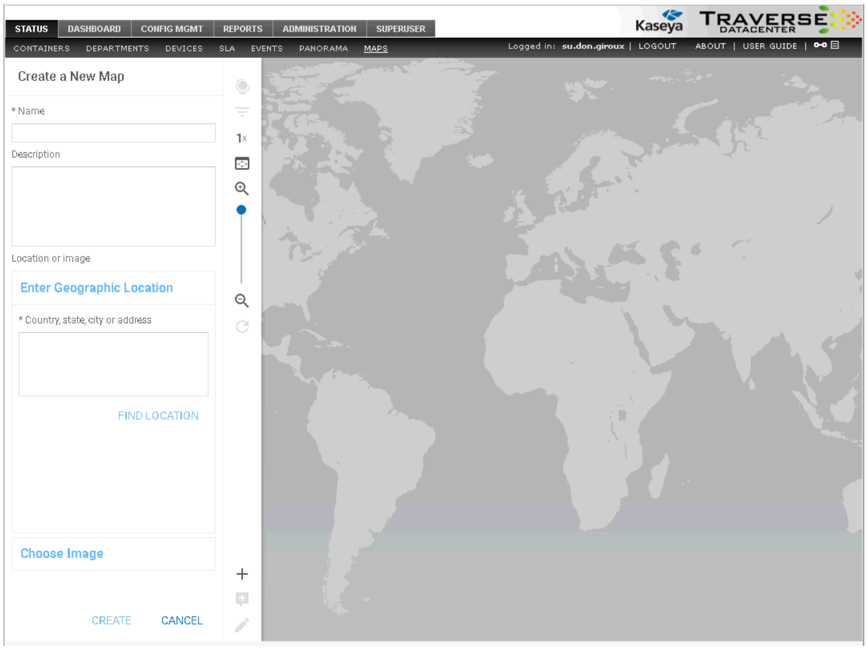
3. Choose between hierarchical (the default), circular, or grid layout options.
4. In edit mode, you can move the position of the nodes on the canvas. You can also add or remove device dependencies. When you click on a device node, a plus sign appears on the icon; click this plus sign and drag to another device to create a new parent/child dependency relationship. When you click on the line connecting two devices, a red X icon appears. Click this X to remove the device dependency.
5. You can filter the devices shown in the topology view by type or status. By default, the **Filter By Device Type & Status** frame opens with the **Device Types** pane expanded. If you click on the **Status** bar, the **Status** pane expands instead. You can also click on the highlight option for each device or state, and device nodes of that type or state will appear highlighted in the topology view.



Devices
Device Status
Device Types
Locations: Default Location
Suspended: Not Suspended
Tag 1
Tag 2

uspended: Not Suspended

6. You can choose to collapse nodes based on depth in the hierarchy or threshold number of child nodes. If you select the **Leaf Nodes Only** check box, only the leaf nodes will be collapsed.
7. After customizing the topology view, you can save it as a custom layout.
8. You can Navigate to Status > **Maps** to view network on a geographical overlay.

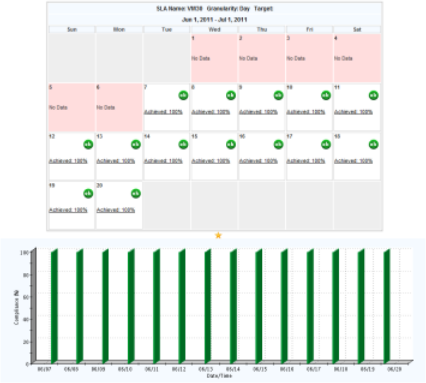


Creating an SLA Measurement

The SLA Manager lets you track compliance against user-defined service level agreement metrics for containers, devices and tests. These SLA metrics are calculated and displayed on a real-time dashboard that displays the amount of time that the metric is within the SLA threshold and also displays how close the metric is to violating the SLA requirement.

1. Navigate to Administration > **SLA**.
2. On the **Configure SLA Manager** page, click **Create an SLA Measurement**.
3. Fill out the fields in the **Create an SLA Measurement** form:
   - **SLA Measurement Name**
   - **Comments/Description**: An optional field that lets you provide some additional descriptive information that will appear in the SLA Manager list of SLA measurements.
   - **Calculation Period**
   - **Calculation Frequency**
   - **Threshold**: The percentage of the Calculation Period that the metric must be in the OK state.
   - **Schedule**: Used to specify business hours and weekdays for calculation of the SLA period.
4. Select whether the SLA is being created for a **Container**, **Device** or **Test**
   - If you selected **Container** or **Device**, then via the drop-down list, select the specific **Container** or **Device** for which the SLA is being created, and then click **Submit**.
   - If you selected **Test**, then click **Submit** to go to the page for selecting the underlying device tests for this SLA metric, and then click **Add**.
5. Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you need, and then click **Apply** to run the search.

6. In the **Search Results** pane, select the tests that you want to be a part of the SLA metric for each device, and then click **Assign to SLA Measurement**.
7. You can now click on the devices you've added in the **Assigned Devices** list, and the tests you selected will appear under **Assigned Tests**.
8. Use the **Add**, **Edit**, and **Remove** buttons to make any further changes to the devices and tests you want to include.
9. Click **Done** to finish creating the SLA measurement.
10. Navigate to Status > **SLA** to view real-time data for your SLA metrics on the SLA Manager dashboard.



SLA Name: VM30 Granularity: Day Target:

Jun 1, 2011 - Jul 1, 2011

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1 No Data	2 No Data	3 No Data	4 No Data
5 No Data	6 No Data	7 Achieved: 100%	8 Achieved: 100%	9 Achieved: 100%	10 Achieved: 100%	11 Achieved: 100%
12 Achieved: 100%	13 Achieved: 100%	14 Achieved: 100%	15 Achieved: 100%	16 Achieved: 100%	17 Achieved: 100%	18 Achieved: 100%
19 Achieved: 100%	20 Achieved: 100%					

Event Manager and Message Transformation

The **Event Manager** console displays messages (traps, logs, windows events) forwarded from **Message Transformation**, as well as threshold violations.

1. Navigate to Status > **Events**.
2. From the **Event Manager** console you can acknowledge, suppress, and delete events. Events can be suppressed until a particular date and time, or until the state changes. The screen refreshes automatically every few minutes (this interval can be changed on the Administration > **Preferences** page).

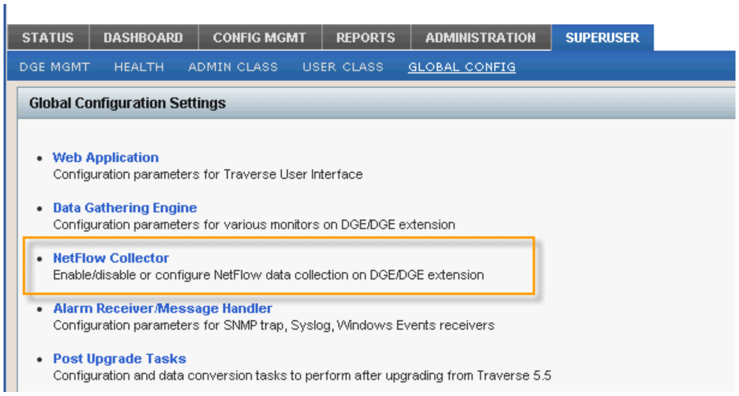
The **Message Transformation** is a distributed component of **Traverse** which accepts syslogs, SNMP traps, Windows events or any other text messages and then searches for specified patterns in these messages. When a pattern match is found, the message string is transformed and a severity assigned to it, and then it is forwarded to the DGE. The processed messages from **Message Transformation** are displayed on the **Event Manager** console and can trigger actions and notifications. For more information, see **Message Transformation** *(http://help.kaseya.com/webhelp/EN/TV/9050000/index.asp#16774.htm)* in the *Traverse User Guide*.

Configuring NetFlow Collectors

Traverse has an integrated NetFlow collector which is pre-installed, but disabled by default.

1. Login to **Traverse** as superuser, or an equivalent user.

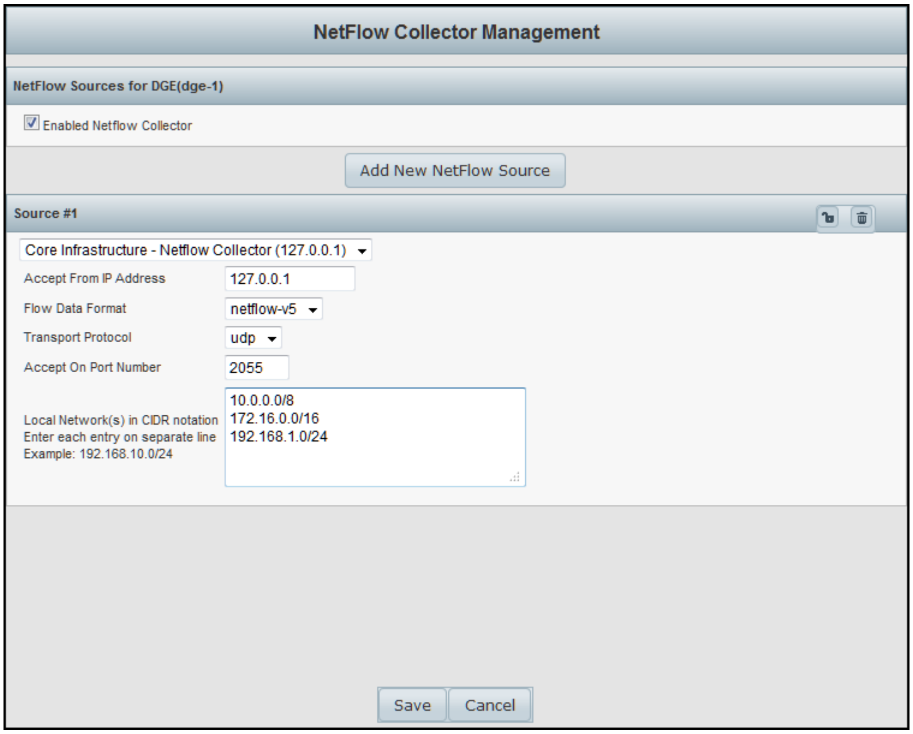
2. Navigate to the Superuser > Global Config > **Netflow Collector** page.



Global Configuration Settings

- Web Application
  Configuration parameters for Traverse User Interface
- Data Gathering Engine
  Configuration parameters for various monitors on DGE/DGE extension
- NetFlow Collector
  Enable/disable or configure NetFlow data collection on DGE/DGE extension
- Alarm Receiver/Message Handler
  Configuration parameters for SNMP trap, Syslog, Windows Events receivers
- Post Upgrade Tasks
  Configuration and data conversion tasks to perform after upgrading from Traverse 5.5

3. Choose the DGE or DGE extension you wish to add a netflow collector on, and select **Update**.
4. Enable the netflow collector, then choose a device from your list of network devices. Only routers, switches, and firewalls can be used as flow sources. Choose the host to allow flow data from. This allows you to send flow data from the loopback interface, or from a different IP than the one provisioned in **Traverse**). Choose the port, and the protocol that **Traverse** will accept. Additionally, you can specify the network that is "inside" of this device, so that **Traverse** can categorize the data from an internal/external standpoint.


NetFlow Collector Management

NetFlow Sources for DGE(dge-1)

☑ Enabled Netflow Collector

Source #1

Core Infrastructure - Netflow Collector (127.0.0.1)

Accept From IP Address: 127.0.0.1

Flow Data Format: netflow-v5

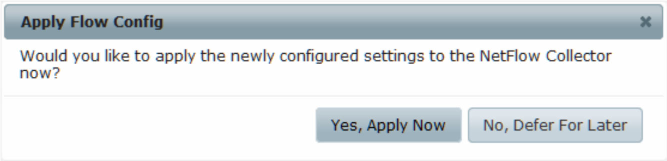
Transport Protocol: udp

Accept On Port Number: 2055

Local Network(s) in CIDR notation
Enter each entry on separate line
Example: 192.168.10.0/24

10.0.0.0/8
172.16.0.0/16
192.168.1.0/24

5. Press the **Save** button when you are done. **Traverse** will respond with the following prompt:

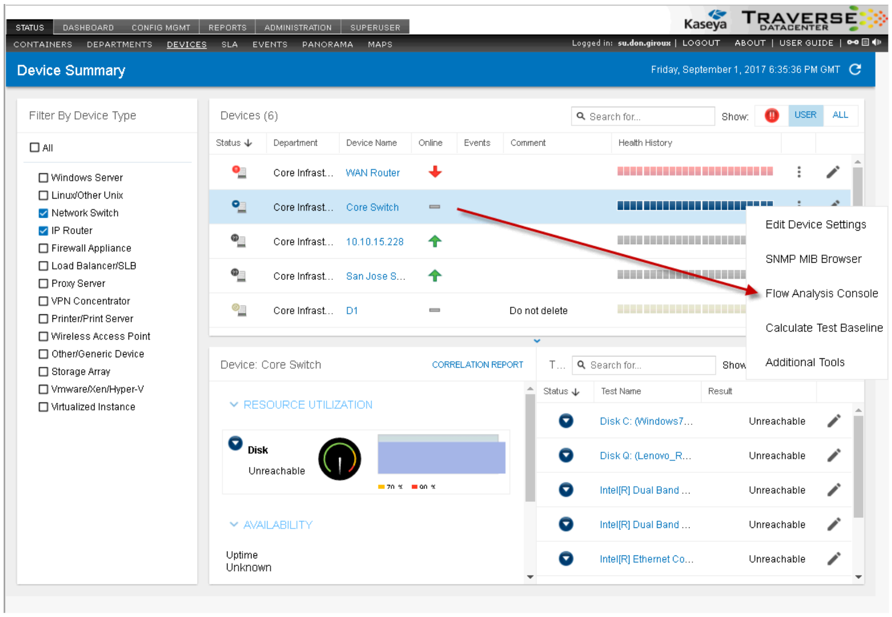

Apply Flow Config

Would you like to apply the newly configured settings to the NetFlow Collector now?

6. Choosing **Yes, Apply Now** will immediately write the new configuration out to the flow collector, and re/start the flow collection subsystem. Choosing **No, Defer For Later** will save your configuration, but not apply it to the DGE extensions nor re/start any flow services.

The Network Flow Analysis Console

Click the **Flow Analysis Console** option for a selected network device or switch on the Status > Devices > **Device Summary** page.



□ All

- □ Windows Server
- □ Linux/Other Unix
- ☑ Network Switch
- ☑ IP Router
- □ Firewall Appliance
- □ Load Balancer/SLB
- □ Proxy Server
- □ VPN Concentrator
- □ Printer/Print Server
- □ Wireless Access Point
- □ Other/Generic Device
- □ Storage Array
- □ Vmware/Xen/Hyper-V
- □ Virtualized Instance

Status	Department	Device Name	Online	Events	Comment	Health History
	Core Infrast...	WAN Router	↓			
	Core Infrast...	Core Switch	–			
	Core Infrast...	10.10.15.228	↑			
	Core Infrast...	San Jose S...	↑			
	Core Infrast...	D1	–		Do not delete	

Uptime
Unknown

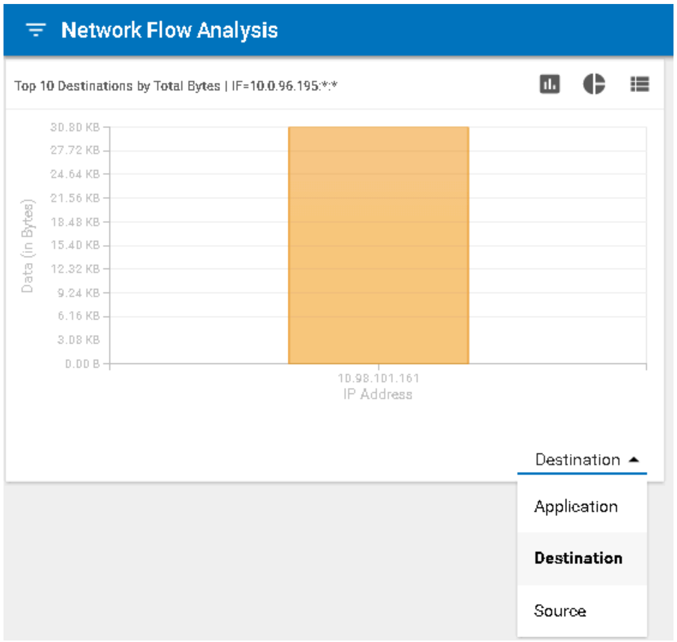
Status	Test Name	Result
	Disk C: (Windows7...	Unreachable
	Disk Q: (Lenovo_R...	Unreachable
	Intel[R] Dual Band ...	Unreachable
	Intel[R] Dual Band ...	Unreachable
	Intel[R] Ethernet Co...	Unreachable

Each chart in the network flow analysis console has a title bar that states which devices (and optionally, which application) are being examined. There are three roles, each represented by an IP address.

- Source
- Destination
- Application

The network flow analysis is always presented from the point of view of the selected device, which may be acting as either source or destination in different contexts. Remember that whether a device is considered the source or destination depends on the direction of flow of packet data on a given port at a given time.

Each chart can be displayed as a table, a pie chart, or a bar chart.



Extensible and Open APIs

Traverse has very powerful APIs which allow access to all components of the software. Users familiar with Perl or C can start using the API very quickly due to its familiar commands and interface. These APIs allow you to configure connections to other legacy products or custom applications.

BVE Flex API

You can use the BVE API to perform bulk changes to tests or devices. The BVE API can be accessed via a direct telnet connection or through the perl API. Any **Traverse** end user can log in to the API and will get access to the same privileges and devices as when logging in via the Web interface.

To log in, ensure that the BVE API is running on the **Traverse** host. Then, from a Windows command prompt, UNIX shell, or alternate telnet client, telnet to port 7661 and enter the following command:

```
telnet your-unique-site-name.kaseyatrials.com 7661
LOGIN <login_id>/<password>
```

The basic commands are list, add, delete, and suspend, which can be applied to contexts such as device, test, and user. The general syntax is `context.command <parameters>`, as in the following examples.

- List all devices.

```
device.list "deviceName=*"
```

- List all tests for a device.

```
test.list "deviceName=xyz", "testName=*"
```

- Set the warning threshold for all line utilization tests to 80%. You can also set this threshold using the Web application.

```
test.update "testName=Line Utilization", "deviceName=*", warningThreshold="80"
```

Other Advanced Features

Linked Device Templates

A **linked device template** contains a group of tests that can then be applied to multiple devices so that each associated device is provisioned with the same tests. The linked device template can also include an action profile and a custom schedule as well. Creating a linked device template, allows you to configure tests for a master device and then apply that template across multiple associated devices. What's important to note is that when the template for the master device is updated, you have the option to push the updated template to all the devices associated with the given linked device template. See the *Traverse User Guide* for instructions on how to use **Linked Device Template** *(http://help.kaseya.com/webhelp/EN/TV/9050000/index.asp#17555.htm)* functionality.

Scheduled Maintenance

Scheduled maintenance allows defining in advance any number of time periods for automatically suspending devices at the start of the time-period, and then automatically resuming the devices at the end of the time-period. This functionality is in addition to the functionality that allows users to manually (on-demand) suspend/resume devices. Both the scheduled and the manual functionality allow you to temporarily turn off all the tests for one or more devices and turn them on again. This is useful for the purpose of performing maintenance tasks on the devices, where you do not want to receive alerts while the device is offline. Once a device is suspended, the polling and data collection for all the tests on the device is suspended and thus any associated actions to the tests will not generate notifications. Furthermore, when a device is suspended (e.g. for maintenance), this time is not included in the total downtime reports since it is considered a planned outage. See the T*raverse User Guide* for instructions on how to use **Scheduled Maintenance** *(http://help.kaseya.com/webhelp/EN/TV/9050000/index.asp#17555.htm)* functionality.

Index